



Administratorhandbuch

HP ThinPro 6.2

© Copyright 2017 HP 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 in den USA und/oder anderen Ländern Marken oder eingetragene Marken der Microsoft Corporation. UNIX ist eine eingetragene Marke von The Open Group. VMware und Horizon View sind in den USA und/oder anderen Ländern eingetragene Marken oder Marken von VMware, Inc.

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

HP haftet – 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 Herstellergarantie für HP Produkte wird ausschließlich in der entsprechenden, zum Produkt gehörigen Garantieerklärung beschrieben. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten.

Erste Ausgabe: August 2017

Dokumentennummer: 940268-041

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, können Sie den Quellcode für die Software von der folgenden Adresse abrufen:

<ftp://ftp.hp.com/pub/tcdebian/pool/thinpro620/>.

Syntaxschlüssel für Benutzereingaben

Text, den Sie in einer Benutzeroberfläche eingeben müssen, wird durch eine Schriftart mit fester Breite dargestellt.

Nr.	Beschreibung
Text ohne Klammern	Elemente, die Sie exakt wie gezeigt eingeben müssen.
<Text in spitzen Klammern>	Ein Platzhalter für einen Wert, den Sie angeben müssen. Lassen Sie dabei die Klammern weg.
[Text in eckigen Klammern]	Optionale Elemente. Lassen Sie dabei die Klammern weg.
{Text in geschweiften Klammern}	Mehrere Elemente, aus denen Sie nur eines auswählen müssen. Lassen Sie dabei die Klammern weg.
	Ein Trennzeichen für Elemente, von denen Sie nur eines auswählen müssen. Lassen Sie dabei den Senkrechtstrich weg.
...	Elemente, die Sie wiederholen können oder müssen. Lassen Sie dabei die Auslassungszeichen weg.

Inhaltsverzeichnis

1 Einführung	1
Weitere Informationen	1
Auswählen einer Betriebssystemkonfiguration	2
Auswählen eines Remoteverwaltungsdiensts	3
Erstmaliges Starten des Thin Clients	3
Wechseln zwischen Administratormodus und Benutzermodus	3
2 Übersicht über die Benutzeroberfläche	5
Desktop	5
Taskleiste	6
Connection Manager (nur ThinPro)	8
3 Verbindungskonfiguration	9
Erweiterte Verbindungseinstellungen	9
Kioskmodus	10
4 Verbindungstypen	11
Citrix	11
Citrix – Allgemeine Einstellungen	11
Optionen	11
Lokale Ressourcen	12
Fenster	12
Firewall	13
Tastenkombinationen	13
Sitzung	14
Citrix – Einstellungen pro Verbindung	14
Verbindung	14
Konfiguration	15
Erweitert	16
RDP	16
RDP – Allgemeine Einstellungen	16
RDP – Einstellungen pro Verbindung	16
Netzwerk	17
Dienst	17
Fenster	18
Optionen	19

Lokale Ressourcen	20
Darstellung	20
Diagnose	21
Erweitert	21
RemoteFX	22
RDP-Sitzungen mit mehreren Monitoren	22
RDP-Multimedia-Umleitung	22
RDP-Geräteumleitung	23
RDP-USB-Umleitung	23
RDP-Massenspeicherumleitung	23
RDP-Druckerumleitung	24
RDP-Audiumleitung	25
RDP-Smart Card-Umleitung	26
VMware Horizon View	26
VMware Horizon View – Einstellungen pro Verbindung	26
Netzwerk	26
Allgemein	27
Sicherheit	27
RDP-Optionen	28
RDP-Darstellung	29
Erweitert	30
VMware Horizon View-Sitzungen mit mehreren Monitoren	30
VMware Horizon View-Tastenkombinationen	31
VMware Horizon View-Multimedia-Umleitung	31
VMware Horizon View-Geräteumleitung	31
VMware Horizon View-USB-Umleitung	31
VMware Horizon View-Massenspeicherumleitung	31
VMware Horizon View-Druckerumleitung	32
VMware Horizon View-Audiumleitung	32
VMware Horizon View-Smart Card-Umleitung	33
VMware Horizon View-Webcam-Umleitung	33
Ändern des VMware Horizon View-Protokolls	34
Anforderungen für die VMware Horizon View HTTPS- und Zertifikatverwaltung	34
Web Browser	35
Web Browser – Allgemeine Einstellungen	35
Web Browser – Einstellungen pro Verbindung	36
Konfiguration	36
Erweitert	36
Zusätzliche Verbindungstypen (nur ThinPro)	36
TeemTalk	36
Konfiguration	36

TeemTalk Sitzungsassistent	37
Erweitert	38
XDMCP	38
Konfiguration	38
Erweitert	38
SSH	39
Konfiguration	39
Erweitert	39
Telnet	39
Konfiguration	39
Erweitert	40
Custom	41
Konfiguration	41
Erweitert	41
5 HP True Graphics	42
Anforderungen auf Server-Seite	42
Anforderungen auf Client-Seite	42
Konfiguration auf Client-Seite	42
Komprimierungseinstellungen	42
Fenstereinstellungen	43
Monitorlayout- und Hardwarebeschränkungen	43
Aktivieren von HP True Graphics für mehrere Monitore auf dem HP t420	43
Tipps und bewährte Vorgehensweisen	44
6 Active Directory Integration	45
Anmeldebildschirm	45
Einmaliges Anmelden	45
Desktop	46
Bildschirmsperre	46
Administratormodus	46
Einstellungen und der Domänenbenutzer	46
7 Systemsteuerung	47
Peripheriegeräte	47
Clientaggregation	48
Konfigurieren der Clientaggregation	49
Konfigurieren der Aggregation-Clients	49
Konfigurieren des Aggregation-Servers	50
Anzeigeeinstellungen	50

Konfigurieren von Druckern	51
Umleiten von USB-Geräten	51
Setup	52
Netzwerkeinstellungen	52
Einstellungen für kabelgebundene Netzwerke	53
Wireless-Netzwerkeinstellungen	54
DNS-Einstellungen	55
IPSec-Regeln	56
Konfigurieren von VPN-Einstellungen	56
Konfigurieren von HP Velocity	57
Sicherheitseinstellungen	57
Lokale Konten	57
Verschlüsselung	57
Optionen	58
Anpassungscenter	58
Verwaltung	59
Komponenten-Manager	60
Entfernen von Komponenten	60
Rückgängigmachen einer Änderung	61
Dauerhaftes Anwenden der Änderungen	61
Active Directory Konfiguration	61
Registerkarte „Status“	61
Registerkarte „Optionen“	62
HP ThinState	62
Verwalten von HP ThinPro-Images	63
Aufzeichnen von HP ThinPro-Images auf einem FTP-Server	63
Bereitstellen eines HP ThinPro-Images über FTP oder HTTP	63
Aufzeichnen eines HP ThinPro-Images auf einem USB-Flash-Laufwerk	64
Bereitstellen eines HP ThinPro-Images mit einem USB-Flash-Laufwerk ...	64
Verwalten eines Clientprofils	64
Speichern eines Clientprofils auf einem FTP-Server	65
Wiederherstellen eines Clientprofils über FTP oder HTTP	65
Speichern eines Clientprofils auf einem USB-Flash-Laufwerk	65
Wiederherstellen eines Clientprofils von einem USB-Flash-Laufwerk	66
VNC-Shadowing	66
Erweitert	67
Zertifikate	67
Zertifikat-Manager	67
SCEP-Manager	68
DHCP-Optionen	68

8 Systeminformationen	70
9 HP Smart Client Services	71
Unterstützte Betriebssysteme	71
Voraussetzungen für HP Smart Client Services	71
Abrufen von HP Smart Client Services	72
Anzeigen der Automatic Update-Website	72
Erstellen eines Automatic Update-Profiles	72
Profile für bestimmte MAC-Adressen	72
Aktualisieren von Thin Clients	73
Verwenden der Methode zur Aktualisierung per Übertragung	73
Verwenden der Methode zur Aktualisierung per DHCP-Kennung	73
Beispiel für die Durchführung DHCP-Kennung	73
Verwenden der Methode zur Aktualisierung per DNS-Alias	74
Verwenden der Methode zur manuellen Aktualisierung	74
Durchführen einer manuellen Aktualisierung	74
10 Profile Editor	76
Öffnen von Profile Editor	76
Laden eines Clientprofils	76
Anpassung von Clientprofilen	76
Auswählen der Plattform für ein Clientprofil	76
Konfigurieren einer Standardverbindung für ein Clientprofil	77
Ändern von Registrierungseinstellungen eines Clientprofils	77
Hinzufügen von Dateien zu einem Clientprofil	77
Hinzufügen einer Konfigurationsdatei zu einem Clientprofil	77
Hinzufügen von Zertifikaten zu einem Clientprofil	78
Hinzufügen eines symbolischen Links zu einem Clientprofil	78
Speichern des Clientprofils	79
Konfiguration eines seriellen oder parallelen Druckers	79
Abrufen der Druckereinstellungen	79
Einrichten von Druckeranschlüssen	79
Installieren von Druckern auf dem Server	80
11 Fehlerbeseitigung	81
Fehlerbeseitigung bei der Netzwerkverbindung	81
Fehlerbeseitigung bei abgelaufenen Citrix Kennwörtern	81
Verwenden der Systemdiagnose für die Fehlerbeseitigung	82
Speichern von Systemdiagnosedaten	82
Dekomprimieren der Systemdiagnosedateien	82


Dekomprimieren der Systemdiagnosedateien auf Windows-basierten Systemen	82
Dekomprimieren der Systemdiagnosedateien auf Linux- oder Unix-basierten Systemen	82
Anzeigen der Systemdiagnosedateien	82
Anzeigen von Dateien im Ordner Commands	82
Anzeigen von Dateien im Ordner /var/log	83
Anzeigen von Dateien im Ordner /etc	83
Anhang A USB-Updates	84
HP ThinUpdate	84
Anhang B BIOS-Tools (nur Desktop-Thin Clients)	85
BIOS-Tool für Einstellungen	85
BIOS Flashing-Tool	85
Anhang C Ändern der Größe der Flash-Laufwerk-Partition	86
Anhang D Registrierungsschlüssel	87
Audio	87
CertMgr	88
ComponentMgr	88
ConnectionManager	88
ConnectionType	89
custom	89
firefox	92
freerdp	98
ssh	108
teemtalk	114
telnet	117
view	121
xdmcp	130
xen	134
DHCP	148
Dashboard	148
Display	149
Domain	151
Network	152
Power	163
SCIM	164
ScepMgr	165

Search	165
Serial	167
SystemInfo	167
TaskMgr	167
USB	168
auto-update	168
background	171
config-wizard	172
desktop	172
entries	173
keyboard	173
logging	174
login	174
mouse	175
restore-points	175
screensaver	176
security	177
shutdown	178
sshd	178
time	179
touchscreen	180
translation	182
usb-update	182
users	183
vncserver	185

Index	189
--------------------	------------

1 Einführung

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

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

Weitere Informationen über diese Betriebssystemkonfigurationen finden Sie unter [Auswählen einer Betriebssystemkonfiguration auf Seite 2](#). Weitere Informationen über das Wechseln zwischen Betriebssystemkonfigurationen finden Sie unter [Anpassungscenter auf Seite 58](#).

Weitere Informationen

 **HINWEIS:** Die Informationen auf den in dieser Tabelle aufgeführten Websites sind möglicherweise nur in englischer Sprache verfügbar.

Ressource	Inhalt
HP Support-Website http://www.hp.com/support	Handbücher für Administratoren, Hardware-Referenzhandbücher, White Papers und weitere Dokumentationen ▲ Suchen Sie nach dem Thin Client-Modell und dann sehen Sie den Abschnitt Benutzerhandbücher der Supportseite für dieses Modell. HINWEIS: HP Device Manager und HP Remote Graphics Software verfügen jeweils über eine dedizierte Supportseite. Suchen Sie daher nach dem Namen der App und sehen Sie dann im Abschnitt Benutzerhandbücher nach.
Microsoft Support-Website http://support.microsoft.com	Dokumentation für Microsoft Software
Citrix Support-Website http://www.citrix.com/support	Dokumentation für Citrix Software
VMware Support-Website http://www.vmware.com/support	Dokumentation für VMware Software

Auswählen einer Betriebssystemkonfiguration

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

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



HINWEIS: Sie können über die Systemsteuerung zwischen Betriebssystemkonfigurationen wechseln (siehe [Anpassungszentrum auf Seite 58](#)).

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

Weitere Informationen zum Kioskmodus finden Sie unter [Kioskmodus auf Seite 10](#).

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

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

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

Auswählen eines Remoteverwaltungsdiensts


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

- **HP Device Manager (HPDM)** ist ideal für große Umgebungen mit einer Vielzahl von Betriebssystemen, einschließlich einer Mischung von HP ThinPro- und Windows®-basierten Thin Clients. HPDM bietet eine größere Vielfalt bei den Verwaltungsoptionen als HP Smart Client Services. Weitere Informationen zu HPDM und eine Downloadoption finden Sie unter <http://www.hp.com/go/hpdm>.
- **HP Smart Client Services** können nur HP ThinPro-basierte Thin Clients verwalten und wurden für die Verwendung mit Smart Zero und ein Szenario ohne Verwaltung optimiert. Weitere Informationen finden Sie unter „[HP Smart Client Services](#)“ auf Seite 71. HP Smart Client Services können Sie von der HP Support-Website herunterladen (siehe [Weitere Informationen auf Seite 1](#)).

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

Erstmaliges Starten des Thin Clients

Wenn Sie einen neuen Thin Client mit HP ThinPro zum ersten Mal starten, wird ein Setup-Programm automatisch ausgeführt. Wenn nach Abschluss des Setup-Programms keine Verbindungen konfiguriert wurden, wird ein Assistent geöffnet, der Ihnen beim Konfigurieren einer Verbindung hilft.

 **TIPP:** Wenn Sie die Konfiguration eines Thin Clients ändern und dann die Konfiguration kopieren und auf anderen Thin Clients bereitstellen möchten, ändern Sie die Konfigurationen zunächst mit der Systemsteuerung. Weitere Informationen finden Sie unter „[Übersicht über die Benutzeroberfläche](#)“ auf Seite 5 oder „[Systemsteuerung](#)“ auf Seite 47. Stellen Sie dann die Konfiguration mit HPDM oder HP ThinState bereit. Weitere Informationen zu HP ThinState finden Sie unter [HP ThinState auf Seite 62](#).

Wechseln zwischen Administratormodus und Benutzermodus

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

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

– oder –

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

Weitere Informationen zur Systemsteuerung finden Sie unter [Taskleiste auf Seite 6](#) und „[Systemsteuerung](#)“ auf Seite 47.




HINWEIS: Wenn Sie zum ersten Mal in den Administratormodus wechseln, werden Sie aufgefordert, ein Administratorkennwort einzurichten. Das Administratorkennwort muss dann jedes Mal eingegeben werden, wenn Sie wieder in den Administratormodus wechseln. Wenn die Active Directory Authentifizierung aktiviert ist, können Sie auch in den Administratormodus wechseln, indem Sie die Domänenanmeldeinformationen eines Benutzers aus der Domänenadministratorgruppe eingeben.

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

2 Übersicht über die Benutzeroberfläche

Desktop

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

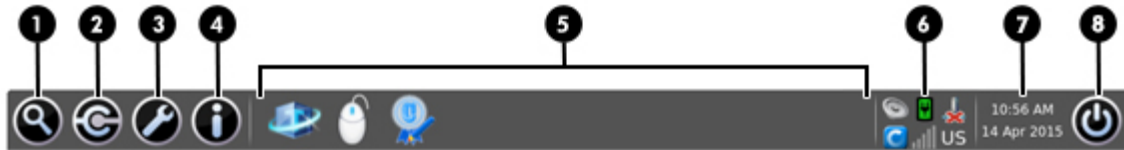


Symbol	Beschreibung
(1)	Desktop <p>In ThinPro können Sie Verbindungsverknüpfungen im Desktopbereich anordnen und das Hintergrunddesign anpassen.</p> <p>In Smart Zero wird der Desktop durch einen anpassbaren Anmeldebildschirm ersetzt. Das Design hängt dabei vom ausgewählten Verbindungstyp ab.</p>
(2)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

Taskleiste



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



Symbol	Beschreibung	
(1)	Suchen	Zum Suchen und Ausführen von konfigurierten Verbindungen, Verbindungs-Managern, Elementen der Systemsteuerung und Energiesparfunktionen.
(2)	Connection Manager	<p>In ThinPro wird mit dieser Schaltfläche Connection Manager in einem neuen Fenster geöffnet. Weitere Informationen finden Sie unter Connection Manager (nur ThinPro) auf Seite 8.</p> <p>In Smart Zero wird mit dieser Schaltfläche ein Menü angezeigt, über das Sie eine Verbindung hinzufügen oder bearbeiten können.</p>
(3)	Systemsteuerung	Zum Konfigurieren des Thin Clients, Wechseln zwischen Administratormodus und Benutzermodus und Suchen nach Software-Updates. Weitere Informationen finden Sie unter „ Systemsteuerung “ auf Seite 47.
(4)	Systeminformationen	Zum Anzeigen von System-, Netzwerk- und Softwareinformationen zum Thin Client. Weitere Informationen finden Sie unter „ Systeminformationen “ auf Seite 70.
(5)	Anwendungsbereich	<p>Zeigt die Symbole für die derzeit geöffneten Anwendungen.</p> <p>TIPP: Um eine Anwendung auszuwählen und in den Vordergrund zu holen, können Sie Strg+Alt gedrückt halten und dann wiederholt auf die Tabulatortaste drücken.</p>
(6)	Systeminfo	<p>Bietet schnellen Zugriff auf Informationen bzw. Informationen zu bestimmten Funktionen und Diensten. Elemente in der Systeminfo können unter anderem folgende sein; einige Elemente werden jedoch möglicherweise abhängig von der Systemkonfiguration nicht angezeigt:</p> <ul style="list-style-type: none"> • Audiomixer • Virtuelle Tastatur • Netzwerkstatus – Wählen Sie dieses Symbol, um eine Liste der verfügbaren Wireless-Netzwerke anzuzeigen und eine Verbindung zu einem der Netzwerke herzustellen, indem Sie ein Wireless-Profil für das Netzwerk erstellen. • Automatic Update-Status – Ein grünes Symbol mit einem Häkchen zeigt an, dass das automatische Update erfolgreich abgeschlossen wurde. Ein gelbes Symbol mit einem Ausrufezeichen weist darauf hin, dass der Automatic Update-Server nicht gefunden wurde oder dass einige Probleme mit den serverseitigen Einstellungen bestehen. Ein rotes Symbol mit einem X weist darauf hin, dass 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) • Symbol für Citrix-Verbindungen • Akkusymbol – Klicken Sie zum Öffnen der Energieverwaltung mit der rechten Maustaste auf dieses Symbol und wählen Sie Energieeinstellungen anpassen.

Symbol		Beschreibung
(7)	Datum und Uhrzeit	Zeigt aktuelle Datums- und Uhrzeitangaben an und öffnet Datums- und Uhrzeiteinstellungen.
(8)	Ein/Aus-Taste	Zum Abmelden, Neustarten oder Herunterfahren des Thin Clients.

Connection Manager (nur ThinPro)

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



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

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

- [„Verbindungskonfiguration“ auf Seite 9](#)
- [„Verbindungstypen“ auf Seite 11](#)

3 Verbindungskonfiguration

Erweiterte Verbindungseinstellungen

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




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

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

Option	Beschreibung
	HINWEIS: Diese Option speichert den Benutzernamen und die Domäne, das Kennwort muss jedoch jedes Mal erneut eingegeben werden.

Kioskmodus

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


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

Der einfachste Weg, einen Thin Client für den Kioskmodus zu konfigurieren, ist, ihn auf Smart Zero umzuschalten (siehe [Anpassungscenter auf Seite 58](#)) und eine Verbindung zu konfigurieren. Wenn dies erfolgt ist, werden die folgenden Einstellungen automatisch festgelegt:

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

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

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

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

4 Verbindungstypen

Citrix

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

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

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

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

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

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

Citrix – Allgemeine Einstellungen



HINWEIS: Diese Einstellungen haben Auswirkungen auf alle Citrix Verbindungen.

Optionen

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

Option	Beschreibung
HDX MediaStream aktivieren	Aktiviert HDX MediaStream.
MultiMedia aktivieren	Aktiviert Multimedia.

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

Lokale Ressourcen

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

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

Fenster

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

Option	Beschreibung
TWI-Modus	Ermöglicht die Anzeige eines einzigen nahtlosen Fensters auf dem lokalen ThinPro-Desktop, als ob es eine systemeigene Anwendung wäre.
Standardfenstergröße	Wenn TWI-Modus auf Nahtlos erzwingen - Aus eingestellt ist, wird damit die Standardfenstergröße gesteuert.

Option	Beschreibung
Standard-Fensterfarben	Legt die Standard-Farbtiefe fest.
Linker Monitor	Wenn Virtuellen Desktop auf allen Monitoren anzeigen deaktiviert ist, können Sie mit diesen Feldern angeben, wie der virtuelle Desktop auf bestimmten Monitoren angezeigt wird.
Rechter Monitor	
Oberer Monitor	
Unterer Monitor	

Firewall

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

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

Tastenkombinationen

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

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

Option	Beschreibung
	<ul style="list-style-type: none"> Direkt – Tastenkombinationen gelten für den Remotedesktop (Server) für nahtlose und nicht nahtlose ICA-Sitzungen, wenn ihre Fenster den Tastaturfokus haben.
Verwendung von Direktaufruftasten stoppen	Gibt die Tastenkombination an, die die direkte Verarbeitung der Tastenkombinationen deaktiviert.
Alt + F1 ... Alt + F12	Zum Hinzufügen von zu verarbeitenden Tastenkombinationen.

Sitzung

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

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



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

Verbindung

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

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

Option	Beschreibung
	<p>HINWEIS: Authentifizierungsoptionen werden nach dieser Option angezeigt und hängen vom ausgewählten Verbindungsmodus ab. Weitere Informationen finden Sie in der Citrix Dokumentation.</p> <p>HINWEIS: Sie können die Verbindungseinstellungen testen, indem Sie die Schaltfläche Verbindung testen auswählen.</p>
URL	<p>Der Citrix Server-Hostname oder die IP-Adresse. Wenn Sie eine Verbindung zu einem Server auf einer HTTPS-Website konfigurieren, geben Sie den FQDN des Standorts und das lokale Stammzertifikat im Citrix Zertifikatsspeicher ein.</p> <p>Ist das Kontrollkästchen neben dieser Option aktiviert, wird eine HTTPS-Verbindung erzwungen.</p>
Zertifikat ignorieren	Umgeht die Überprüfung des Zertifikats des Citrix Servers.
Anmeldeinformationen	<p>Legt den Authentifizierungscode auf eine der folgenden Optionen fest:</p> <ul style="list-style-type: none"> • Anonyme Anmeldung: Für StoreFront Server, die nicht authentifizierte (anonyme) Benutzer zulassen. • Anmeldeinformationen zum einmaligen Anmelden verwenden: Die bei der Anmeldung verwendeten Anmeldeinformationen werden auch zum Herstellen der Verbindung verwendet. • Bei jedem Verbindungsbeginn Anmeldeinformationen abfragen: Es werden keinerlei Anmeldeinformationen vorab bereitgestellt. • Vordefinierte Angaben zu Benutzer, Kennwort und/oder Domäne verwenden: Einige oder alle der Anmeldeinformationen werden gespeichert und für die Verbindung bereitgestellt. • Vordefinierte Smart Card verwenden: Für die Nutzung der Verbindung ist die Verwendung einer Smart Card zur Authentifizierung vorgesehen.
Benutzer	Der Benutzername für diese Verbindung.
Kennwort	Das Kennwort für diese Verbindung.
Domäne	Der Domänenname für diese Verbindung (optional).
Verbindung testen	Zum Überprüfen der URL und Anmeldeinformationen.

Konfiguration

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

Option	Beschreibung
Anwendungen bei Anmeldung automatisch erneut verbinden	<p>Wenn diese Option ausgewählt ist, werden Ressourcen, die geöffnet waren, als sich der Benutzer zuletzt abgemeldet hat, wieder geöffnet, wenn er sich erneut anmeldet.</p> <p>TIPP: Wenn Sie die Citrix SmoothRoaming-Funktion nicht verwenden, deaktivieren Sie diese Option, um Ihre Verbindungsgeschwindigkeit zu erhöhen.</p>
Modus für automatisches Starten	<p>Zum Festlegen einer bestimmten Anwendung oder eines Desktops, die bzw. der mit Beginn der Citrix Verbindung automatisch gestartet wird. Wenn die Option auf Eine Ressource automatisch starten festgelegt ist und nur eine veröffentlichte Ressource vorhanden ist, wird diese Ressource automatisch gestartet.</p> <p>HINWEIS: Diese Option hat keine Auswirkungen, wenn Anwendungen bei Anmeldung automatisch erneut verbinden ausgewählt ist und entsprechende Anwendungen vorhanden sind.</p>

Option	Beschreibung
	Wenn Sie das automatische Starten einer Anwendung oder eines Desktops ausgewählt haben, wählen Sie die Schaltfläche Enumeration , um eine Liste der Ressourcen (Anwendungen oder Desktops) abzurufen und in Citrix Connection Manager anzuzeigen. So können Sie die Ressourcen auswählen, die beim Herstellen einer Verbindung automatisch gestartet werden.
	Wenn Sie das automatische Starten einer Ressource ausgewählt haben, wählen Sie die Schaltfläche Enumeration , um die Anzahl der Ressourcen abzurufen. Wenn nur eine Ressource vorhanden ist, wird sie beim Herstellen der Verbindung automatisch gestartet.
Ressourcen auf Desktop anzeigen	Wenn diese Option ausgewählt ist, werden Remoteressourcen der Verbindung auf dem lokalen ThinPro-Desktop angezeigt.
Ressourcen in der Taskleiste anzeigen	Wenn diese Option ausgewählt ist, werden Remoteressourcen der Verbindung auf der lokalen ThinPro-Taskleiste angezeigt.
Nur abonnierte Ressourcen anzeigen	Wenn diese Option ausgewählt ist, werden während einer Citrix Verbindung nur abonnierte Ressourcen angezeigt.

Erweitert



HINWEIS: Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Erweitert“ verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 9](#).

RDP

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

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

RDP – Allgemeine Einstellungen

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



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

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

RDP – Einstellungen pro Verbindung



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

Netzwerk

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

Option	Beschreibung
Verbindungsname	Ein benutzerdefinierter Name für diese Verbindung.
Servename/-adresse	Die IP-Adresse oder der Servename 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 <code>https://</code> beginnen. Standardmäßig wird dies automatisch hinzugefügt, gemäß den Angaben im Registrierungsschlüssel <code>rdWebFeedUrlPattern</code> , der das Muster der URL definiert.
Anmeldeinformationen	<ul style="list-style-type: none">• Anmeldeinformationen zum einmaligen Anmelden verwenden: Die bei der Anmeldung verwendeten Anmeldeinformationen werden auch zum Herstellen der Verbindung verwendet.• Bei jedem Verbindungsbeginn Anmeldeinformationen abfragen: Es werden keinerlei Anmeldeinformationen vorab bereitgestellt.• Vordefinierte Angaben zu Benutzer, Kennwort und/oder Domäne verwenden: Einige oder alle der Anmeldeinformationen werden gespeichert und für die Verbindung bereitgestellt.• Vordefinierte Smart Card verwenden: Für die Nutzung der Verbindung ist die Verwendung einer Smart Card zur Authentifizierung vorgesehen.
Benutzer	Der Benutzername für diese Verbindung.
Kennwort	Das Kennwort für diese Verbindung.
Domäne	Der Domänenname für diese Verbindung (optional).
RD Gateway verwenden	Ermöglicht zusätzliche RD-Gateway-Optionen, wie Gateway-Adresse, -Port und -Anmeldeinformationen).
Servertest	Startet den Servertest, der verwendet werden kann, um festzustellen, welche RDP-Funktionen von Ihrem RDP-Server unterstützt werden.

Dienst

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

Option	Beschreibung
Dienst	Legt den RDP-Dienst auf eine der folgenden Optionen fest: <ul style="list-style-type: none">• 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:<ul style="list-style-type: none">• Wenn Modus auf Remoteanwendung festgelegt ist, ist im Feld Anwendung der Pfad der auszuführenden Anwendung angegeben.

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

Fenster

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

Option	Beschreibung
Fensterdekoration ausblenden	Mit dieser Einstellung wird sichergestellt, dass Bildelemente, wie z. B. die Menüleiste, die Minimierungs- und Schließ-Optionen sowie die Ränder von Fensterbereichen nicht angezeigt werden.
Fenstergröße	Legt die Fenstergröße auf voll , fest oder prozentual fest.
Größe (Prozent)	Wenn Fenstergröße auf 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.
Feste Größe	Wenn Fenstergröße auf fest eingestellt ist, legt diese Option die Breite und Höhe, die das Desktopfenster einnimmt, in Pixeln fest.

Optionen

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

Option	Beschreibung
Bewegungsereignisse aktivieren	Wenn aktiviert, werden die Mausbewegungen beständig an den RDP-Server übermittelt.
Datenkomprimierung aktivieren	Ermöglicht die Massenkompimierung von Daten zwischen dem RDP-Server und dem RDP-Client.
Veraltete RPD-Verschlüsselung aktivieren	Aktiviert die RDP-Verschlüsselung der letzten Generation, wenn NLA nicht verfügbar ist.
Nicht sichtbaren Cache aktivieren	Wenn aktiviert, wird der Offscreen-Speicher verwendet, um Bitmaps zu cachen.
An Administratorkonsole anheften	Fügt die Verbindung zum Administrator-Konsolenanschluss hinzu.
Sitzungsübergreifendes Kopieren/Einfügen	Wenn aktiviert, ist das Kopieren und Einfügen zwischen verschiedenen RDP-Sitzungen möglich.
Pufferung von RDP6-Grundtypen aktivieren	Wenn diese Option aktiviert ist, wird die Nicht-RemoteFX-Grafikleistung über weniger häufige Bildschirmaktualisierungen erhöht.
Progressive RemoteFX Codec aktivieren	Aktiviert den progressiven RemoteFX-Codec, mit dem der Desktop in einer Reihe immer schärferer Bilder übertragen wird. HINWEIS: Dieser Codec kann auf Desktops mit sehr dynamischem Inhalt zu visuellen Artefakten führen. Er kann also bei Bedarf deaktiviert werden.
Richtlinie zur Zertifikatsüberprüfung	Führen Sie eine der folgenden Aktionen aus: <ul style="list-style-type: none">• Alle RDP-Serverzertifikate akzeptieren• Gespeicherte Hosts verwenden; Bei unbekannten oder ungültigen Zertifikaten warnen• Gespeicherte Hosts überspringen; Bei unbekannten oder ungültigen Zertifikaten warnen• Nur mit vorab genehmigten RDP-Servern verbinden
TLS-Version	Legt die Transport Layer Security-Version fest, die in den Anfangsphasen der Aushandlung mit dem RDP-Server verwendet wird. Legen Sie diese Option auf die TLS-Version Ihres RDP-Servers fest oder verwenden Sie auto . HINWEIS: Durch einige Serverfehler auf einigen ungepatchten RDP-Servern kann die automatische Einstellung zu einem Fehler führen, deshalb ist es nicht die Standardeinstellung.
Zu sendender Hostname	Normalerweise wird der Thin Client-Hostname für Client-Zugriffslizenzen verwendet. Dieses Feld erlaubt das Senden eines anderen Werts. TIPP: Wählen Sie das Symbol ? neben dieser Option, um weitere Informationen zu erhalten.
Lastenausgleichsinfo	Verwenden Sie diese Option mit einer vermittelten RDP-Verbindung. TIPP: Wählen Sie das Symbol ? neben dieser Option, um weitere Informationen zu erhalten.



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

Lokale Ressourcen

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



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

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

Darstellung

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

Option	Beschreibung
Auswahl der Verbindungsgeschwindigkeit zur Optimierung der Leistung	<p>Das Auswählen einer Verbindungsgeschwindigkeit (LAN, Breitband oder Modem) wird die folgenden Optionen aktivieren oder deaktivieren, um die Leistung zu optimieren:</p> <ul style="list-style-type: none">• Desktop-Hintergrund• Schriftglättung• Desktopgestaltung• Inhalte des Fensters beim Verschieben anzeigen• Menü- und Fensteranimation• Designs <p>Die Auswahl von Vom Client bevorzugte Einstellungen ermöglicht dem RDP-Client die Auswahl der Optionen, die zur besten RDP-Erfahrung führen.</p> <p>Sie können auch Ihre eigene benutzerdefinierte Kombination von Optionen auswählen.</p>
Ende-zu-Ende Verbindungs-Health-Überwachung	<p>Dient zum Aktivieren der Timeout-Options.</p> <p>HINWEIS: Weitere Informationen finden Sie im HP ThinPro-Whitepaper <i>RDP Connection Drop Detection</i> (nur auf Englisch verfügbar).</p>

Option	Beschreibung
Zeitlimit bei Warnung	<p>Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, bevor der Benutzer eine Warnung zur abgebrochenen Verbindung erhält. Diese Funktion kann deaktiviert werden, indem Sie die Option löschen oder die Zeit auf Null setzen.</p> <p>Wenn die Option Dialogfeld mit Warnung anzeigen ausgewählt ist, wird ein Warnungsdialogfeld angezeigt, wenn dieses Zeitlimit erreicht ist. Andernfalls wird die Warnung nur in das Verbindungsprotokoll geschrieben.</p> <p>TIPP: HP empfiehlt, den Wert des Zeitlimits für Netzwerke, die regelmäßig hoch belastet oder zeitweise überlastet sind bzw. ausfallen, zu erhöhen.</p>
Zeitlimit bei Wiederherstellung	<p>Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, die der RDP-Client auf die Wiederherstellung der Verbindung wartet, bevor eine bestimmte Maßnahme eingeleitet wird. Am Ende dieser Frist versucht der RDP-Client kurz, erneut eine Verbindung mit der Sitzung aufzubauen.</p>
Zeitlimit bei Fehler	<p>Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, die der RDP-Client wartet, bevor er aufhört zu versuchen, die Verbindung mit diesem Server wiederherzustellen.</p> <p>TIPP: Wählen Sie das Symbol ? neben diesem Feld, um weitere Informationen zu erhalten.</p>

Diagnose

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

Option	Beschreibung
RDP-Dashboard anzeigen	<p>Wenn diese Option aktiviert ist, wird das RDP-Dashboard während der Verbindung angezeigt.</p> <p>TIPP: Wählen Sie das Symbol ? neben dieser Option, um weitere Informationen zu erhalten.</p>
Diagramm zum Verbindungszustand anzeigen	<p>Wenn diese Option aktiviert ist, wird ein zweidimensionales Diagramm der Antwortzeit vom RDP-Server angezeigt, wenn die Verbindung gestartet wird.</p> <p>TIPP: Wählen Sie das Symbol ? neben dieser Option, um weitere Informationen zu erhalten.</p>
Analyse der USB-Umleitungen	<p>Diese Funktion bestimmt und zeigt die aktuelle Umleitungsmethode für jedes umgeleitete USB-Gerät.</p> <p>TIPP: Wählen Sie das Symbol ? neben dieser Option, um weitere Informationen zu erhalten.</p>
Synchrones X11	Erzwingt das häufige Übertragen von X11-Puffern zulasten der Leistung.
Protokollierung	Aktiviert die X11-Protokolldatei. Wählen Sie die Option Automatische Leerung , um die Häufigkeit von Protokollausgaben zulasten der Leistung zu erhöhen.
Aufzeichnen	Ermöglicht die Aufzeichnung und Wiedergabe von X11-Ausgaben einer Sitzung.

Erweitert



HINWEIS: Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Erweitert“ verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 9](#).

RemoteFX

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

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



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

RDP-Sitzungen mit mehreren Monitoren

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

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

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



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



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

RDP-Multimedia-Umleitung

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

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

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

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

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

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

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

RDP-Geräteumleitung

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

RDP-USB-Umleitung

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

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

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

- Der Server muss die USB-Umleitung unterstützen, um für den Thin Client verfügbar zu sein. Die USB-Umleitung für allgemeine Zwecke wird bei RDVH-Servern mit RemoteFX, Windows 8, Windows 10, Windows Server 2012 und Windows Server 2016 unterstützt.
- Das Protokoll im USB-Manager in der Systemsteuerung muss auf RDP festgelegt werden.
- Für RDP-Verbindungen bestimmen die Steuerelemente im USB-Manager, ob ein USB-Gerät umgeleitet wird. Die Einstellungen für die einzelnen Verbindung bestimmen, wie ein USB-Gerät umgeleitet wird.

RDP-Massenspeicherumleitung

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

Es gibt drei Einschränkungen für diese Art von Umleitung.

- Das Gerät wird nicht in der Taskleiste auf dem Remote-Host mit einem Symbol zum Auswerfen angezeigt. Aus diesem Grund müssen Sie dem Gerät nach einer Kopie genügend Zeit zur Datensynchronisation geben, bevor Sie das Gerät entfernen, um sicherzustellen, dass das Gerät nicht beschädigt wird. In der Regel dauert dies weniger als eine Sekunde nachdem der Dialog Datei kopieren

beendet ist, aber es können bis zu 10 Sekunden erforderlich sein, je nach der Schreibgeschwindigkeit des Geräts und der Netzwerklatenz.

- Nur vom Thin Client unterstützte Dateisysteme werden bereitgestellt. Die unterstützten Dateisysteme sind FAT32, NTFS, ISO9660 (CD-ROMs), UDF (DVD-ROMs) und ext3.
- Das Gerät wird als Verzeichnis behandelt. Häufige Laufwerksaufgaben wie die Formatierung und die Änderung der Festplattenbezeichnung stehen nicht zur Verfügung.

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

Registrierungseintrag	Einzurichtender Wert	Beschreibung
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`.

RDP-Druckerumleitung

Standardmäßig hat RDP zwei Methoden der Druckerumleitung aktiviert:

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

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



HINWEIS: Weitere Informationen finden Sie unter [Konfiguration eines seriellen oder parallelen Druckers auf Seite 79](#).

RDP-Audioumleitung

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-Lautstärkeinstellungen haben Auswirkungen auf die endgültige Lautstärke. HP empfiehlt, die lokale Lautstärke auf das Maximum einzustellen und die Lautstärke innerhalb des Remote-Host anzupassen.

RDP-Smart Card-Umleitung

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

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

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

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

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



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

VMware Horizon View

VMware Horizon View – Einstellungen pro Verbindung



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

Netzwerk

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

Option	Beschreibung
Name	Eingabe des Namens für diese Verbindung.
Adresse	Den Hostnamen oder die IP-Adresse des VMware Horizon View-Servers eingeben.
Anmeldeinformationen	<ul style="list-style-type: none">• Anonym anmelden mit nicht authentifiziertem Zugriff• Anmeldeinformationen zum einmaligen Anmelden verwenden: Die bei der Anmeldung verwendeten Anmeldeinformationen werden auch zum Herstellen der Verbindung verwendet.• Bei jedem Verbindungsbeginn Anmeldeinformationen abfragen: Es werden keinerlei Anmeldeinformationen vorab bereitgestellt.• Vordefinierte Angaben zu Benutzer, Kennwort und/oder Domäne verwenden: Einige oder alle der Anmeldeinformationen werden gespeichert und für die Verbindung bereitgestellt.• Vordefinierte Smart Card verwenden: Für die Nutzung der Verbindung ist die Verwendung einer Smart Card zur Authentifizierung vorgesehen.
Benutzer	Den für die Verbindung zu verwendenden Benutzernamen eingeben.
Kennwort	Das für die Verbindung zu verwendende Kennwort eingeben.
Domäne	Die für die Verbindung zu verwendende Domäne eingeben.

Allgemein

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

Option	Beschreibung
Automatische Anmeldung	Wenn aktiviert, wird der Benutzer automatisch angemeldet, wenn die Verbindung hergestellt ist. HINWEIS: HP empfiehlt das Aktivieren dieser Option.
Smart Card-Anmeldung zulassen	Aktiviert die Smart Card-Anmeldung. HINWEIS: Weitere Informationen zu Smart Cards finden Sie unter VMware Horizon View-Smart Card-Umleitung auf Seite 33 .
Anwendung nicht maximiert starten	Wenn aktiviert, starten Anwendungen nicht maximiert in Windows.
Bevorzugtes Protokoll	Ermöglicht die Auswahl von PCoIP, RDP oder BLAST als bevorzugtes Protokoll. Sie können das Protokoll aber auch später auswählen.
Anwendungsgröße	Legt die Fenstergröße der Anwendung fest. Sie können Alle Monitore , Vollbild , Großes Fenster oder Kleines Fenster auswählen.
Desktopgröße	Legt die Fenstergröße des Desktops fest. Sie können Alle Monitore , Vollbild , Großes Fenster oder Kleines Fenster auswählen.

Sicherheit

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

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

RDP-Optionen

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

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

Option	Beschreibung
	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.
Freigegebene Ordner	Hinzufügen, Entfernen oder Bearbeiten freigegebener Ordner.

RDP-Darstellung

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

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

Erweitert



HINWEIS: Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Erweitert“ verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 9](#).

VMware Horizon View-Sitzungen mit mehreren Monitoren

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


VMware Horizon View-Tastenkombinationen

Windows Tastenkombinationen

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

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

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

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

Medientasten

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

VMware Horizon View-Multimedia-Umleitung

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

Weitere Informationen hierzu finden Sie unter [RDP-Multimedia-Umleitung auf Seite 22](#).

VMware Horizon View-Geräteumleitung

VMware Horizon View-USB-Umleitung

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

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

VMware Horizon View-Massenspeicherumleitung

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

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

- ▲ Fügen Sie in der Option Befehlszeilenargumente – `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 [RDP-Massenspeicherumleitung auf Seite 23](#).

VMware Horizon View-Druckerumleitung

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

VMware Horizon View-Audioumleitung

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

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

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



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

- Wenn Sie ein USB-Headset mit einem Mikrofon haben, können Sie 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 „Geräte“ zur Umleitung ausgewählt 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.

VMware Horizon View-Smart Card-Umleitung

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

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

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

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



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



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



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

VMware Horizon View-Webcam-Umleitung

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

Ändern des VMware Horizon View-Protokolls

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

So ändern Sie das Protokoll:

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



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



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

Anforderungen für die VMware Horizon View HTTPS- und Zertifikatverwaltung

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

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

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

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

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

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

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

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

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

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

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

Web Browser

Web Browser – Allgemeine Einstellungen

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



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

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

Web Browser – Einstellungen pro Verbindung



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

Konfiguration

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

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

Erweitert



HINWEIS: Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Erweitert“ verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 9](#).

Zusätzliche Verbindungstypen (nur ThinPro)



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

TeemTalk



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

Weitere Informationen zu HP TeemTalk finden Sie im *Benutzerhandbuch* für HP TeemTalk.

Konfiguration

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

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

TeemTalk Sitzungsassistent

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

Option	Beschreibung
Sitzungsname	Der Name der Sitzung.
Transport	Der Netzwerktransport, der für die Verbindung verwendet werden soll. Gültige Transportoptionen sind: TCP/IP , Seriell , SSH2 und SSL .
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 .

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

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

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

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

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

Option	Beschreibung
Konfigurationsleiste anzeigen	Zeigt die Konfigurationsleiste an.
Aktuelle Fensterposition speichern	Speichert die aktuelle Größe und Position des Fensters, wenn Sie Einstellungen speichern auswählen. Das Fenster wird beim nächsten Systemstart wiederhergestellt.

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

Erweitert



HINWEIS: Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Erweitert“ verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 9](#).

XDMCP



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

Konfiguration

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

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

Erweitert



HINWEIS: Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Erweitert“ verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 9](#).

SSH



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

Konfiguration

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

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

Erweitert



HINWEIS: Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Erweitert“ verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 9](#).

Telnet



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

Konfiguration

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

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

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

Erweitert



HINWEIS: Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Erweitert“ verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 9](#).

Custom

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



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

Konfiguration

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

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

Erweitert



HINWEIS: Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Erweitert“ verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 9](#).

5 HP True Graphics

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

Anforderungen auf Server-Seite

Die folgende Tabelle enthält eine Liste der vom Server unterstützten Produkte des Independent Software Vendor (ISV), die Sie für Ihre virtuelle Desktop-Infrastruktur (VDI) verwenden.

ISV	Unterstützte Produkte
Citrix®	XenApp®/XenDesktop® 7.0 oder höher WICHTIG: Der Citrix Server muss das Senden von Sitzungsdaten im H.264-Format unterstützen (eine Citrix Technologie, die als SuperCodec bezeichnet wird). H.264 ist standardmäßig aktiviert und wird mit dem DeepCompressionV2-Encoder verarbeitet, einem CPU-basierten Komprimierungsalgorithmus.
VMware®	VMware Horizon™ 6.0 und höher VMware Horizon View™ 5.2 und 5.3 VMware View® 5.1

Anforderungen auf Client-Seite

Die folgende Tabelle enthält eine Liste der unterstützten Thin Client-Betriebssysteme sowie der vom Client unterstützten Software des ISP, die Sie für Ihre VDI verwenden.

Unterstützte Betriebssysteme	Unterstützte Citrix Clients	Unterstützte VMware Clients
HP ThinPro 5.0 und höher	Citrix Receiver 13.1.1 und höher HINWEIS: Eine Version von Citrix Receiver, die HP True Graphics unterstützt, ist ab HP ThinPro 5.2 vorinstalliert und als Add-on für HP ThinPro 5.0 und 5.1 erhältlich.	VMware Horizon Client 4.0 und höher (unter Verwendung des Blast-Protokolls)

Konfiguration auf Client-Seite



HINWEIS: Die Informationen in diesem Abschnitt gelten nur für Citrix. Bei VMware können Sie HP True Graphics ganz einfach mit dem Blast-Protokoll aktivieren.

Komprimierungseinstellungen

So aktivieren Sie HP True Graphics auf HP ThinPro:

- ▲ Wählen Sie die allgemeine Einstellung **H264-Komprimierung** für Citrix Verbindungen.



HINWEIS: 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

So erzwingen Sie, dass Remote-Anwendungen im Fenstermodus ausgeführt werden:

- ▲ Legen Sie die allgemeine Einstellung **TWI-Modus** für Citrix Verbindungen auf **Nahtlos erzwingen - Aus** fest.

Monitorlayout- und Hardwarebeschränkungen

Beachten Sie die folgenden Beschränkungen für das Monitorlayout:

- Die meisten Konfigurationen mit maximal zwei Monitoren mit einer Auflösung von jeweils 1920 × 1200 werden unterstützt.
- HP t420 Thin Client: Durch die Standard-BIOS-Konfiguration verwendet dieses Modell HP True Graphics standardmäßig nur für einen Monitor. Weitere Informationen finden Sie unter [Aktivieren von HP True Graphics für mehrere Monitore auf dem HP t420 auf Seite 43](#).
- HP t630 Thin Client: Dieses Modell unterstützt maximal zwei Monitore mit einer Auflösung von 1920 × 1200 oder einen Monitor mit einer Auflösung von 3840 × 2160.
- HP t730 Thin Client: Dieses Modell unterstützt maximal drei Monitore mit einer Auflösung von 1920 × 1200.
- Gedrehte Monitore werden möglicherweise nicht korrekt angezeigt.
- Wenn Sie HP True Graphics mit zwei Monitoren verwenden und versuchen, ein Video mit HDX MediaStream wiederzugeben, kann das Video nicht wiedergegeben werden, weil H.264 nur zwei Sitzungen für die Hardware-Decodierung unterstützt, die bereits von den Monitoren genutzt werden.



HINWEIS: Des Weiteren versucht HDX MediaStream, eine lokale Hardware-Decodierung für H.264 zu verwenden, was dann den Fehler verursacht.

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. Wählen Sie **Erweitert ► Integrierte Grafiken**.
3. Legen Sie **Integrierte Grafiken** auf **Erzwingen** fest.
4. Legen Sie **Größe des UMA-Frame-Puffers** auf **512 MB** 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.

Tipps und bewährte Vorgehensweisen

Beachten Sie bei der Verwendung von HP True Graphics folgende Hinweise:

- Verwenden Sie nach dem Herstellen einer Verbindung mit einem Remote-Desktop den Citrix HDX Monitor, um zu bestimmen, welcher Encoder für die Sitzung verwendet wird. Prüfen Sie dazu den Wert für **Component_Encoder** unter **Grafik > Thinwire erweitert**. 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 die Leistung wird durch HP True Graphics nicht verbessert.
-
- HP True Graphics kann möglicherweise Vorteile für ältere Versionen von XenDesktop bringen, wenn HDX 3D Pro verwendet wird. Es sind keine Vorteile zu erkennen, wenn HDX 3D Pro verwendet wird und die visuelle Qualität auf **Immer verlustfrei** festgelegt ist, da dann die grafischen Informationen nicht im Format H.264 an den Thin Client gesendet werden.

6 Active Directory Integration

Durch die Verwendung Active Directory Integration können Sie Benutzer zwingen, sich beim Thin Client mithilfe von Domänenanmeldeinformationen anzumelden. Optional können diese Anmeldeinformationen verschlüsselt und gespeichert werden, um sie später zum Herstellen von Remote-Verbindungen bereitzustellen. Dieses Verfahren wird als „Single Sign-on“ oder „Einmaliges Anmelden“ bezeichnet.



HINWEIS: Für die Aktivierung der Authentifizierung sind keine speziellen Domänenberechtigungen erforderlich.

Es gibt zwei Modi für die Nutzung der Active Directory Integration. Indem einfach die Authentifizierung mit der Domäne aktiviert wird, können Domänenanmeldeinformationen für die folgenden Vorgänge verwendet werden:

- Anmelden am Thin Client
- Herstellen einer Verbindung mithilfe der Funktion zum einmaligen Anmelden
- Wechseln in den Administratormodus mithilfe von Administratoranmeldeinformationen
- Entsperren eines gesperrten Bildschirms mithilfe der Anmeldeinformationen
- Außerkraftsetzen eines gesperrten Bildschirms mithilfe von Administratoranmeldeinformationen

Der Thin Client kann auch formell zur Domäne hinzugefügt werden. Damit wird der Thin Client zur Domänen Datenbank hinzugefügt und möglicherweise dynamisches DNS aktiviert, sodass der Thin Client den DNS-Server informiert, wenn sich seine IP-Adresse-/Hostnamenzuordnung ändert. Anders als bei der Domänenauthentifizierung müssen für einen formellen Beitritt die Anmeldeinformationen eines Domänenbenutzers eingegeben werden, der autorisiert ist, Clients zur Domäne hinzuzufügen. Der Domänenbeitritt ist optional. Abgesehen vom dynamischen DNS sind alle Domänenfunktionen ohne einen Beitritt verfügbar.

Anmeldebildschirm

Wenn die Domänenauthentifizierung aktiviert ist, zeigt ThinPro beim Start einen Domänenanmeldebildschirm an. Domänenanmeldebildschirm umfasst auch Optionen, die möglicherweise vor dem Anmelden konfiguriert werden müssen.

Das Layout des Desktop-Hintergrunds, der Stil des Anmeldedialogfelds, der Text des Anmeldedialogs und die verfügbaren Schaltflächen können mithilfe der Registrierungseinstellungen und/oder Konfigurationsdateieinstellungen angepasst werden. Weitere Informationen finden Sie im HP ThinPro-Whitepaper *Login Screen Customization* (nur auf Englisch verfügbar).

Wenn das System erkennt, dass der Benutzer versucht hat, sich mit abgelaufenen Anmeldeinformationen anzumelden, wird er dazu aufgefordert, seine Anmeldeinformationen zu aktualisieren.

Einmaliges Anmelden

Nachdem sich ein Domänenbenutzer angemeldet hat, können die dabei verwendeten Anmeldeinformationen auch beim Herstellen sämtlicher dafür konfigurierter Verbindungen präsentiert werden. Dies ermöglicht es dem Benutzer, sich am Thin Client anzumelden und Citrix-, VMware Horizon View- und RDP-Sitzungen zu starten, ohne sich erneut anmelden zu müssen, solange er am Thin Client angemeldet bleibt.

Desktop

Sobald sich der Benutzer mit seinen Domänenanmeldeinformationen angemeldet hat, wird in der Taskleiste ein Active Directory Symbol angezeigt. Der Benutzer kann auf das Symbol klicken, um Folgendes zu tun:

- Anzeigen, wer am System angemeldet ist
- Sperren des Bildschirms
- Ändern des Domänenkennworts

Bildschirmsperre

Der Bildschirm kann aufgrund der Überschreitung eines Inaktivitätszeitlimits oder durch eine manuelle Sperrung gesperrt werden. Wenn der Bildschirm durch einen Domänenbenutzer gesperrt wurde, fordert das Dialogfeld zum Entsperren den Benutzer auf, dasselbe Domänenkennwort einzugeben, das für die Anmeldung verwendet wurde. Es werden dieselben Optionen wie im Anmeldedialogfeld sowie die zusätzliche Funktion zum Entsperren des Bildschirms bereitgestellt. Wenn auf die Schaltfläche zum Entsperren des Bildschirms geklickt wird, wird der Benutzer stattdessen zu Eingabe des Stammkennworts (Administratorkennwort) oder von Anmeldeinformationen für die Domänenadministratorgruppe aufgefordert, die während des Setups der Domänenauthentifizierung festgelegt wurde. Wenn der Benutzer Anmeldeinformationen zum Überschreiben der Bildschirmsperre eingibt, wird anschließend anstelle des Desktops der Anmeldebildschirm angezeigt.

Administratormodus

Abgesehen von der herkömmlichen Methode zur Verwendung des Stammkennworts für den Wechsel in den Administratormodus können dazu auch die Domänenanmeldeinformationen eines Benutzers aus der festgelegten Domänenadministratorgruppe verwendet werden.

Einstellungen und der Domänenbenutzer

Wenn ein Domänenbenutzer angemeldet ist, werden jegliche an den Einstellungen vorgenommene Änderungen in einer Registrierungsschicht gespeichert, die nur für den jeweiligen Benutzer vorgesehen ist. Dies umfasst neu hergestellte Verbindungen.

Wenn der Benutzer keine Änderungen an Systemeinstellungen oder Verbindungen vorgenommen hat, werden stattdessen die Systemstandardwerte übernommen.

Wenn das System in den Administratormodus versetzt wird, werden an der benutzerspezifischen Registrierungsschicht keine Einstellungs- und Verbindungsänderungen mehr vorgenommen. Stattdessen werden im Administratormodus alle Änderungen auf grundlegender Registrierungsebene übernommen. Auf diese Weise wird eine im Administratormodus vorgenommene Änderung an einer Einstellung für alle Benutzer übernommen, sofern nicht bereits eine benutzerspezifische und -definierte Einstellung angegeben wurde.

7 Systemsteuerung

Mit der Systemsteuerung können Sie die Systemkonfiguration ändern.



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



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

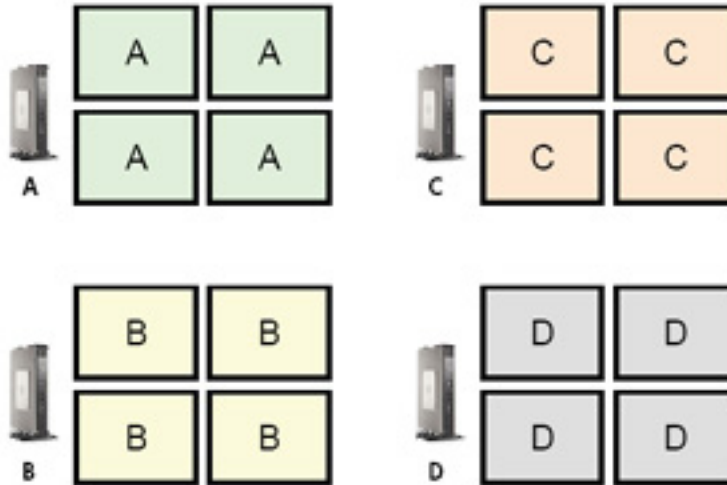
Peripheriegeräte

Menüoption	Beschreibung
Clientaggregation	<p>Zum Kombinieren von Thin Clients, um einen zusätzlichen Anzeigebereich zu erstellen.</p> <p>Weitere Informationen finden Sie unter Clientaggregation auf Seite 48.</p>
Anzeigeeinstellungen	<p>Zum Konfigurieren und Testen von Displayoptionen.</p> <p>Weitere Informationen finden Sie unter Anzeigeeinstellungen auf Seite 50.</p>
Tastaturlayout	<p>Damit können Sie das Tastaturlayout ändern, um es der Sprache der Tastatur anzupassen.</p>
Audio	<p>Zur Stufenregelung von Audio-Wiedergabe und -Eingang.</p>
Maus	<p>Zum Konfigurieren der Mausgeschwindigkeit und der Mauseingabe für Rechtshänder oder Linkshänder.</p> <p>Bei Thin Clients mit einem TouchPad können Sie über diese Menüoption auch das TouchPad deaktivieren bzw. aktivieren.</p>
Drucker	<p>Zum Einrichten von lokalen und Netzwerkdruckern. Lokale Drucker können im Netzwerk gemeinsam genutzt werden.</p> <p>Weitere Informationen finden Sie unter Konfigurieren von Druckern auf Seite 51.</p>
Touchscreen	<p>Zum Konfigurieren der Touchscreen-Optionen.</p>
USB-Manager	<p>Zum Konfigurieren der Umleitungsoptionen für USB-Geräte.</p> <p>Weitere Informationen finden Sie unter Umleiten von USB-Geräten auf Seite 51.</p>
Einrichten der SCIM-Eingabemethode	<p>Zum Konfigurieren der Smart Common Input Method (SCIM) für die Eingabe von Chinesisch, Japanisch und Koreanisch.</p> <p>Weitere Informationen zu diesem Open-Source-Programm finden Sie unter http://sourceforge.net/apps/mediawiki/scim/index.php?title=Main_Page.</p>

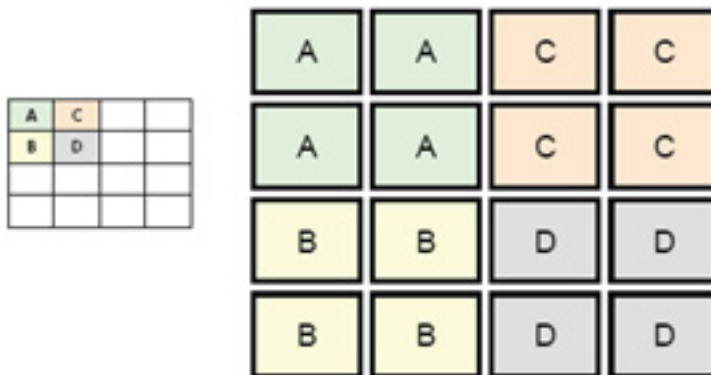
Clientaggregation

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

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

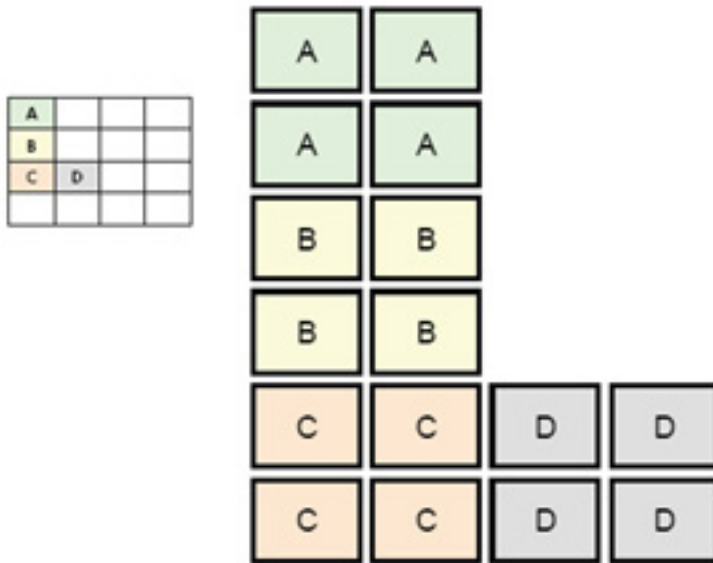


Mithilfe der Clientaggregation können Sie die vier Thin Clients in einem 4 x 4-Raster anordnen. Die folgende Abbildung zeigt eine der möglichen Anordnungen.



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

Die folgende Abbildung zeigt eine weitere mögliche Anordnung.



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



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

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

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

Konfigurieren der Clientaggregation

Die Konfiguration der Clientaggregation erfolgt in zwei Arbeitsschritten:

1. [Konfigurieren der Aggregation-Clients auf Seite 49](#)
2. [Konfigurieren des Aggregation-Servers auf Seite 50](#)

Konfigurieren der Aggregation-Clients

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

1. Wählen Sie in der Systemsteuerung **Peripheriegeräte > Clientaggregation**.
2. Wählen Sie **Client** aus.

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

Konfigurieren des Aggregation-Servers

So konfigurieren Sie den Aggregation-Server:

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

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

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

Anzeigeeinstellungen

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

So konfigurieren Sie Anzeigeprofile:

1. Wählen Sie in der Systemsteuerung **Peripheriegeräte > Anzeigeeinstellungen**.
2. Konfigurieren Sie die Optionen nach Bedarf und wählen Sie anschließend **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.

So ändern Sie bei Verwendung externer Monitore schnell die Displaykonfiguration (nur mobile Thin Clients):

- ▲ Drücken Sie **Fn + F4**.

Konfigurieren von Druckern

So konfigurieren Sie einen Drucker:

1. Wählen Sie in der Systemsteuerung **Peripheriegeräte > Drucker**.
2. Wählen Sie im Dialogfeld **Drucken** die Option **Hinzufügen**.
3. Wählen Sie im Dialogfeld **Neuer Drucker** den Drucker, den Sie konfigurieren möchten, und wählen Sie dann **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 **Allgemein (empfohlen)** und dann **Weiter**.
5. Wählen Sie das Modell und den Treiber für den Drucker und dann **Weiter**.



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

Stellen Sie bei Verwendung der Option **Allgemein (empfohlen)** sicher, dass Sie für das Modell **nur-Text (empfohlen)** auswählen, und für den Treiber **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 Treiber** eingeben. Wenn bei einer Verbindungsherstellung zu einer Remote-Sitzung kein Treiber zugeordnet werden kann, verwendet Windows möglicherweise den falschen Treiber und das Drucken funktioniert nicht. Damit der Drucker ordnungsgemäß funktioniert, muss der Treiber auch auf dem Windows Server installiert werden.

7. Wählen Sie **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 **Eigenschaften**, und ändern Sie dann Fabrikat und Modell.

Umleiten von USB-Geräten

So leiten Sie USB-Geräte um:

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

Wenn die Einstellung **Lokal** ist, können Sie auch die Optionen **Bereitstellung von Geräten erlauben** und **Geräte schreibgeschützt bereitstellen** angeben.

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

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

Setup

Menüoption	Beschreibung
Hintergrundeinstellungen	<p>Zum Konfigurieren des Hintergrunddesigns und der dynamischen Anzeige von Systeminformationen (wie Hostname, IP-Adresse, Hardwaremodell und MAC-Adresse des Thin Clients) im Hintergrund.</p> <p>Weitere Informationen finden Sie im HP ThinPro-Whitepaper <i>Login Screen Customization</i> (nur auf Englisch verfügbar).</p>
Datum und Uhrzeit	Zum Konfigurieren der Zeitzone sowie der Datums- und Uhrzeitoptionen.
Firewall-Manager	Zum Konfigurieren der Firewall-Einstellungen.
Sprache	Zum Anzeigen der HP ThinPro-Oberfläche in einer anderen Sprache.
Netzwerk	<p>Zum Konfigurieren der Netzwerkeinstellungen.</p> <p>Weitere Informationen finden Sie unter Netzwerkeinstellungen auf Seite 52.</p>
Energieverwaltung	Zum Konfigurieren von Energieverwaltungseinstellungen wie Bildschirmschoner, CPU-Einstellungen sowie Einstellungen für die Deaktivierung der Anzeige und den Wechsel in den Standbymodus.
Sicherheit	Weitere Informationen finden Sie unter Sicherheitseinstellungen auf Seite 57 .
Anpassungscenter	<p>Es stehen folgende Aktionen zur Verfügung:</p> <ul style="list-style-type: none"> • Wechseln zwischen den ThinPro- und Smart Zero-Konfigurationen • Konfigurieren der Desktop- und Taskleisten-Optionen • Auswählen der Verbindungstypen und Elemente der Systemsteuerung, auf die Endbenutzer zugreifen können <p>Weitere Informationen finden Sie unter Anpassungscenter auf Seite 58.</p>

Netzwerkeinstellungen

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

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

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

- [Einstellungen für kabelgebundene Netzwerke](#)
- [Wireless-Netzwerkeinstellungen](#)

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

Einstellungen für kabelgebundene Netzwerke

Die folgende Tabelle beschreibt die im Netzwerk-Manager auf der Registerkarte **Kabelgebunden** verfügbaren Optionen.

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

Wireless-Netzwerkeinstellungen

Über diese Registerkarte können Sie Wireless-Profile für Wireless-Netzwerke hinzufügen, bearbeiten und löschen.

In den folgenden Tabellen sind die verfügbaren Optionen beim Hinzufügen oder Bearbeiten von Wireless-Profilen beschrieben.



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



TIPP: Sie können auf diese Einstellungen auch zugreifen, indem Sie das Netzwerkstatussymbol in der Taskleiste wählen.

Wechseln Sie zur Registerkarte **Wireless**, um die allgemeinen Einstellungen zu konfigurieren.

Option	Beschreibung
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.
Wireless-Band	Wählen Sie Auto , 2,4 GHz oder 5 GHz .
SSID ausgeblendet	Aktivieren Sie diese Option, wenn die SSID des Wireless-Netzwerks auf „Ausgeblendet“ eingestellt ist (nicht übermitteln).
IPv6 aktivieren	Aktiviert das IPv6. Standardmäßig wird IPv4 verwendet und es können nicht beide gleichzeitig verwendet werden.
Energieverwaltung aktivieren	Aktiviert die Energieverwaltungsfunktion für den Wireless-Adapter.
Verbindungsmethode	<p>Zur Auswahl zwischen Automatisch und Statisch. Wenn Ihre Netzwerkumgebung DHCP verwendet wird, sollte die Option Automatisch ohne weitere Konfigurationen funktionieren.</p> <p>Wenn Statisch ausgewählt ist, werden die Einstellungen für Statische Adressenkonfiguration zur Verfügung stehen. Vergewissern Sie sich, dass Sie diese Werte dementsprechend eingeben, ob Sie IPv4 oder IPv6 verwenden.</p>
Sicherheitseinstellungen	<p>Zum Festlegen der Authentifizierungseinstellung auf eine der folgenden Optionen:</p> <ul style="list-style-type: none">• Keine• WEP• WPA/WPA2-PSK• 802.1X-TTLS• 802.1X-PEAP• 802.1X-TLS• EAP-FAST <p>Für WEP und WPA/WPA2-PSK müssen Sie nur den Netzwerkschlüssel eingeben und OK auswählen.</p> <p>Stellen Sie für EAP-FAST Anonyme Identität, Benutzername, Kennwort und Bereitstellungsmethode ein. Die Einstellungen der PAC-Datei müssen Sie nicht ändern.</p> <p>Weitere Informationen über TTLS, PEAP und TLS finden Sie unter Einstellungen für kabelgebundene Netzwerke auf Seite 53.</p>
Automatische Verbindung	Diese Option ist zur künftigen Verwendung vorgesehen.
Wireless aktivieren	Aktiviert den Wireless-Adapter.

Über die Registerkarte **IPv4** können Sie IPv4-Verbindungseinstellungen konfigurieren.

Option	Beschreibung
IPv4 aktiviert	Aktiviert das IPv4.
IPv4-Methode	<p>Zur Auswahl zwischen Automatisch und Statisch. Wenn Ihre Netzwerkumgebung DHCP verwendet wird, sollte die Option Automatisch ohne weitere Konfigurationen funktionieren.</p> <p>Wenn Statisch gewählt ist, werden die Einstellungen für die Statische Adressenkonfiguration angezeigt und Sie müssen die IPv4-Einstellungen eingeben.</p>

Über die Registerkarte **IPv6** können Sie die IPv6-Verbindungseinstellungen konfigurieren.

Option	Beschreibung
IPv6 aktiviert	<p>Ermöglicht die Nutzung einer globalen IPv6-Adresse.</p> <p>HINWEIS: HP ThinPro versucht, eine globale IPv6-Adresse über Routenankündigung oder DHCPv6 abzurufen.</p>
IPv6-Methode	<p>Zur Auswahl zwischen Automatisch und Statisch. Wenn Ihre Netzwerkumgebung DHCP verwendet wird, sollte die Option Automatisch ohne weitere Konfigurationen funktionieren.</p> <p>Wenn Statisch gewählt ist, werden die Einstellungen für die Statische Adressenkonfiguration angezeigt und Sie müssen die IPv6-Einstellungen eingeben.</p>

Über die Registerkarte **Sicherheit** können Sie die Sicherheitseinstellungen für die Verbindung konfigurieren.

Option	Beschreibung
Authentifizierung	<p>Zum Festlegen der Authentifizierungseinstellung auf eine der folgenden Optionen:</p> <ul style="list-style-type: none">• None (Keine)• WEP• WPA/WPA2-PSK• WPA/WPA2 Enterprise-TTLS• WPA/WPA2 Enterprise-PEAP• WPA/WPA2 Enterprise-TLS• EAP-FAST <p>Für WEP und WPA/WPA2-PSK müssen Sie nur den Netzwerkschlüssel eingeben und OK auswählen.</p> <p>Stellen Sie für EAP-FAST Anonyme Identität, Benutzername, Kennwort und Bereitstellungsmethode ein. Die Einstellungen der PAC-Datei müssen Sie nicht ändern.</p> <p>Weitere Informationen über TTLS, PEAP und TLS finden Sie unter Einstellungen für kabelgebundene Netzwerke auf Seite 53.</p>

DNS-Einstellungen

Die folgende Tabelle beschreibt die im Netzwerk-Manager auf der Registerkarte **DNS** verfügbaren Optionen.

Option	Beschreibung
Hostname	Dieser wird entsprechend der MAC-Adresse des Thin Client automatisch generiert. Alternativ können Sie auch einen benutzerdefinierten Hostnamen festlegen.
DNS-Server	Verwenden Sie dieses Feld, um benutzerdefinierte Informationen des DNS-Servers festzulegen.
Suchbereiche	Verwenden Sie dieses Feld, um die Domänen zu beschränken, die durchsucht werden.
HTTP-Proxy	Verwenden Sie diese Felder, um Proxy-Server-Informationen im folgenden Format einzugeben:
FTP-Proxy	<code>http://<Adresse>:<Port></code>
HTTPS-Proxy	HP empfiehlt das Präfix <code>http://</code> 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 **Allgemein**, um Informationen, Adressen und Authentifizierungsmethode für die Regel festzulegen. Die **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 **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 **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 **Gruppenname** und das **Kennwort der Gruppe** sind die IPSec-ID und das IPSec-Kennwort.
- Die Einstellung der **Domäne** ist optional.
- Der **Benutzername** und das **Benutzerkennwort** sind die Benutzeranmeldeinformationen, die Rechte zum Erstellen einer VPN-Verbindung auf der Serverseite besitzen.
- Der **Sicherheitstyp** sollte identisch eingestellt werden wie auf der Serverseite.
- Die Option **NAT-Traversal** sollte abhängig von Ihrer VPN-Umgebung festgelegt werden.

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

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

- Das **Gateway** ist die IP-Adresse oder der Hostname des Gateway.
- Die Einstellung der **NT-Domäne** ist optional.
- Der **Benutzername** und das **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>.

Sicherheitseinstellungen


Sicherheitseinstellungen können mit dem Security Manager konfiguriert werden. Wählen Sie in der Systemsteuerung **Setup > Sicherheit** aus, um den Security Manager zu öffnen.

In den folgenden Abschnitten finden Sie weitere Informationen über die verschiedenen Registerkarten im Security Manager.


- [Lokale Konten auf Seite 57](#)
- [Verschlüsselung auf Seite 57](#)
- [Optionen auf Seite 58](#)

Lokale Konten

Über die Registerkarte „Lokale Konten“ können die Kennwörter für das lokale Stamm- und Benutzerkonto geändert oder die Authentifizierung mithilfe dieser Konten deaktiviert werden.

 **ACHTUNG:** Durch die Deaktivierung der Stamm- und/oder Benutzerkonten wird das System möglicherweise in einen unbestimmten Zustand versetzt, sofern die Active Directory Authentifizierung nicht aktiviert ist. Wenn beispielsweise das Stammkonto deaktiviert ist, können Sie nur unter Verwendung von Domänenanmeldeinformationen eines Administrators in den Administratormodus wechseln. Allerdings kann durch Deaktivierung der lokalen Konten die Sicherheit erhöht werden, wenn die Active Directory Authentifizierung aktiviert ist, da Sie dann keine gemeinsamen geheimen Schlüssel wie das Stammkennwort des Thin Clients verwalten und aktualisieren müssen.

Wenn die Active Directory Authentifizierung verwendet wurde und sich auf dem Thin Client zwischengespeicherte Daten für Domänenbenutzer befinden, können Sie über diese Registerkarte auch die zwischengespeicherten Daten des betreffenden Benutzers löschen.

 **HINWEIS:** Wenn sich der Benutzer mit den Anmeldeinformationen für ein Domänenkonto angemeldet hat, kann er die Daten seines eigenen Kontos nicht löschen, da das System dadurch in einen unbestimmten Zustand versetzt würde.

Verschlüsselung

Active Directory Anmeldeinformationen und andere geheime Schlüssel können für Funktionen wie das Entsperren des Bildschirms zwischengespeichert und/oder zum einmaligen Anmelden auf dem System verschlüsselt und gespeichert werden.

Über dieses Menü kann der Hash-Algorithmus zum Erstellen des Hashs für ein Kennwort ausgewählt werden. Die Standardfunktion Scrypt ist eine anerkannte Schlüsselableitungsfunktion. Außerdem ist die Schlüsselableitungsfunktion Argon2 verfügbar sowie die herkömmlichen Hashes SHA-256 und SHA-512. Der Vorteil einer Schlüsselableitungsfunktion ist, dass der Aufwand zur Berechnung einer Rainbow Table für den Abgleich von unverschlüsselten Kennwörtern mit vorberechneten Hash-Werten hoch ist, wohingegen herkömmliche Hashes auf eine möglichst schnelle Ausführung abzielen. Alle Hashes, die mit mindestens 128 Bit zufällig gewählter Zeichenfolgen („Salt“) gespeichert werden, ändern sich jedes Mal, wenn der Kennwort-Hash berechnet und gespeichert wird.

Verschlüsselte Kennwörter werden in Fällen verwendet, in denen sie zurückgesetzt und zum Herstellen von Verbindungen bereitgestellt werden können (einmaliges Anmelden). Der Verschlüsselungsalgorithmus kann hier aus einer Vielzahl von Algorithmen ausgewählt werden, die von OpenSSL unterstützt werden. Sofern es keinen wichtigen Grund für die Auswahl eines anderen Werts gibt, empfiehlt HP die Verwendung des standardmäßigen Verschlüsselungsalgorithmus, der von Sicherheitsexperten allgemein als moderner und sicherer Algorithmus betrachtet wird. Die Anzahl der Salt-Bits und Schlüsselbits variiert je nach Algorithmus. Entsprechende Details können Sie abrufen, indem Sie auf die Info-Schaltfläche neben der Algorithmusauswahl klicken. Die Verschlüsselungsschlüssel sind für jeden Thin Client eindeutig und werden an einem Ort gespeichert, den nur Administratoren Zugriff haben. Darüber hinaus kann eine Entschlüsselung nur mit bestimmten autorisierten Anwendungen auf dem System erfolgen.

Für Hashes und verschlüsselte geheime Schlüssel kann eine Gültigkeitsdauer festgelegt werden. Wenn die zwischen Hashcodierung oder Verschlüsselung des geheimen Schlüssels und dessen Entschlüsselung verstrichene Zeitdauer die festgelegte Gültigkeitsdauer überschreitet, schlägt der Hash-Abgleich oder die Entschlüsselung fehl.

Optionen

Lokaler Benutzer muss sich anmelden: Wenn diese Option ausgewählt ist, während die Active Directory Authentifizierung deaktiviert ist, wird beim Start und beim Abmelden trotzdem noch der Anmeldebildschirm angezeigt. In diesem Fall ist der Zugriff auf das System nur mit den Anmeldeinformationen des lokalen Benutzers oder Stammkontos möglich.

Vorschau für verschlüsselte Inhalte aktivieren: Wenn diese Option aktiviert ist, wird in der Systemanzeige rechts neben den meisten Eingabefeldern für das Kennwort und den geheime Schlüssel ein kleines Augensymbol angezeigt. Wenn Sie dieses Augensymbol durch Drücken und Halten der linken Maustaste auswählen, wird der geheime Schlüssel in Klartext angezeigt, solange Sie die Taste gedrückt halten. Sobald Sie die Taste wieder loslassen, wird der geheime Schlüssel wieder verborgen.

Domänentexteingabe verwenden: Wenn diese Option aktiviert ist, wird ggf. ein eigenes Eingabefeld für den Domänennamen angezeigt. Wenn diese Option deaktiviert ist, wird die Domäne anhand des im Feld „Benutzer“ angegebenen Werts bestimmt. Wenn im Feld „Benutzer“ beispielsweise „mike@mycorp“ angegeben wurde, wird davon ausgegangen, dass die Domäne „mycorp“ ist. Wenn im Feld „Benutzer“ „graycorp\mary“ angegeben wurde, wird davon ausgegangen, dass die Domäne „graycorp“ ist.

Überschreiben der Bildschirmsperre durch Administratoren zulassen: Wenn diese Option aktiviert ist, können Sie einen gesperrten Bildschirm überschreiben und zum Anmeldebildschirm oder zum ThinPro-Desktop zurückkehren, ganz so, als ob der Benutzer sich manuell vom Thin Client abgemeldet hätte.

Anpassungscenter

So öffnen Sie das Anpassungscenter:

▲ Wählen Sie in der Systemsteuerung **Setup > Anpassungscenter**.

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



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

Vor dem Wechsel in den Smart Zero-Modus sollte die Funktion zur Domänenauthentifizierung auf dem Thin Client deaktiviert werden. Die Domänenauthentifizierung und der Smart Zero-Modus sind nicht kompatibel.

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

Option	Beschreibung
Beim Start den Connection Manager starten	Wenn aktiviert, wird Connection Manager beim Systemstart automatisch gestartet.
Kontextmenü aktivieren	Deaktivieren Sie diese Option, um das Kontextmenü zu deaktivieren, das angezeigt wird, wenn Sie mit der rechten Maustaste auf den Desktop klicken.
Zugriffssteuerungssicherheit für X-Host aktivieren	Wenn aktiviert, dürfen nur die Systeme, die im Bereich X-Host-Zugriffskontrollliste aufgeführt werden, den Thin Client über Fernzugriff steuern.
USB-Update aktivieren	Ermöglicht die Installation von Updates über ein USB-Flash-Laufwerk. Weitere Informationen finden Sie unter „ USB-Updates “ auf Seite 84.
USB-Update authentifizieren	Deaktivieren Sie diese Option, um Endbenutzern die Installation von Updates über USB zu erlauben.
Benutzer erlauben, in Administratormodus zu wechseln	Deaktivieren Sie diese Option, um die Option Wechsel zwischen Administrator-/Benutzermodus in der Systemsteuerung im Benutzermodus zu entfernen.
Zeit (in Minuten), bevor der Administratormodus beendet wird	Gibt die Leerlaufzeitüberschreitung (in Minuten) an, nach der die Ausführung im Administratormodus beendet wird. Wenn der Wert 0 oder eine negative Zahl ist, wird die Ausführung im Administratormodus nicht automatisch beendet.

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

Verwenden Sie die Seite **Taskleiste**, um die Taskleiste zu konfigurieren.

Verwaltung

Menüoption	Beschreibung
Active Directory	Weitere Informationen finden Sie unter Active Directory Konfiguration auf Seite 61 .
HPDM Agent	Zum Konfigurieren des HP Device Manager (HPDM) Agent. Weitere Informationen finden Sie im <i>Administratorhandbuch</i> für HPDM.
Automatische Updates	Damit können Sie den Automatic Update-Server manuell zurücksetzen. Weitere Informationen finden Sie unter „ HP Smart Client Services “ auf Seite 71.
Komponenten-Manager	Zum Entfernen von Systemkomponenten. Weitere Informationen finden Sie unter Komponenten-Manager auf Seite 60 .

Menüoption	Beschreibung
Werkseinstellungen	Zum Wiederherstellen der Standard-Werkseinstellungen des Thin Client.
Snapshots	Zum Wiederherstellen eines früheren Zustands oder der Standard-Werkseinstellungen des Thin Client.
SSHD-Manager	Ermöglicht den Zugriff über eine Secure Shell.
ThinState	Mit HP ThinState kann entweder das gesamte Betriebssystem-Image oder nur seine Konfigurationseinstellungen kopiert oder wiederhergestellt werden. Weitere Informationen finden Sie unter HP ThinState auf Seite 62 .
VNC-Shadow	Zum Konfigurieren von VNC-Shading-Optionen. Weitere Informationen finden Sie unter VNC-Shading auf Seite 66 .
Wireless-Statistiken	Zum Anzeigen von Informationen zu WLAN-Access Points.

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 **Verwaltung > Komponenten-Manager**.

Entfernen von Komponenten

So entfernen Sie Komponenten:

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



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

2. Wählen Sie **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 **Letzte Änderung rückgängig machen** aus.
2. Klicken Sie auf **Ja**, um den Thin Client neu zu starten.

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

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

Dauerhaftes Anwenden der Änderungen

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

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

1. Wählen Sie im Komponenten-Manager **Komponentenkonfiguration anwenden** aus.
2. Wählen Sie **Ja**.

Active Directory Konfiguration

Registerkarte „Status“

Mit diesem Steuerelement können Sie die Authentifizierung mit einer Domäne, den Beitritt zu einer Domäne und zahlreiche andere domänenbezogene Optionen aktivieren und deaktivieren.

Nachdem Sie auf der Registerkarte „Status“ eine Änderung an den Domänenparametern vorgenommen haben, wird auf der Seite eine ausstehende Aktion angezeigt und Sie müssen **Übernehmen** auswählen, damit die Aktion ausgeführt wird. Für den Beitritt oder das Verlassen einer Domäne sind Anmeldeinformationen mit Berechtigungen zum Durchführen dieser Vorgänge erforderlich. Nach dem Aktivieren der Authentifizierung oder dem Beitritt zur Domäne können einige Unterparameter schreibgeschützt sein, da es zum betreffenden Zeitpunkt nicht möglich ist, sie zu ändern. Veranlassen Sie stattdessen den Austritt aus der Domäne bzw. deaktivieren Sie die Authentifizierung und übernehmen Sie dann die Änderungen. Anschließend können Sie die Authentifizierung wieder aktivieren oder mit geänderten Unterparametern beitreten.

Option	Beschreibung
Domänenname	Wenn der Thin Client den Domänennamen mithilfe von DHCP-Optionen bestimmen kann, wird dieser hier angezeigt. Andernfalls müssen Sie den vollständig qualifizierten Domänennamen manuell eingeben.
Authentifizieren mit Domäne	Wenn diese Option aktiviert ist, können die Domänen-Anmeldeinformationen verwendet werden, wie in diesem Handbuch im Abschnitt zur Active Directory Integration erläutert.

Option	Beschreibung
Thin Client-Anmeldung erforderlich	Diese Option ist standardmäßig aktiviert und veranlasst das System, beim Start den Domänen-Anmeldebildschirm anzuzeigen. Wenn diese Option deaktiviert ist, können die Domänen-Anmeldeinformationen weiterhin verwendet werden, um in den Administratormodus zu wechseln oder einen gesperrten Bildschirm zu überschreiben, allerdings ist die Funktion zum einmaligen Anmelden nicht verfügbar.
Arbeitsgruppe	Normalerweise wird diese automatisch anhand der von den Netzwerkservers bereitgestellten Informationen erkannt, aber Sie können damit eine manuelle Überschreibung vornehmen, wenn Ihre spezielle Netzwerktopologie dies erfordert.
Domänencontroller	Diese werden normalerweise mithilfe von DNS-Lookups erkannt, aber Sie können sie manuell angeben, wenn diese Informationen nicht vom Netzwerk bereitgestellt werden.
Thin Client zur Domäne hinzufügen	Wie im Kapitel über die Active Directory Integration erläutert, können Sie den Thin Client mit dieser Option den Active Directory Datenbanken formell hinzufügen.
Organisationseinheit (OE)	Der Thin Client wird normalerweise zur OE „Computer“ der Datenbank hinzugefügt, aber Sie können hier manuell einen anderen Wert eingeben, wenn das Datenbankschema dies erfordert.
Dynamischer DNS	Wenn diese Option aktiviert ist, versucht der Thin Client, den DNS-Server bei jeder Änderung seiner IP-Adresse-/Hostnamenzuordnung zu informieren.

Registerkarte „Optionen“

Option	Beschreibung
Einmaliges Anmelden aktivieren	Wenn diese Option aktiviert ist, wird ein bei der Anmeldung angegebenes Kennwort verschlüsselt und auf dem System gespeichert. Wenn eine Verbindung mit konfigurierten Anmeldeinformationen für einmaliges Anmelden hergestellt wird, kann das Kennwort entschlüsselt und an die Verbindung übergeben werden, um es für eine Remote-Anmeldung zu verwenden.
Domänenanmeldegruppe	Wenn diese Option aktiviert ist, wird die Anmeldung auf Benutzer beschränkt, die Mitglied der aufgeführten Domänengruppe sind.
Domänenadministratorgruppe	Wenn diese Option aktiviert ist, wird der Wechsel in den Administratormodus und das Überschreiben der Bildschirmsperre auf Mitglieder der aufgeführten Domänengruppe beschränkt.
Zwischenspeicherung für Domänenanmeldung aktivieren	Wenn diese Option aktiviert ist, wird ein Hash mit dem Kennwort des Benutzers auf dem System gespeichert, sodass spätere Anmeldungen auch dann erfolgen können, wenn kein Zugriff auf den Active Directory Server möglich ist.
Benutzereinstellungen bei Abmeldung beibehalten	Wenn diese Option aktiviert ist, werden jegliche von einem Domänenbenutzer vorgenommene Änderungen an den Einstellungen an einem Ort gespeichert, an dem diese Einstellungen nur für diesen Benutzer angewendet werden. Wenn diese Option deaktiviert ist, werden derartige benutzerspezifische Änderungen verworfen, wenn sich der Benutzer abmeldet.
Domänenkennwortänderungen zulassen	Wenn diese Option aktiviert ist, werden die Benutzer bei Ablauf des Kennworts aufgefordert, ihr Kennwort zu aktualisieren. Sie können ihr Kennwort dann manuell durch Klicken auf das Benutzersymbol in der Taskleiste ändern.


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

Aufzeichnen 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 **Verwaltung > ThinState**.
2. Wählen Sie das **HP ThinPro-Image** und anschließend **Weiter**.
3. Wählen Sie **HP ThinPro-Image kopieren** und anschließend **Weiter**.
4. Wählen Sie **Einen FTP-Server** und anschließend **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 **Image komprimieren**, wenn Sie möchten, dass das aufgezeichnete Image komprimiert wird.

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

6. Wählen Sie **Fertig stellen**.

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

Bereitstellen 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 **Verwaltung > ThinState**.
2. Wählen Sie das **HP ThinPro-Image** und anschließend **Weiter**.
3. Wählen Sie **HP ThinPro-Image wiederherstellen** und anschließend **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 **Benutzername** und **Kennwort** sind nicht erforderlich, wenn Sie das HTTP-Protokoll verwenden.

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

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



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

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

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



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

1. Wählen Sie in der Systemsteuerung **Verwaltung > ThinState**.
2. Wählen Sie das **HP ThinPro-Image** und anschließend **Weiter**.
3. Wählen Sie **HP ThinPro-Image kopieren** und anschließend **Weiter**.
4. Wählen Sie **Bootfähiges USB-Flash-Laufwerk erstellen** und anschließend **Weiter**.

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

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

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

Bereitstellen eines HP ThinPro-Images mit einem USB-Flash-Laufwerk

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



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

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



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

Verwalten eines Clientprofils

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



HINWEIS: Ein Clientprofil kann auch mit Profile Editor und Automatic Update vorkonfiguriert und bereitgestellt werden (weitere Informationen finden Sie unter [„Profile Editor“ auf Seite 76](#) und [„HP Smart Client Services“ auf Seite 71](#)).

Speichern eines Clientprofils auf einem FTP-Server

So speichern Sie ein Clientprofil auf einem FTP-Server:



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

1. Wählen Sie in der Systemsteuerung **Verwaltung > ThinState**.
2. Wählen Sie die **HP ThinPro-Konfiguration** und anschließend **Weiter**.
3. Wählen Sie **Konfiguration speichern** und anschließend **Weiter**.
4. Wählen Sie **Auf einem FTP-Server** und anschließend **Weiter**.
5. Geben Sie die FTP-Server-Informationen in die Felder ein.
6. Wählen Sie **Fertig stellen**.

Wiederherstellen eines Clientprofils über FTP oder HTTP

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

1. Wählen Sie in der Systemsteuerung **Verwaltung > ThinState**.
2. Wählen Sie die **HP ThinPro-Konfiguration** und anschließend **Weiter**.
3. Wählen Sie **Konfiguration wiederherstellen** und anschließend **Weiter**.
4. Wählen Sie **Auf einem Remoteserver** und anschließend **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 **Benutzername** und **Kennwort** sind nicht erforderlich, wenn Sie das HTTP-Protokoll verwenden.

6. Wählen Sie **Fertig stellen**.

Speichern eines Clientprofils auf einem USB-Flash-Laufwerk

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

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

Wiederherstellen eines Clientprofils von einem USB-Flash-Laufwerk

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

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

VNC-Shadowing

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

So greifen Sie auf das VNC Shadow-Tool zu:

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



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

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

Option	Beschreibung
VNC-Shadow aktivieren	Ermöglicht das VNC-Shadowing.
VNC Schreibgeschützt	Öffnet die VNC-Sitzung als schreibgeschützt.
VNC: Kennwort verwenden	Macht beim Zugriff auf den Thin Client über VNC ein Kennwort erforderlich. Wählen Sie Kennwort festlegen , um das Kennwort festzulegen.
Shadowing stoppen	Wenn diese Option aktiviert ist, wird oben links im Remote-System die Schaltfläche Shadowing stoppen angezeigt, mit der sich das VNC-Shadowing stoppen lässt.
VNC: Benutzer benachrichtigen, um Ablehnung zuzulassen	Ermöglicht ein Benachrichtigungs-Dialogfeld auf dem Remote-System, das den Remote-Benutzer informiert, wenn jemand versucht eine Verbindung über VNC herzustellen. Der Benutzer kann den Zugriff entweder zulassen oder verweigern.
Benachrichtigung automatisch nach x Sekunden schließen	Schließt die Benutzerbenachrichtigung nach x Sekunden.
Benutzerbenachrichtigung	Ermöglicht Ihnen, eine Nachricht im Dialogfeld für die Benachrichtigung an den Remote-Benutzer anzuzeigen.

Option	Beschreibung
Verbindungen standardmäßig verweigern	Wenn aktiviert, wird die VNC-Verbindung standardmäßig verweigert, sobald die Zeit abgelaufen ist.
VNC-Server jetzt zurücksetzen	Setzt den VNC-Server zurück, nachdem die neuen Einstellungen angewendet wurden.

Erweitert

Menüoption	Beschreibung
Zertifikate	Öffnet den Zertifikat-Manager, mit dem man ganz einfach Zertifikate importieren, anzeigen oder entfernen kann. Weitere Informationen finden Sie unter Zertifikat-Manager auf Seite 67 .
DHCP-Optionen	Zum Konfigurieren der DHCP-Optionen. Weitere Informationen finden Sie unter DHCP-Optionen auf Seite 68 .
HP Lizenz	Zum Anzeigen des HP Endbenutzer-Lizenzvertrags (EULA).
SCEP-Manager	Ermöglicht die netzwerkbasierte Zertifikatsverwaltung.
Serial Manager	Zur Konfiguration serieller Geräte.
Tastenkombinationen	Zum Erstellen, Ändern und Löschen von Tastenkombinationen.
Snipping Tool	Zum Aufnehmen eines Schnappschusses einer rechteckigen Auswahl des Bildschirms, eines bestimmten Fensters oder des gesamten Bildschirms.
Task-Manager	Zum Überwachen der CPU-Auslastung und des Verlaufs der CPU-Auslastung für den Thin Client.
Text-Editor	Öffnet einen einfachen Texteditor zum Anzeigen und Bearbeiten von Textdateien.
X-Terminal	Zum Ausführen von Linux-Befehlen.

Zertifikate



HINWEIS: Weitere Informationen über die Verwendung der Zertifikate unter Linux finden Sie auf der Website <https://www.openssl.org/docs/>.

Zertifikat-Manager

So öffnen Sie den Zertifikat-Manager:

- ▲ Wählen Sie in der Systemsteuerung **Erweitert > Zertifikate**.

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

Falls gewünscht, können Sie Profile Editor verwenden, um das Zertifikat einem Profil zuzuweisen, wie unter [Hinzufügen von Zertifikaten zu einem Clientprofil auf Seite 78](#) beschrieben.



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

SCEP-Manager

So öffnen Sie den SCEP-Manager:

- ▲ Wählen Sie in der Systemsteuerung **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 **Identifizierung** im SCEP-Manager, um ggf. Informationen über den Benutzer einzugeben.



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

Verwenden Sie die Registerkarte **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 **Einstellungen**, um zurückzukehren und eine Registrierung durchzuführen.

DHCP-Optionen

So öffnen Sie den DHCP-Options-Manager:

- ▲ Wählen Sie in der Systemsteuerung **Erweitert > DHCP-Optionen**.

Der DHCP-Options-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-Options-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 **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 **Angefordert** aktiviert ist.

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

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

8 Systeminformationen

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

Bereich	Beschreibung
Allgemein	Zeigt Informationen über BIOS, Betriebssystem, CPU und Speicher an.
Netzwerk	Zeigt Informationen über Netzwerkschnittstelle, Gateway und DNS-Einstellungen an.
Netzwerktools	<p>Bietet die folgenden Tools zur Überwachung und Problembehebung:</p> <ul style="list-style-type: none">• Ping – Spezifizieren einer IP-Adresse von einem anderen Gerät im Netzwerk, um eine Verbindung aufzubauen.• DNS-Lookup – Zum Auflösen eines Domännennamens in eine IP-Adresse.• Route verfolgen – Zum Nachverfolgen des Pfades, auf dem ein Netzwerkpaket von einem Gerät zum anderen gesendet wird.
Softwareinformationen	<p>Zeigt eine Liste der installierten Add-ons auf der Registerkarte Service-Pakete an, sowie Informationen zur Software-Version auf der Registerkarte Installierte Software.</p> <p>TIPP: Sie können auch das Administrator-Handbuch (dieses Dokument) über diesen Bildschirm aufrufen.</p>
Systemprotokolle	<p>Zeigt folgende Protokolle an:</p> <ul style="list-style-type: none">• Autorisierung und Sicherheit• Connection Manager• DHCP-Leases• Allgemeines Systemprotokoll• Kernel• Netzwerkmanager• Smart Client Services• X Server <p>Im Administratormodus kann die Debugstufe geändert werden, um weitere Informationen anzuzeigen, die möglicherweise vom HP Support bei der Problembehebung angefragt werden.</p> <p>Wählen Sie Diagnose, um eine Diagnosedatei zu speichern. Weitere Informationen finden Sie unter Verwenden der Systemdiagnose für die Fehlerbeseitigung auf Seite 82.</p>



HINWEIS: Siehe [SystemInfo auf Seite 167](#) für Informationen über die Registrierungsschlüssel, die zum Ausblenden von Systeminformationen verwendet werden können.

9 HP Smart Client Services

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

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

Unterstützte Betriebssysteme

HP Smart Client Services unterstützt die folgenden Betriebssysteme:

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



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

Voraussetzungen für HP Smart Client Services

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

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

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

Abrufen von HP Smart Client Services

Die HP Smart Client Services können Sie unter <ftp://ftp.hp.com/pub/tcdebian/SmartClientServices/> abrufen.

Anzeigen der Automatic Update-Website

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



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

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

Erstellen eines Automatic Update-Profiles

Automatic Update verwendet Profile zum Verteilen einer Konfiguration an Thin Clients. Wenn Sie ein Profil mit Profile Editor erstellen (siehe „[Profile Editor](#)“ auf Seite 76), können Sie es standardmäßig im folgenden Ordner speichern:

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

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

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

Profile für bestimmte MAC-Adressen

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

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

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

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

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

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

1. Ermitteln Sie die MAC-Adresse des Thin Client über die Systeminformationen. In den folgenden Schritten wird z. B. die MAC-Adresse 00fcab8522ac verwendet.
2. Verwenden Sie Profile Editor zum Erstellen oder Ändern eines Clientprofils (siehe [„Profile Editor“ auf Seite 76](#)), bevor Sie das Clientprofil speichern.
3. Wählen Sie in **Profile Editor** im linken Bereich **Fertig stellen**, um auf den Bereich **Aktuelles Profil** zuzugreifen.
4. Wählen Sie **Profil speichern unter** aus, um das Clientprofil wie folgt zu speichern:

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

Aktualisieren von Thin Clients

Verwenden der Methode zur Aktualisierung per Übertragung

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



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



TIPP: Um zu überprüfen, ob die Aktualisierung per Übertragung funktioniert, führen Sie Profile Editor aus und nehmen Sie einige Änderungen vor. Schließen Sie den Thin Client an und überprüfen Sie, ob das neue Profil heruntergeladen wurde. Falls nicht, siehe [„Fehlerbeseitigung“ auf Seite 81](#).

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 > Verwaltungstools > DHCP**.
2. Wählen Sie im linken Bereich des Bildschirms **DHCP** die Domäne aus, mit der die Thin Clients verbunden sind.
3. Erweitern Sie im rechten Bereich des Bildschirms **DHCP** den Eintrag **IPv4**, klicken Sie mit der rechten Maustaste darauf und wählen Sie dann **Vordefinierte Optionen einstellen** aus.
4. Wählen Sie im Dialogfeld **Vordefinierte Optionen und Werte** die Option **Hinzufügen** aus.

5. Im Feld **Optionstyp** konfigurieren Sie die Optionen wie in der folgenden Tabelle beschrieben.

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

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

Verwenden der Methode zur Aktualisierung per DNS-Alias


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

So konfigurieren Sie die Aktualisierungsmethode mit DNS Alias:

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

Verwenden der Methode zur manuellen Aktualisierung

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

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

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

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

Durchführen einer manuellen Aktualisierung

1. Wählen Sie in der Systemsteuerung **Verwaltung > Automatic Update**.
2. Wählen Sie **Manuelle Konfiguration aktivieren**.
3. Stellen Sie das **Protokoll** auf **http** ein.

4. Geben Sie im Feld **Server** Hostname und Port des Aktualisierungsservers im folgenden Format ein:
`<Hostname>:18287`
5. Geben Sie im Feld **Pfad** Folgendes ein:
`auto-update`
6. Wählen Sie **Thin Client-Konfiguration beibehalten** aus, wenn Sie alle zuvor konfigurierten Einstellungen beibehalten möchten.
7. Wählen Sie **OK** und der Thin Client ruft die Aktualisierungen ab.

10 Profile Editor

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

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

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

Öffnen von Profile Editor

- ▲ Wählen Sie **Start, Alle Programme, HP, HP Automatic Update Server** und dann **Profile Editor** aus.

Laden eines Clientprofils

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

So laden Sie ein anderes Clientprofil:

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

Anpassung von Clientprofilen

Auswählen der Plattform für ein Clientprofil

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

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



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

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

So konfigurieren Sie die Plattformeinstellungen eines Clientprofils:

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



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



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

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



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

Konfigurieren einer Standardverbindung für ein Clientprofil

So konfigurieren Sie eine Standardverbindung für ein Clientprofil:

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



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

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

Ändern von Registrierungseinstellungen eines Clientprofils

So ändern Sie die Standard-Registrierungseinstellungen für ein Clientprofil:

1. Erweitern Sie auf dem Bildschirm **Registrierung** in Profile Editor die Ordner in der Baumstruktur **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 **Wert** ein.



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

Hinzufügen von Dateien zu einem Clientprofil

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

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

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

Hinzufügen einer Konfigurationsdatei zu einem Clientprofil

1. Wählen Sie auf dem Bildschirm **Dateien** in Profile Editor **Datei hinzufügen**.
2. Wählen Sie **Datei importieren** aus, um nach der zu importierenden Datei zu suchen, und klicken Sie dann auf **Öffnen**.



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

3. Geben Sie im Feld **Pfad** den Pfad ein, in dem die Datei auf dem Thin Client installiert werden soll.

4. Legen Sie im Abschnitt **Dateidetails** die Felder **Besitzer**, **Gruppe** und **Berechtigungen** auf die entsprechenden Werte fest.



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

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



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

Hinzufügen von Zertifikaten zu einem Clientprofil

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

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

So importieren Sie andere Zertifikate zu einem Client-Profil:

1. Wählen Sie auf dem Bildschirm **Dateien** in Profile Editor **Datei hinzufügen**.
2. Wählen Sie **Datei importieren** aus, ermitteln Sie das Zertifikat und wählen Sie auf **Öffnen** aus.



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

3. Stellen Sie im Feld **Pfad** den Pfad auf Folgendes ein:
`/usr/local/share/ca-certificates`
4. Wählen Sie **Speichern**, um das Hinzufügen des Zertifikats zum Clientprofil abzuschließen.
5. Verwenden Sie nach der Installation des Clientprofils den **Zertifikat-Manager**, um zu überprüfen, ob das Zertifikat ordnungsgemäß importiert wurde.

Hinzufügen eines symbolischen Links zu einem Clientprofil

1. Wählen Sie auf dem Bildschirm **Dateien** in Profile Editor **Datei hinzufügen**.
2. Wählen Sie in der Dropdown-Liste **Typ** die Option **Link**.
3. Legen Sie im Abschnitt **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 **Speichern** aus, um das Hinzufügen des symbolischen Links abzuschließen.

Speichern des Clientprofils

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



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

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

Konfiguration eines seriellen oder parallelen Druckers

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

Abrufen der Druckereinstellungen

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

1. Bei den meisten Druckern drücken und halten Sie die Taste **Papierzufuhr** gedrückt, während das Gerät eingeschaltet wird.
2. Nach einigen Sekunden lassen Sie die **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 **Papierzufuhr**-Taste nochmals drücken, damit die Diagnosesseite gedruckt wird.

Einrichten von Druckeranschlüssen

1. Wählen Sie im **Profile Editor** die Option **Registrierung** und aktivieren Sie dann das Kontrollkästchen **Alle Einstellungen anzeigen**.
2. Aktivieren Sie die Druckerportzuordnung für Ihren Verbindungstyp:
 - Citrix – Es sind keine Aktionen erforderlich.
 - RDP – Navigieren Sie zu **root > ConnectionType > freerdp**. Klicken Sie mit der rechten Maustaste auf den Ordner **connections**, wählen Sie **Neue Verbindung** und dann **OK**. Legen Sie den Registrierungsschlüssel **portMapping** auf 1 fest, um die Zuordnung des Druckeranschlusses zu aktivieren.
 - VMware Horizon View – Navigieren Sie zu **root > ConnectionType > view**. Klicken Sie mit der rechten Maustaste auf den Ordner **connections**, wählen Sie **Neue Verbindung** und dann **OK**. Legen Sie im Ordner **xfreerdpOptions** den Registrierungsschlüssel **portMapping** auf 1 fest, um die Zuordnung des Druckeranschlusses zu aktivieren.

3. Navigieren Sie zu **root > Serial**. Klicken Sie mit der rechten Maustaste auf den Ordner **Serial** und wählen Sie **Neue UUID** und dann **OK**.
4. Stellen Sie unter dem neuen Verzeichnis die Werte **Baud**, **Datenbits**, **Fluss** und **Parität** gemäß der Werte unter [Abrufen der Druckereinstellungen auf Seite 79](#) ein.

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

Installieren von Druckern auf dem Server

1. Auf dem Windows Desktop wählen Sie **Start > Drucker und Faxgeräte**.
2. Wählen Sie **Drucker hinzufügen** und dann **Weiter**.
3. Wählen Sie **Lokaler Drucker, der an den Computer angeschlossen ist** und bei Bedarf deaktivieren Sie **Plug & Play-Drucker automatisch ermitteln und installieren**.
4. Klicken Sie dann auf **Weiter**.
5. Wählen Sie im Menü einen Anschluss.



HINWEIS: Der Port, den Sie benötigen, befindet sich im Bereich mit den als **TS###** gekennzeichneten Ports, wobei ### eine Zahl von 000 bis 009 oder von 033 bis 044 ist. Welcher Port der Richtige ist, hängt von Ihrem Host-Namen und von dem zu installierenden Drucker ab. Wenn der Host-Name ZTAHENAKOS lautet und Sie einen seriellen Drucker installieren möchten, wählen Sie den Port mit der Bezeichnung **ZTAHENAKOS:COM1**. Für einen parallelen Drucker wählen Sie (**ZTAHENAKOS:LPT1**). Die Kennzeichnung **TS###** wird vom Server zugewiesen und kann sich daher jedes Mal ändern.

6. Wählen Sie den Hersteller und den Treiber für Ihren Drucker aus.



TIPP: Falls gewünscht, verwenden Sie die Treiber-Disc **Windows Update** zum Installieren des Treibers.



HINWEIS: Für einfache oder Testdrucke funktioniert normalerweise der Drucker **Allgemeiner Hersteller** oder **Allgemein / Nur Text**.

7. Wenn Sie dazu aufgefordert werden, den vorhandenen funktionsfähigen Treiber beizubehalten, tun Sie es und wählen Sie dann **Weiter** aus.
8. Weisen Sie dem Drucker einen Namen zu. Wählen Sie **Ja**, um ihn als Standarddrucker zu verwenden, und wählen Sie dann **Weiter**.
9. Um den Drucker freizugeben, wählen Sie **Freigabename** und weisen Sie ihm einen Freigabennamen zu. Wählen Sie andernfalls **Weiter**.
10. Auf der nächsten Seite können Sie einen Testdruck anfordern. HP empfiehlt dies, weil Sie dadurch überprüfen können, ob der Drucker korrekt eingerichtet ist. Falls der Drucker nicht korrekt eingerichtet ist, überprüfen Sie die Einstellungen und versuchen Sie es erneut.



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

11 Fehlerbeseitigung

Fehlerbeseitigung bei der Netzwerkverbindung

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

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

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

```
64 bytes from 10.30.8.52: icmp_seq=1 ttl=64 time=0.81 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 Netzkabel und die Netzwerkeinstellungen in der Systemsteuerung.
 - b. Versuchen Sie, den Ping-Befehl für andere Server oder Thin Clients auszuführen.
 - c. Wenn Sie andere Thin Clients erreichen können, überprüfen Sie, ob Sie die richtige Serveradresse eingegeben haben.
 - d. Führen Sie einen Ping unter Verwendung der IP-Adresse durch anstelle des Domänennamens oder umgekehrt.
3. Überprüfen Sie die Systemprotokolle indem Sie Folgendes durchführen:
 - a. Wählen Sie die Schaltfläche „Systeminformationen“ in der Taskleiste und dann die Registerkarte **Systemprotokolle**.
 - b. Überprüfen Sie die Protokolle auf Fehler.
 - c. Wenn ein Fehler aufgetreten ist, wird die Benachrichtigung **Server is not set up** (Server ist nicht eingerichtet) angezeigt. Stellen Sie sicher, dass der Server richtig eingerichtet ist und dass HP Smart Client Services ausgeführt wird.

Fehlerbeseitigung bei abgelaufenen Citrix Kennwörtern

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

Verwenden der Systemdiagnose für die Fehlerbeseitigung

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



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


Speichern von Systemdiagnosedaten

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

Dekomprimieren der Systemdiagnosedateien

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

Dekomprimieren der Systemdiagnosedateien auf Windows-basierten Systemen

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

Anzeigen von Dateien im Ordner Commands

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

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

Anzeigen von Dateien im Ordner **/var/log**

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

Anzeigen von Dateien im Ordner **/etc**

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

A USB-Updates

Wenn die USB-Updates aktiviert sind (siehe [Anpassungszentrum auf Seite 58](#)), können Sie ein USB-Flash-Laufwerk verwenden, um gleichzeitig mehrere Add-ons und Zertifikate zu installieren oder zum Bereitstellen eines Profils.

So führen Sie USB-Updates durch:

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



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

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

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

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

HP ThinUpdate

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

B BIOS-Tools (nur Desktop-Thin Clients)

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

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

Diese Tools können über einen X-Terminal ausgeführt werden.

BIOS-Tool für Einstellungen

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



HINWEIS: Änderungen werden erst beim nächsten Neustart wirksam.

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

BIOS Flashing-Tool

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



HINWEIS: Änderungen werden erst beim nächsten Neustart wirksam.

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

C Ändern der Größe der Flash-Laufwerk-Partition



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

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



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

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

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

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

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

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



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

Audio

Registrierungsschlüssel	Beschreibung
<code>root/Audio/AdjustSoundPath</code>	Legt den vollständigen Pfad auf den wiedergegebenen Sound fest, wenn die Wiedergabelautstärke über die Lautstärkeregler geändert wird.
<code>root/Audio/JackRetask</code>	<p>Dieser Registrierungsschlüssel kann nur für Thin Clients verwendet werden, die über für unterschiedliche Zwecke verwendbare Buchsen verfügen.</p> <p>Für den Anschluss unten auf der Vorderseite des t730:</p> <ul style="list-style-type: none">• 0/1: Keine Änderung/Kopfhörer• 2: Mikrofon <p>Für den Anschluss auf der Rückseite des t630:</p> <ul style="list-style-type: none">• 0: Keine Änderung/Line In• 1: Kopfhörer/Line Out <p>Nach dem Ändern dieser Einstellungen müssen Sie den Thin Client neu starten.</p>
<code>root/Audio/OutputMute</code>	Wenn der Wert 1 ist, sind die internen Lautsprecher und die Kopfhörerbuchse stumm geschaltet.
<code>root/Audio/OutputScale</code>	Bestimmt die Lautstärke-Skalierung für die internen Lautsprecher und die Kopfhörerbuchse, die zwischen 1 und 400 liegt.
<code>root/Audio/OutputScaleAuto</code>	Wenn der Wert 1 ist, wird der <code>OutputScale</code> -Wert automatisch basierend auf dem Thin Client-Modell gesetzt.
<code>root/Audio/OutputVolume</code>	Legt die Lautstärke für die internen Lautsprecher und die Kopfhörerbuchse fest, die zwischen 1 bis 100 liegt.
<code>root/Audio/PlaybackDevice</code>	Legt fest, dass das Gerät für die Wiedergabe verwendet wird.

Registrierungsschlüssel	Beschreibung
<code>root/Audio/PulseBuffer</code>	Der empfohlene Bereich für diesen Wert liegt zwischen 1024 und 8192. Ein zu hoher Wert kann zu Schwankungen bei der Wiedergabe führen, ein zu geringer Wert hingegen kann zum Absturz des Thin Client führen.
<code>root/Audio/RecordDevice</code>	Legt fest, dass das Gerät für die Aufzeichnung verwendet wird.
<code>root/Audio/RecordMute</code>	Wenn der Wert 1 ist, ist das Mikrofon stumm geschaltet.
<code>root/Audio/RecordScale</code>	Legt die Lautstärkeskalierung für die Mikrofonbuchse fest, die zwischen 1 und 400 liegt.
<code>root/Audio/RecordScaleAuto</code>	Wenn der Wert 1 ist, wird der <code>RecordScale</code> -Wert automatisch basierend auf dem Thin Client-Modell gesetzt.
<code>root/Audio/RecordVolume</code>	Legt die Lautstärke für die Mikrofonbuchse fest, die zwischen 1 bis 100 liegt.
<code>root/Audio/VisibleInSystray</code>	Wenn der Wert 1 ist, dann ist ein Lautsprechersymbol in der Taskleiste sichtbar.
<code>root/Audio/shortcutPassThrough</code>	Definiert die Apps, die mithilfe einer durch Leerzeichen getrennten Liste die Weitergabe von Verknüpfungen mit Audio-Inhalten zulassen. Die verfügbaren Optionen sind <code>freerdp</code> , <code>view</code> und <code>xen</code> .

CertMgr

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

ComponentMgr

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

ConnectionManager

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionManager/customLogoPath</code>	
<code>root/ConnectionManager/defaultConnection</code>	Um eine Verbindung beim Start ordnungsgemäß zu starten, muss dies als eine gültige Verbindung im Format <code><Typ>:<Label></code> eingestellt werden, wie im folgenden Beispiel gezeigt: <code>xen:Default Connection</code>
<code>root/ConnectionManager/minHeight</code>	
<code>root/ConnectionManager/minWidth</code>	
<code>root/ConnectionManager/splashLogoPath</code>	Zeigt den vollständigen Pfad zum Standard-Image an, während eine Verbindung geladen wird.

Registrierungsschlüssel	Beschreibung
root/ConnectionManager/useKioskMode	
root/ConnectionManager/useSplashOnConnectionStartup	Wenn der Wert 1 ist, wird das durch <code>splashLogoPath</code> festgelegte Image aktiviert. Standardmäßig wird dies für ThinPro aktiviert und für Smart Zero deaktiviert.

ConnectionType

custom

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/custom/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/custom/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/custom/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/custom/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/custom/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/custom/connections/<UUID>/waitForNetwork	Wenn der Wert 1 ist, wird die Verbindung erst gestartet, wenn der Netzbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzbetrieb 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 Connection Manager 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.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/custom/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlménú der Verbindungstypen angezeigt wird.
root/ConnectionType/custom/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert verschiebt den Verbindungstyp in der Liste nach oben. Wenn der Wert 0 ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar und wird als letzter in Connection Manager angezeigt. Verbindungstypen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/custom/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
root/ConnectionType/custom/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn <code>connection-mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
root/ConnectionType/custom/coreSettings/watchPid	Wenn der Wert 1 ist, wird die unter dem Namen <code>AppName</code> angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/coreSettings/wrapperScript	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/gui/CustomManager/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/gui/CustomManager/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/gui/CustomManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/gui/CustomManager/widgets/autoReconnect	Zum Einstellen des Status für das Widget Automatische Verbindungswiederherstellung in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/autostart	Zum Einstellen des Status für das Widget Autostart Priorität in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/custom/gui/CustomManager/widgets/command	Zum Einstellen des Status für das Widget Auszuführenden Befehl eingeben in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/fallBackConnection	Zum Einstellen des Status für das Widget Alternative Verbindung in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/hasDesktopIcon	Zum Einstellen des Status für das Widget Symbol auf Desktop anzeigen in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/label	Zum Einstellen des Status für das Widget Name in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/waitForNetwork	Zum Einstellen des Status für das Widget Vor der Anmeldung auf Netzwerkverbindung warten in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

firefox

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/firefox/connections/<UUID>/authorizations/user/edit	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
root/ConnectionType/firefox/connections/<UUID>/authorizations/user/execution	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
root/ConnectionType/firefox/connections/<UUID>/autoReconnect	Wenn der Wert 1 ist, 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>/enableSmartCard	Wenn der Wert 1 ist, ist die Smart Card-Anmeldung für Citrix Verbindungen aktiviert, die über den Internetbrowser erstellt werden.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/firefox/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/firefox/connections/<UUID>/forbiddenFiles	Dieser Registrierungsschlüssel funktioniert nur, wenn Verbindungen die Verwaltung der eigenen Einstellungen ermöglichen im Web Browser Connection General Settings Manager ausgewählt ist. Die Dateien, die im Wert dieses Registrierungsschlüssels aufgeführt sind, werden entfernt, sobald eine Web Browser-Verbindung beendet wurde. Die Dateinamen sollte durch Kommas getrennt werden und ein Platzhalter wird unterstützt. Beispiel: *.rdf,cookies.sqlite

Registrierungsschlüssel	Beschreibung
root/ConnectionType/firefox/connections/<UUID>/fullscreen	Wenn der Wert 1 ist, startet der Webbrowser im Vollbildmodus. Wenn <code>KioskMode</code> deaktiviert ist, ist die Benutzeroberfläche des Browsers im Vollbildmodus zugänglich.
root/ConnectionType/firefox/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/firefox/connections/<UUID>/intendedUse	Legt die vorgesehene Nutzung dieser Web Browser-Verbindung auf Citrix, RDP oder Internet fest.
root/ConnectionType/firefox/connections/<UUID>/kioskMode	Wenn der Wert 1 ist, wird der Internetbrowser im Kioskmodus gestartet, was bedeutet, dass der Internetbrowser im Vollbildmodus gestartet wird, (selbst wenn <code>fullscreen</code> auf 0 eingestellt ist) und die Benutzeroberfläche des Browsers nicht zur Verfügung steht.
root/ConnectionType/firefox/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/firefox/connections/<UUID>/showBackForwardButton	Wenn der Wert 1 ist, werden die Schaltflächen „Zurück“ und „Vorwärts“ des Internetbrowsers angezeigt, wenn der Kioskmodus aktiviert ist.
root/ConnectionType/firefox/connections/<UUID>/showHomeButton	Wenn der Wert 1 ist, wird die Schaltfläche „Startseite“ des Internetbrowsers angezeigt, wenn der Kioskmodus aktiviert ist.
root/ConnectionType/firefox/connections/<UUID>/showSearchBar	Wenn der Wert 1 ist, wird die Suchleiste des Internetbrowsers angezeigt, wenn der Kioskmodus aktiviert ist.
root/ConnectionType/firefox/connections/<UUID>/showTabsBar	Wenn der Wert 1 ist, werden Registerkarten des Internetbrowsers angezeigt, wenn der Kioskmodus aktiviert ist.
root/ConnectionType/firefox/connections/<UUID>/showTaskBar	Wenn der Wert 1 ist, wird die Taskleiste des Internetbrowsers angezeigt, wenn der Kioskmodus aktiviert ist.
root/ConnectionType/firefox/connections/<UUID>/showUrlBarRefreshButton	Wenn der Wert 1 ist, werden die URL-Leiste und die Schaltfläche „Aktualisieren“ des Internetbrowsers angezeigt, wenn der Kioskmodus aktiviert ist.
root/ConnectionType/firefox/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/firefox/connections/<UUID>/waitForNetwork	Wenn der Wert 1 ist, 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.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/firefox/gui/FirefoxManager/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/gui/FirefoxManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/address	Zum Einstellen des Status für das Widget URL in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autoReconnect	Zum Einstellen des Status für das Widget Automatische Verbindungswiederherstellung in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autostart	Zum Einstellen des Status für das Widget Autostart Priorität in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/enablePrintDialog	Zum Einstellen des Status für das Widget Druckdialog aktivieren in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/fallBackConnection	Zum Einstellen des Status für das Widget Alternative Verbindung in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/hasDesktopIcon	Zum Einstellen des Status für das Widget Symbol auf Desktop anzeigen in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/kioskMode	Zum Einstellen des Status für das Widget Kiosk-Modus aktivieren in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/label	Zum Einstellen des Status für das Widget Name in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/showBackForwardButton	Zum Einstellen des Status für das Widget Schaltfläche „Zurück“ und „Vorwärts“ anzeigen in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/showHomeButton	Zum Einstellen des Status für das Widget Schaltfläche „Startseite“ anzeigen in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/showSearchBar	Zum Einstellen des Status für das Widget Suchleiste anzeigen in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/showTabsBar	Zum Einstellen des Status für das Widget Registerkartenleiste anzeigen in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/showTaskBar	Zum Einstellen des Status für das Widget Taskleiste anzeigen in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/ showUrlBarRefreshButton	Zum Einstellen des Status für das Widget URL-Leiste und Aktualisierungsschaltfläche anzeigen in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/startMode	Zum Einstellen des Status für das Widget Vollbildmodus aktivieren in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die

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

freerdp

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/freerdp/authorizations/user/add</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/freerdp/authorizations/user/general</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/freerdp/connections/<UUID>/ExtraArgs</code>	Gibt zusätzliche Argumente zum Xfreerd-Client an. Führen Sie <code>xfreerd -help</code> über ein X-Terminal aus, um alle verfügbaren Argumente zu sehen.
<code>root/ConnectionType/freerdp/connections/<UUID>/SingleSignOn</code>	
<code>root/ConnectionType/freerdp/connections/<UUID>/address</code>	Legt den Hostnamen bzw. die IP-Adresse fest, zu der die Verbindung aufgebaut werden soll. Die Portnummer kann nach einem Doppelpunkt am Ende angehängt werden. Beispiel: <code>servername:3389</code>
<code>root/ConnectionType/freerdp/connections/<UUID>/afterStoppedCommand</code>	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/freerdp/connections/<UUID>/application</code>	Gibt eine alternative Shell oder Anwendung an, die ausgeführt werden soll.
<code>root/ConnectionType/freerdp/connections/<UUID>/attachToConsole</code>	
<code>root/ConnectionType/freerdp/connections/<UUID>/audioLatency</code>	Legt den durchschnittlichen Offset in Millisekunden zwischen dem Audiostream und der Anzeige der entsprechenden Videoframes nach dem Entschlüsseln fest.
<code>root/ConnectionType/freerdp/connections/<UUID>/authorizations/user/edit</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
<code>root/ConnectionType/freerdp/connections/<UUID>/authorizations/user/execution</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
<code>root/ConnectionType/freerdp/connections/<UUID>/autoReconnect</code>	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
<code>root/ConnectionType/freerdp/connections/<UUID>/autoReconnectDelay</code>	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort

Registrierungsschlüssel	Beschreibung
	neu gestartet. Diese Einstellung wird nur wirksam, wenn <code>autoReconnect</code> auf 1 eingestellt ist.
<code>root/ConnectionType/freerdp/connections/<UUID>/autostart</code>	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
<code>root/ConnectionType/freerdp/connections/<UUID>/autostartDelay</code>	Gibt die Wartezeit in Sekunden an, bevor die Verbindung beim Systemstart gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Systemstart gestartet. Diese Einstellung wird nur wirksam, wenn <code>autostart</code> auf 1 eingestellt ist.
<code>root/ConnectionType/freerdp/connections/<UUID>/bandwidthLimitation</code>	Wenn der Wert größer als 0 ist, stellt der Wert eine ungefähre Bandbreitenbegrenzung für das Herunter- und Hochladen in Kilobytes pro Sekunde dar. Ist der Wert 0 (Standardwert), gibt es keine Begrenzung.
<code>root/ConnectionType/freerdp/connections/<UUID>/beforeStartingCommand</code>	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/freerdp/connections/<UUID>/clipboardExtension</code>	Wenn der Wert 1 ist, die Zwischenablage sowohl zwischen verschiedenen RDP-Sitzungen als auch zwischen RDP-Sitzungen und dem lokalen System aktiviert.
<code>root/ConnectionType/freerdp/connections/<UUID>/compression</code>	Wenn der Wert 1 ist, wird die Komprimierung von RDP-Daten zwischen dem Client und dem Server aktiviert.
<code>root/ConnectionType/freerdp/connections/<UUID>/credentialsType</code>	Gibt den Anmeldeinformationstyp abhängig davon an, ob die Anmeldeinformationen durch <code>sso</code> (einmaliges Anmelden), <code>startup</code> (Anmeldeinformationen werden beim Start abgefragt), <code>password</code> (vorkonfigurierte(r/s) Benutzer/Domäne/Kennwort) oder <code>smartcard</code> (vorkonfigurierte Smart Card) bereitgestellt werden sollen.
<code>root/ConnectionType/freerdp/connections/<UUID>/dependConnectionId</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/freerdp/connections/<UUID>/directory</code>	Gibt das Systemstart-Verzeichnis an, in dem eine alternative Shell-Anwendung ausgeführt wird.
<code>root/ConnectionType/freerdp/connections/<UUID>/disableMMRwithRFX</code>	Wenn die Einstellung 1 ist, wird die Multimedia-Umleitung deaktiviert, wenn eine gültige RemoteFX-Sitzung aufgebaut wurde.
<code>root/ConnectionType/freerdp/connections/<UUID>/domain</code>	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.
<code>root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/key</code>	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
<code>root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/value</code>	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
<code>root/ConnectionType/freerdp/connections/<UUID>/fallBackConnection</code>	Legt die alternative Verbindung über seine UUID fest.
<code>root/ConnectionType/freerdp/connections/<UUID>/frameAcknowledgeCount</code>	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. Wenn der Wert 0 ist, wird

Registrierungsschlüssel	Beschreibung
	die Frame-Bestätigung bei den Client-Server-Interaktionen nicht verwendet.
root/ConnectionType/freerdp/connections/<UUID>/gatewayAddress	Legt den RD-Gateway-Servernamen oder die Adresse fest.
root/ConnectionType/freerdp/connections/<UUID>/gatewayCredentialsType	Gibt den Anmeldeinformationstyp abhängig davon an, ob die Anmeldeinformationen durch <code>sso</code> (einmaliges Anmelden), <code>startup</code> (Anmeldeinformationen werden beim Start abgefragt) oder <code>password</code> (vorkonfigurierte(r/s) Benutzer/Domäne/Kennwort) bereitgestellt werden sollen.
root/ConnectionType/freerdp/connections/<UUID>/gatewayDomain	Legt die Standarddomäne fest, die während der Anmeldung vom RD-Gateway benötigt wird. In der Regel, wird diese Einstellung bei Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername zur Anmeldung verwendet wird. Wenn <code>GatewayUsesSameCredentials</code> auf 1 eingestellt ist, wird dieser Wert deaktiviert.
root/ConnectionType/freerdp/connections/<UUID>/gatewayEnabled	Wenn der Wert 1 ist, wird die Verwendung des RD-Gateway erwartet.
root/ConnectionType/freerdp/connections/<UUID>/gatewayPassword	Gibt das Standardkennwort an, das vom RD-Gateway während der Anmeldung benötigt wird. Dieser Wert ist normalerweise verschlüsselt. In der Regel, wird diese Einstellung bei Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername zur Anmeldung verwendet wird. Wenn <code>GatewayUsesSameCredentials</code> auf 1 eingestellt ist, wird dieser Wert deaktiviert.
root/ConnectionType/freerdp/connections/<UUID>/gatewayPort	Gibt die Portnummer an, die bei Kontaktaufnahme mit den RDP-Server zu verwenden ist. Dieser Schlüssel kann leer gelassen werden. Der am häufigsten verwendete Wert ist 443.
root/ConnectionType/freerdp/connections/<UUID>/gatewayUser	Gibt den Standard-Benutzernamen an, der vom Gateway während der Anmeldung benötigt wird. In der Regel, wird diese Einstellung bei Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername zur Anmeldung verwendet wird. Wenn <code>GatewayUsesSameCredentials</code> auf 1 eingestellt ist, wird dieser Wert deaktiviert.
root/ConnectionType/freerdp/connections/<UUID>/gatewayUsesSameCredentials	Wenn der Wert 1 ist, verwendet das Gerät zur Herstellung einer Verbindung zum RD-Gateway dieselben Anmeldeinformationen, die auch zur Verbindung mit dem endgültigen Server verwendet werden.
root/ConnectionType/freerdp/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/freerdp/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/freerdp/connections/<UUID>/loadBalanceInfo	Dieser Wert ist der Lastenausgleich-Cookie, der zu Vermittlungszwecken beim Herstellen einer Verbindung an den Server gesendet wird und entspricht dem Feld <code>Loadbalanceinfo</code> in der Datei <code>.rdp</code> . Der Standardwert ist leer.
root/ConnectionType/freerdp/connections/<UUID>/localPartitionRedirection	Wenn der Wert 1 ist, werden die lokalen nicht-USB-Speicherpartitionen über die <code>Storage</code> zum Remote-Host umgeleitet. Wenn der Wert 0 ist, ist die Erweiterung für nicht-USB-Speicher Partitionen deaktiviert, die nicht von HP ThinPro verwendet werden.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/<UUID>/loginfields/domain	Wenn der Wert 1 ist, wird das Feld 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 Kennwort im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/rememberme	Wenn der Wert 1 ist, wird das Kontrollkästchen 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 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-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 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	Wenn der Wert 0 ist, 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	Wenn der Wert 0 ist, 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	Wenn der Wert 1 ist, ist die Desktopgestaltung (wie durchsichtige Rahmen) möglich, sofern 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	Wenn der Wert 1 ist, ist die Schriftglättung möglich, sofern 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.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorSettings	Wenn der Wert 1 ist, wird das Blinken des Cursors deaktiviert, 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	Wenn der Wert ist, wird der Mauscursor-Schatten deaktiviert, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoMenuAnimations	Wenn der Wert 1 ist, werden die Menüanimationen deaktiviert, 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	Wenn der Wert 1 ist, werden die Designs der Benutzeroberfläche deaktiviert, 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	Wenn der Wert 1 ist, werden die Desktop-Hintergrundbilder deaktiviert, 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	Wenn der Wert 1, wird die Option zum Ziehen von Fenstern mit vollem Inhalt deaktiviert, 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. Wenn der Wert 2 ist, werden USB-Drucker entsprechend der Konfiguration im USB-Manager weitergeleitet.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/autoDisconnectTimeout	Legt die Anzahl von Minuten fest, die ohne Ausführung einer RemoteApp- und Desktop-Ressource verstreichen kann, bevor die Verbindung automatisch beendet wird. Ein Countdown-Zähler wird während der letzten 20 Sekunden angezeigt, sodass der Benutzer die Möglichkeit hat, den Timer zu deaktivieren. Ist der Wert 0 (Standardwert), ist der Timer deaktiviert.
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.

Registrierungsschlüssel	Beschreibung
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>/rdWebFeed/ trustedPublisherShalThumbprints	Gibt eine durch Kommas getrennte Liste der SHA1-Fingerabdrücke vertrauenswürdiger Herausgeber von Ressourcen an. Beachten Sie, dass ein Zertifikat nicht überprüft wird, das mit einem dieser Fingerabdrücke übereinstimmt. Importieren Sie zur Erhöhung der Sicherheit die Stamm-CA des Herausgebers. Weitere Informationen finden Sie unter dem Registrierungsschlüssel <code>verifyPublisherSignature</code> und im Zertifikat-Manager in der Systemsteuerung.
root/ConnectionType/freerdp/connections/ <UUID>/rdWebFeed/verifyPublisherSignature	Wenn der Wert 1 ist, wird die Signatur des Herausgebers überprüft, sofern sie in veröffentlichten RDP-Dateien verfügbar ist. Nur Ressourcen mit einer gültigen Signatur von einem vertrauenswürdigen Herausgeber können ausgeführt werden. Wenn der Wert 0 ist, wird die Signatur nicht überprüft. Weitere Informationen finden Sie unter dem Registrierungsschlüssel <code>trustedPublisherShalThumbprints</code> .
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/freerdp/connections/ <UUID>/rdpEncryption	Wenn der Wert 1 ist, 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>/redirectPreference	Zur Umleitung erhält der RDP-Client verschiedene mögliche Ziele. Diese werden normalerweise in der folgenden Reihenfolge ausprobiert: FQDN, primäre IP, IP-Liste, NetBIOS. Wenn FQDN nicht gewünscht ist, kann eine der Alternativen zuerst ausprobiert werden, indem dieser Registrierungsschlüssel festgelegt wird. Wenn diese Methode nicht funktioniert, wird auf dem RDP-Client wieder die ursprüngliche Reihenfolge herangezogen. Mit der Einstellung <code>auto</code> wird die ursprüngliche Reihenfolge erzwungen.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/freerdp/connections/<UUID>/remoteApp</code>	Gibt den Namen einer verfügbaren Anwendung an, die im RAIL-Modus (Remote Application Integrated Locally) ausgeführt werden soll.
<code>root/ConnectionType/freerdp/connections/<UUID>/remoteDesktopService</code>	Wenn der Wert <code>Remote Computer</code> ist, wird eine direkte RDP-Verbindung mit einem Remotecomputer hergestellt. Wenn der Wert <code>RD Web Access</code> ist, wird zuerst eine Verbindung mit einem RD Web Access-Dienst hergestellt, um einen Feed der veröffentlichte RemoteApp-Ressourcen abzurufen.
<code>root/ConnectionType/freerdp/connections/<UUID>/remoteFx</code>	Wenn der Wert 1 ist, wird RemoteFX in der Form von RDP 7.1 verwendet, wenn verfügbar. Diese Einstellung ist veraltet und ist möglicherweise in einer zukünftigen Version von HP ThinPro nicht mehr enthalten. Diese Einstellung sollte nur bei einem Fehler des RemoteFX-Protokolls deaktiviert werden. Durch das Deaktivieren dieser Einstellung können auch erweiterte Codecs deaktiviert werden.
<code>root/ConnectionType/freerdp/connections/<UUID>/scCertificate</code>	Wenn eine vorkonfigurierte Smart Card-Anmeldung ausgewählt ist, wird damit eine Kennung vorgegeben, die dem Zertifikat auf der zur Authentifizierung verwendeten Smart Card entspricht.
<code>root/ConnectionType/freerdp/connections/<UUID>/scPin</code>	Wenn eine vorkonfigurierte Smart Card-Anmeldung ausgewählt ist, wird damit die PIN oder das Kennwort für diese Smart Card vorgegeben.
<code>root/ConnectionType/freerdp/connections/<UUID>/seamlessWindow</code>	Wenn der Wert 1 ist, sind die Fensterdekorationen deaktiviert. Dies kann in einer Konfiguration mit mehreren Monitoren wünschenswert sein, um die Einstellung der Verbindung auf die Größe des primären Monitors zu ermöglichen.
<code>root/ConnectionType/freerdp/connections/<UUID>/securityLevel</code>	Legt die Sicherheitsstufe von Zertifikaten fest. Wenn der Wert 0 ist, sind alle Verbindungen zulässig. Wenn der Wert 1 ist, werden beibehaltene Hosts ausgewählt und eine Warnung wird angezeigt, sofern die Überprüfung nicht erfolgreich ist. Wenn der Wert 2 ist, werden beibehaltene Hosts nicht ausgewählt und eine Warnung wird angezeigt, sofern die Überprüfung nicht erfolgreich ist. Wenn der Wert 3 ist, werden alle unsichere Verbindungen verweigert.
<code>root/ConnectionType/freerdp/connections/<UUID>/sendHostname</code>	Legt den Thin Client-Hostnamen fest, der an den Remote-Host gesendet wird. Wenn keine Eintragung vorgenommen wird, wird der System-Host-Namen gesendet. Der Registrierungsschlüssel <code>root/ConnectionType/freerdp/general/sendHostname</code> muss auf <code>hostname</code> eingestellt sein, damit dieser Schlüssel verwendet wird.
<code>root/ConnectionType/freerdp/connections/<UUID>/showConnectionGraph</code>	Dies ist eine Diagnosefunktion. Wenn der Wert 1 ist, wird beim Starten der Sitzung ein separates Programm gestartet, um den Verbindungszustand grafisch darzustellen.
<code>root/ConnectionType/freerdp/connections/<UUID>/showRDPDashboard</code>	Ist der Wert 1, wenn die Sitzung gestartet wird, werden in einem gesonderten Fenster RDP-Leistung und -Status angezeigt.
<code>root/ConnectionType/freerdp/connections/<UUID>/smartcard</code>	Wenn der Wert 1 ist, ist die lokale Smart Card-Authentifizierung zum Remote-Host zulässig. Zurzeit wird dadurch Network Level Authentication (NLA) deaktiviert.
<code>root/ConnectionType/freerdp/connections/<UUID>/sound</code>	Durch die Einstellung 1 werden die Wiedergabe- und Aufnahmegeräte über die Erweiterung von <code>Audio</code> zum Remote-Host umgeleitet. Durch die Einstellung 0 wird die Erweiterung deaktiviert. Wenn der Wert 2 ist, werden USB-Audiogeräte entsprechend der Konfiguration im USB-Manager weitergeleitet. In der Regel, empfiehlt HP, dass dieser Wert auf 1 gesetzt wird, sodass High-Level-Audio-Umleitung verwendet wird. Dadurch

Registrierungsschlüssel	Beschreibung
	wird die Audioqualität verbessert und sichergestellt, dass Client-Audio, das mittels anderer Methoden umgeleitet wird (wie zum Beispiel <code>Multimedia Redirection</code>), den lokalen Audioeinstellungen entspricht.
<code>root/ConnectionType/freerdp/connections/<UUID>/startMode</code>	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
<code>root/ConnectionType/freerdp/connections/<UUID>/timeoutError</code>	Legt die Anzahl von Millisekunden fest, die nach dem Verlust einer Verbindung gewartet werden, bevor der Versuch, eine Verbindung mit dem Server herzustellen, aufgegeben wird. Wenn der Wert 0 ist, dann wird immer wieder versucht, die Verbindung wieder herzustellen.
<code>root/ConnectionType/freerdp/connections/<UUID>/timeoutRecovery</code>	Legt die Anzahl von Millisekunden fest, die nach dem Ausfall einer Verbindung für die Wiederherstellung des Netzwerkbetriebs vergehen, bevor versucht wird eine erneute Verbindung zu erzwingen.
<code>root/ConnectionType/freerdp/connections/<UUID>/timeoutWarning</code>	Legt die Anzahl von Millisekunden fest, die nach dem Ausfall einer Verbindung mit dem Server vergehen, bevor der Benutzer gewarnt wird, dass die Verbindung getrennt wurde.
<code>root/ConnectionType/freerdp/connections/<UUID>/timeoutWarningDialog</code>	Wenn der Wert 1 ist, dann wird ein Dialogfeld angezeigt, wenn ein Abfallen einer Ende-zu-Ende-Verbindung erkannt wird, und das Display wird grau. Andernfalls werden Nachrichten in das Verbindungsprotokoll geschrieben und die Sitzung fährt sich fest.
<code>root/ConnectionType/freerdp/connections/<UUID>/timeoutsEnabled</code>	Wenn der Wert 1 ist, dann sind die Health-Tests der Ende-zu-Ende-Verbindung abgeschlossen.
<code>root/ConnectionType/freerdp/connections/<UUID>/tlsVersion</code>	<p>Legt die Transport Layer Security-Version fest, die in den Anfangsphasen der Aushandlung mit dem RDP-Server verwendet wird. Legen Sie diese Option auf die TLS-Version Ihres RDP-Servers fest oder verwenden Sie <code>auto</code>.</p> <p>HINWEIS: Durch einige Serverfehler auf einigen ungepatchten RDP-Servern kann die automatische Einstellung zu einem Fehler führen, deshalb ist es nicht die Standardeinstellung.</p>
<code>root/ConnectionType/freerdp/connections/<UUID>/usbMiscRedirection</code>	Wenn der Wert 0 ist, ist die Umleitung für alle USB-Geräte deaktiviert, ausgenommen jener, die über <code>sound</code> , <code>printerMapping</code> , <code>portMapping</code> , <code>usbStorageRedirection</code> und <code>localPartitionRedirection</code> gehandhabt werden. Wenn der Wert 2 ist, werden alle anderen USB-Geräte zum Remotehost umgeleitet, wie im USB-Manager konfiguriert.
<code>root/ConnectionType/freerdp/connections/<UUID>/usbStorageRedirection</code>	Wenn der Wert 1 ist, werden alle USB-Speichergeräte über die <code>Storage-Erweiterung</code> zum Remote-Host weitergeleitet werden. Durch die Einstellung 0 wird die Erweiterung deaktiviert. Wenn der Wert 2 ist, werden USB-Speichergeräte entsprechend der Konfiguration im USB-Manager weitergeleitet.
<code>root/ConnectionType/freerdp/connections/<UUID>/username</code>	Legt den Standard-Benutzernamen fest, der vom Remote-Host während der Anmeldung benötigt wird. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
<code>root/ConnectionType/freerdp/connections/<UUID>/waitForNetwork</code>	Wenn der Wert 1 ist, wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor

Registrierungsschlüssel	Beschreibung
	der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
root/ConnectionType/freerdp/connections/<UUID>/windowMode	Bei einer Einstellung auf <code>Remote Application</code> wird RDP im Remote Application Integrated Local (RAIL) ausgeführt. Dies erfordert, dass der RemoteApp-Server die gewünschte Anwendung als Remoteanwendung ausführen kann. Die Anwendung wird in einem separaten Fenster innerhalb der Desktop-Umgebung angezeigt, sodass es wirkt, als wäre die Anwendung Teil des lokalen Systems. Siehe auch den Registrierungsschlüssel <code>RemoteApp</code> . Bei einer Einstellung auf <code>Alternate Shell</code> wird eine nicht-standardmäßige Shell aufgerufen. Siehe auch die Registrierungsschlüssel <code>application</code> und <code>directory</code> .
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>/x11Capture	Dies ist eine Diagnosefunktion. Wenn der Wert 1 ist, werden X11-Vorgänge für eine spätere Wiedergabe aufgezeichnet.
root/ConnectionType/freerdp/connections/<UUID>/x11CaptureDir	Dies ist eine Diagnosefunktion. Mit diesem Wert wird das Verzeichnis für X11-Aufzeichnungsdateien festgelegt.
root/ConnectionType/freerdp/connections/<UUID>/x11LogAutoflush	Dies ist eine Diagnosefunktion. Wenn der Wert 1 ist, wird die X11-Protokolldatei häufiger auf den Datenträger übertragen.
root/ConnectionType/freerdp/connections/<UUID>/x11Logfile	Dies ist eine Diagnosefunktion. Mit dem Wert wird der Pfad der X11-Protokolldatei festgelegt.
root/ConnectionType/freerdp/connections/<UUID>/x11Logging	Dies ist eine Diagnosefunktion. Wenn der Wert 1 ist, werden X11-Vorgänge protokolliert.
root/ConnectionType/freerdp/connections/<UUID>/x11Synchronous	Dies ist eine Diagnosefunktion. Wenn der Wert 1 ist, werden X11-Vorgänge nicht gepuffert.
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: <code>xfreerdp --kbd-list</code> .
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.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn Connection Manager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/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/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 Auswahlménü der Verbindungstypen angezeigt wird.
root/ConnectionType/freerdp/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/freerdp/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn <code>connection-mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
root/ConnectionType/freerdp/coreSettings/watchPid	Wenn der Wert 1 ist, wird die unter dem Namen <code>AppName</code> angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/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/coreSettings/wrapperScriptGeneration	Informiert Connection Manager darüber, welche Parametertypen dem Wrapperskript übergeben werden sollen.
root/ConnectionType/freerdp/general/autoReconnectDialogTimeout	Wenn <code>AutoReconnect</code> aktiviert ist, ist dies die Anzahl der Sekunden, bevor Fehlerdialoge für die Verbindung ein Zeitlimit erreichen. Wenn der Wert 0 ist, warten die Dialogen unbegrenzt auf eine Benutzerinteraktion.

Registrierungsschlüssel	Beschreibung
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	Wenn der Wert 1 ist, 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/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, z. B. myserver.com, wird durch den Wert im Feld Adresse der Verbindung ersetzt. Dieses Muster wird nicht verwendet, wenn die Adresse bereits eine URL ist.
root/ConnectionType/freerdp/general/sendHostname	Wenn 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 verbindungspezifischen 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.

ssh

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/connections/<UUID>/authorizations/user/edit	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
root/ConnectionType/ssh/connections/<UUID>/authorizations/user/execution	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
root/ConnectionType/ssh/connections/<UUID>/autoReconnect	Wenn der Wert 1 ist, 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 <code>autoReconnect</code> 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 <code>autostart</code> 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 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.

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

Registrierungsschlüssel	Beschreibung
	angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/ssh/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
root/ConnectionType/ssh/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn <code>connection-mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
root/ConnectionType/ssh/coreSettings/watchPid	Wenn der Wert 1 ist, wird die unter dem Namen <code>AppName</code> angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/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	Zum Einstellen des Status für das Widget Adresse in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/application	Zum Einstellen des Status für das Widget Anwendung ausführen in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/autoReconnect	Zum Einstellen des Status für das Widget Automatische Verbindungswiederherstellung in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget

Registrierungsschlüssel	Beschreibung
	ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/autostart</code>	Zum Einstellen des Status für das Widget Autostart Priorität in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/backgroundColor</code>	Zum Einstellen des Status für das Widget Hintergrundfarbe in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/compression</code>	Zum Einstellen des Status für das Widget Komprimierung in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/fallBackConnection</code>	Zum Einstellen des Status für das Widget Alternative Verbindung in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/font</code>	Zum Einstellen des Status für das Widget Schriftart in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/foregroundColor</code>	Zum Einstellen des Status für das Widget Vordergrundfarbe in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/fork</code>	Zum Einstellen des Status für das Widget Ausführung im Hintergrund in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/hasDesktopIcon</code>	Zum Einstellen des Status für das Widget Symbol auf Desktop anzeigen in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die

Registrierungsschlüssel	Beschreibung
	Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/isInMenu</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/label</code>	Zum Einstellen des Status für das Widget Name in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/port</code>	Zum Einstellen des Status für das Widget Port in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/tty</code>	Zum Einstellen des Status für das Widget TTY-Zuordnung erzwingen in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/username</code>	Zum Einstellen des Status für das Widget Benutzername in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/waitForNetwork</code>	Zum Einstellen des Status für das Widget Vor der Anmeldung auf Netzwerkverbindung warten in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/x11</code>	Zum Einstellen des Status für das Widget X11-Verbindungsweiterleitung in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/teemtalk/authorizations/user/add	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/teemtalk/authorizations/user/general	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/teemtalk/connections/<UUID>/afterStartedCommand	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/teemtalk/connections/<UUID>/afterStoppedCommand	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
root/ConnectionType/teemtalk/connections/<UUID>/authorizations/user/edit	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
root/ConnectionType/teemtalk/connections/<UUID>/authorizations/user/execution	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
root/ConnectionType/teemtalk/connections/<UUID>/autoReconnect	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
root/ConnectionType/teemtalk/connections/<UUID>/autostart	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
root/ConnectionType/teemtalk/connections/<UUID>/beforeStartingCommand	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/teemtalk/connections/<UUID>/connectionEndAction	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/teemtalk/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/teemtalk/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/teemtalk/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/teemtalk/connections/<UUID>/isInMenu	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf Default Connection eingestellt und wird in der Benutzeroberfläche nicht angezeigt.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/teemtalk/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/teemtalk/connections/<UUID>/systembeep	Wenn der Wert 1 ist, dann sind Systemsignale für die Verbindung aktiviert.
root/ConnectionType/teemtalk/connections/<UUID>/ttsName	Gibt den TeemTalk Profilnamen an.
root/ConnectionType/teemtalk/connections/<UUID>/waitForNetwork	Wenn der Wert 1 ist, wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
root/ConnectionType/teemtalk/coreSettings/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
root/ConnectionType/teemtalk/coreSettings/appName	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/className	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn Connection Manager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/generalSettingsEditor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/icon16Path	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
root/ConnectionType/teemtalk/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
root/ConnectionType/teemtalk/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
root/ConnectionType/teemtalk/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlménü der Verbindungstypen angezeigt wird.
root/ConnectionType/teemtalk/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/teemtalk/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
root/ConnectionType/teemtalk/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn <code>connection-mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist

Registrierungsschlüssel	Beschreibung
	dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
<code>root/ConnectionType/teemtalk/coreSettings/wrapperScript</code>	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/name</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/status</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/title</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autoReconnect</code>	Zum Einstellen des Status für das Widget Automatische Verbindungswiederherstellung in TeemTalk Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autostart</code>	Zum Einstellen des Status für das Widget Autostart Priorität in TeemTalk Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/hasDesktopIcon</code>	Zum Einstellen des Status für das Widget Symbol auf Desktop anzeigen in TeemTalk Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/isInMenu</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/label</code>	Zum Einstellen des Status für das Widget Name in TeemTalk Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/waitForNetwork</code>	Zum Einstellen des Status für das Widget Vor der Anmeldung auf Netzwerkverbindung warten in TeemTalk Connection Manager.

Registrierungsschlüssel	Beschreibung
	Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

telnet

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/telnet/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/telnet/connections/<UUID>/font	Gibt die Schriftgröße für die Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/foregroundColor	Gibt die Vordergrundfarbe der Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/telnet/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/telnet/connections/<UUID>/locale	Gibt das Gebietsschema der Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/port	Gibt die Portnummer an, die bei der Verbindungsherstellung mit dem Server verwendet wird. Die Standardeinstellung ist 23.
root/ConnectionType/telnet/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/telnet/connections/<UUID>/waitForNetwork	Wenn der Wert 1 ist, wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
root/ConnectionType/telnet/coreSettings/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
root/ConnectionType/telnet/coreSettings/appName	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/className	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn Connection Manager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/generalSettingsEditor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/icon16Path	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
root/ConnectionType/telnet/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/telnet/gui/TelnetManager/widgets/autostart	Zum Einstellen des Status für das Widget Autostart Priorität in Telnet Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/backgroundColor	Zum Einstellen des Status für das Widget Hintergrundfarbe im Telnet-Verbindungs-Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/fallBackConnection	Zum Einstellen des Status für das Widget Alternative Verbindung in Telnet Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/foregroundColor	Zum Einstellen des Status für das Widget Vordergrundfarbe im Telnet-Verbindungs-Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/hasDesktopIcon	Zum Einstellen des Status für das Widget Symbol auf Desktop anzeigen im Telnet-Verbindungs-Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/label	Zum Einstellen des Status für das Widget Name in Telnet Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/port	Zum Einstellen des Status für das Widget Port im Telnet-Verbindungs-Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/waitForNetwork	Zum Einstellen des Status für das Widget Vor der Anmeldung auf Netzwerkverbindung warten in Telnet Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/view/authorizations/user/add</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/view/authorizations/user/commandLineBox</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Eingeben von Befehlszeilenargumenten in VMware Horizon View Connection Manager.
<code>root/ConnectionType/view/authorizations/user/general</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/view/connections/<UUID>/ExtraArgs</code>	Gibt zusätzliche Argumente zum VMware Horizon View-Client an. Führen Sie <code>view_client --help</code> oder <code>vmware-view --help</code> über ein X-Terminal aus, um alle verfügbaren Argumente anzuzeigen.
<code>root/ConnectionType/view/connections/<UUID>/SingleSignOn</code>	
<code>root/ConnectionType/view/connections/<UUID>/afterStartedCommand</code>	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/view/connections/<UUID>/afterStoppedCommand</code>	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/view/connections/<UUID>/appInMenu</code>	Wenn der Wert 1 ist, werden alle Anwendungen für diese Verbindung im Menü der Taskleiste angezeigt.
<code>root/ConnectionType/view/connections/<UUID>/appOnDesktop</code>	Wenn der Wert 1 ist, werden alle Anwendungen für diese Verbindung auf dem Desktop angezeigt.
<code>root/ConnectionType/view/connections/<UUID>/applicationSize</code>	Legt die Größe fest, in der VMware Horizon View-Client Anwendungen startet.
<code>root/ConnectionType/view/connections/<UUID>/attachToConsole</code>	
<code>root/ConnectionType/view/connections/<UUID>/authorizations/user/edit</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
<code>root/ConnectionType/view/connections/<UUID>/authorizations/user/execution</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
<code>root/ConnectionType/view/connections/<UUID>/autoReconnect</code>	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
<code>root/ConnectionType/view/connections/<UUID>/autoReconnectDelay</code>	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn <code>autoReconnect</code> auf 1 eingestellt ist.
<code>root/ConnectionType/view/connections/<UUID>/automaticLogin</code>	Wenn der Wert 1 ist, dann wird der VMware Horizon View-Client versuchen, sich automatisch anzumelden, wenn alle Felder zur Verfügung stehen. Wenn der Wert 0 ist, müssen Benutzer im VMware Horizon View-Client manuell Verbinden auswählen, sich anmelden und einen Desktop auswählen.
<code>root/ConnectionType/view/connections/<UUID>/autostart</code>	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/<UUID>/autostartDelay	Gibt die Wartezeit in Sekunden an, bevor die Verbindung beim Systemstart gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Systemstart gestartet. Diese Einstellung wird nur wirksam, wenn <code>autostart</code> auf 1 eingestellt ist.
root/ConnectionType/view/connections/<UUID>/beforeStartingCommand	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/view/connections/<UUID>/closeAfterDisconnect	Wenn der Wert 1 ist, wird die Verbindung beendet, nachdem der erste Desktop geschlossen wurde. Wenn der Wert 0 ist, wird der VMware Horizon View-Client zum Desktop-Auswahl-Bildschirm zurückkehren. Dies ist standardmäßig aktiviert, um zu verhindern, dass Benutzer versehentlich die Verbindung auf dem Desktop-Auswahl-Bildschirm bestehen lassen, nachdem sie sich abgemeldet haben.
root/ConnectionType/view/connections/<UUID>/closeAfterRoaming	Wenn der Wert 1 ist, wird die VMware-Verbindung nach einem nach einem Roaming-Vorgang getrennt.
root/ConnectionType/view/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/view/connections/<UUID>/credentialsType	Gibt den Anmeldeinformationstyp abhängig davon an, ob die Anmeldeinformationen durch <code>anonymous</code> (nicht authentifizierter Zugriff), <code>sso</code> (einmaliges Anmelden), <code>startup</code> (Anmeldeinformationen werden beim Start abgefragt), <code>password</code> (vorkonfigurierte(r/s) Benutzer/Domäne/Kennwort) oder <code>smartcard</code> (vorkonfigurierte Smart Card) bereitgestellt werden sollen.
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>/enableMMR	Wenn der Wert 1 ist, wird die <code>Multimedia Redirection</code> aktiviert, sodass unterstützte Codecs, die über den Windows Media Player abgespielt werden, an den Client umgeleitet werden. Dies verbessert die Videowiedergabe im Vollbild- und High-Definition-Modus für Codecs wie z. B. WMV9, VC1 und MPEG4 erheblich.
root/ConnectionType/view/connections/<UUID>/enableSingleMode	

Registrierungsschlüssel	Beschreibung
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	Wenn der Wert 1 ist, wird die obere Menüleiste innerhalb des Desktops ausgeblendet. Diese Leiste wird zur Verwaltung von Remote-Geräten und zum Starten anderer Desktops verwendet.
root/ConnectionType/view/connections/<UUID>/isInMenu	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/view/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/view/connections/<UUID>/lockServer	Wenn der Wert 1 ist, können Endbenutzer die Serveradresse nicht ändern.
root/ConnectionType/view/connections/<UUID>/loginfields/domain	Wenn der Wert 1 ist, wird das Feld 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 Kennwort im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/view/connections/<UUID>/loginfields/rememberme	Wenn der Wert 1 ist, wird das Kontrollkästchen 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 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-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 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.

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

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/audioLatency</code>	Legt den durchschnittlichen Offset in Millisekunden zwischen dem Audiostream und der Anzeige der entsprechenden Videoframes nach dem Entschlüsseln fest.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/clipboardExtension</code>	Wenn der Wert 1 ist, ist die Zwischenablage sowohl zwischen verschiedenen RDP-Sitzungen als auch zwischen RDP-Sitzungen und dem lokalen System aktiviert.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/colorDepth</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/compression</code>	Wenn der Wert 1 ist, wird die Komprimierung von RDP-Daten zwischen dem Client und dem Server aktiviert.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/disableMMRwithRFX</code>	Wenn die Einstellung 1 ist, wird die Multimedia-Umleitung deaktiviert, wenn eine gültige RemoteFX-Sitzung aufgebaut wurde.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/frameAcknowledgeCount</code>	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. Wenn der Wert 0 ist, wird die Frame-Bestätigung bei den Client-Server-Interaktionen nicht verwendet.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname</code>	Wenn <code>hostname</code> eingestellt ist, wird der System-Hostname an den Remote-Host gesendet. Dies wird in der Regel verwendet, um den mit einer bestimmten RDP-Sitzung verknüpften Thin Client zu identifizieren. Der gesendete Host-Name kann mit <code>sendHostname</code> in den verbindungspezifischen Einstellungen außer Kraft gesetzt werden. Bei der Einstellung <code>mac</code> wird die MAC-Adresse des ersten verfügbaren Netzwerkadapters anstelle des Hostnamen gesendet.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/loadBalanceInfo</code>	Dieser Wert ist der Lastenausgleich-Cookie, der zu Vermittlungszwecken beim Herstellen einer Verbindung an den Server gesendet wird und entspricht dem Feld <code>Loadbalanceinfo</code> in der Datei <code>.rdp</code> . Der Standardwert ist leer.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/mouseMotionEvents</code>	Wenn der Wert 0 ist, Mausbewegungsereignisse nicht an den Server gesendet. Dies kann dazu führen, dass einige Benutzerfeedbacks, wie z. B. Quickinfos, nicht richtig funktionieren.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/offScreenBitmaps</code>	Wenn der Wert 0 ist, Off-Screen-Bitmaps deaktiviert. Dies kann die Leistung etwas erhöhen, bewirkt aber, dass die Bildschirmblöcke asynchron aktualisiert werden, wodurch auch Übergänge nicht gleichmäßig aktualisiert werden.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagDesktopComposition</code>	Wenn der Wert 1 ist, ist die Desktopgestaltung (wie durchsichtige Rahmen) möglich, sofern dies vom Server unterstützt wird. Das Ausschalten der Desktopgestaltung kann die Leistung für Verbindungen mit niedriger Bandbreite verbessern. Im Allgemeinen betrifft dies nur RemoteFX. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagFontSmoothing</code>	Wenn der Wert 1 ist, ist die Schriftglättung möglich, sofern dies vom Server unterstützt wird und aktiviert ist. Das Ausschalten dieser Option kann die Leistung bei Verbindungen mit niedriger

Registrierungsschlüssel	Beschreibung
	Bandbreite verbessern. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoCursorSettings	Wenn der Wert 1 ist, wird das Blinken des Cursors deaktiviert, 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	Wenn der Wert ist, wird der Mauscursor-Schatten deaktiviert, 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	Wenn der Wert 1 ist, werden die Menüanimationen deaktiviert, 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	Wenn der Wert 1 ist, werden die Designs der Benutzeroberfläche deaktiviert, 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	Wenn der Wert 1 ist, werden die Desktop-Hintergrundbilder deaktiviert, 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	Wenn der Wert 1, wird die Option zum Ziehen von Fenstern mit vollem Inhalt deaktiviert, 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/view/connections/<UUID>/xfreerdpOptions/portMapping	Wenn der Wert 1 ist, 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	Wenn der Wert 1 ist, 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

Registrierungsschlüssel	Beschreibung
	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>/redirectPreference	Zur Umleitung erhält der RDP-Client verschiedene mögliche Ziele. Diese werden normalerweise in der folgenden Reihenfolge ausprobiert: FQDN, primäre IP, IP-Liste, NetBIOS. Wenn FQDN nicht gewünscht ist, kann eine der Alternativen zuerst ausprobiert werden, indem dieser Registrierungsschlüssel festgelegt wird. Wenn diese Methode nicht funktioniert, wird auf dem RDP-Client wieder die ursprüngliche Reihenfolge herangezogen. Mit der Einstellung <code>auto</code> wird die ursprüngliche Reihenfolge erzwungen.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/remoteFx	Wenn der Wert 1 ist, dann wird RemoteFX verwendet, wenn verfügbar.
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 <code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname</code> muss auf <code>hostname</code> eingestellt sein, damit diese Taste verwendet werden kann.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sound	Durch die Standardeinstellung <code>Bring to this computer</code> wird der Sound mithilfe eines virtuellen Kanals vom Remote-Host zum Client umgeleitet. Durch die Einstellung <code>Leave at remote computer</code> verbleibt der Sound am Remote-Host. Dies kann nützlich sein, wenn ein USB-umgeleitetes Audiogerät verwendet wird. Durch die Einstellung auf irgendeinen anderen Wert, wird Audio deaktiviert. In der Regel empfiehlt HP, den Wert <code>Bring to this computer</code> einzustellen und USB-Wiedergabegeräte nicht zum Remote-Host umzuleiten. Dadurch wird die Audioqualität verbessert und sichergestellt, dass Client-Audio, das mittels anderer Methoden umgeleitet wird (wie zum Beispiel <code>Multimedia Redirection</code>), den lokalen Audioeinstellungen entspricht.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/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/view/connections/<UUID>/xfreerdpOptions/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/view/connections/<UUID>/xfreerdpOptions/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/view/connections/<UUID>/xfreerdpOptions/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 fort.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutsEnabled	Wenn der Wert 1 ist, dann sind die Health-Tests der Ende-zu-Ende-Verbindung abgeschlossen.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/tlsVersion	<p>Legt die Transport Layer Security-Version fest, die in den Anfangsphasen der Aushandlung mit dem RDP-Server verwendet wird. Legen Sie diese Option auf die TLS-Version Ihres RDP-Servers fest oder verwenden Sie „auto“.</p> <p>HINWEIS: Durch einige Serverfehler auf einigen ungepatchten RDP-Servern kann die automatische Einstellung zu einem Fehler führen, deshalb ist es nicht die Standardeinstellung.</p>
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: <code>xfreerdp --kbd-list</code> .
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 Connection Manager 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 Auswahlménü der Verbindungstypen angezeigt wird.
root/ConnectionType/view/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/view/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
root/ConnectionType/view/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn <code>connection-mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein

Registrierungsschlüssel	Beschreibung
	benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
<code>root/ConnectionType/view/coreSettings/watchPid</code>	Wenn der Wert 1 ist, wird die unter dem Namen <code>AppName</code> angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/view/coreSettings/wrapperScript</code>	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/view/coreSettings/wrapperScriptGeneration</code>	Informiert Connection Manager darüber, welche Parametertypen dem Wrapperskript übergeben werden sollen.
<code>root/ConnectionType/view/general/rdpOptions</code>	Die hier angegebenen Optionen werden direkt an den RDP-Client weitergeleitet, wenn RDP als Anzeigeprotokoll für die VMware Horizon View-Verbindung verwendet wird. Um eine vollständige Liste der Optionen anzuzeigen, geben Sie den folgenden Befehl in ein X-Terminal ein: <code>rdesktop --help</code>
<code>root/ConnectionType/view/gui/viewManager/name</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/view/gui/viewManager/status</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/view/gui/viewManager/title</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/view/gui/viewManager/widgets/autostart</code>	Zum Einstellen des Status für das Widget Autostart Priorität in VMware Horizon View Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/view/gui/viewManager/widgets/fallBackConnection</code>	Zum Einstellen des Status für das Widget Alternative Verbindung in VMware Horizon View Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/view/gui/viewManager/widgets/label</code>	Zum Einstellen des Status für das Widget Name in VMware Horizon View Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xdmcp/authorizations/user/add	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/xdmcp/authorizations/user/general	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/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, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
root/ConnectionType/xdmcp/connections/<UUID>/authorizations/user/execution	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
root/ConnectionType/xdmcp/connections/<UUID>/autoReconnect	Wenn der Wert 1 ist, 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.
root/ConnectionType/xdmcp/connections/<UUID>/fontServer	Legt die Adresse des zu verwendenden Schriftartenservers fest. Der Registrierungsschlüssel UseFontServer muss auch auf 1 eingestellt werden.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xdmcp/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/xdmcp/connections/<UUID>/isInMenu	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/xdmcp/connections/<UUID>/refreshRate	Legt die Bildwiederholungsrate für das Display der Verbindung fest.
root/ConnectionType/xdmcp/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/xdmcp/connections/<UUID>/type	Gibt den XDMCP-Verbindungstyp an. Durch die Einstellung <code>chooser</code> werden alle verfügbaren Hosts aufgelistet und der Benutzer kann wählen, zu welchem eine Verbindung hergestellt werden soll. Durch die Einstellung <code>query</code> wird eine XDMCP-Anforderung direkt zum angegebenen Host gesendet. Durch die Einstellung <code>broadcast</code> werden alle verfügbaren Hosts aufgelistet und es wird automatisch eine Verbindung mit dem ersten Host hergestellt.
root/ConnectionType/xdmcp/connections/<UUID>/useFontServer	Wenn der Wert 1 ist, wird der Schriftartenserver aktiviert. Wenn der Wert 0 ist, wird die lokale Schriftart verwendet.
root/ConnectionType/xdmcp/connections/<UUID>/waitForNetwork	Wenn der Wert 1 ist, 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.
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 Connection Manager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.

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

Registrierungsschlüssel	Beschreibung
	kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autoReconnect</code>	Zum Einstellen des Status für das Widget Automatische Verbindungswiederherstellung in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autostart</code>	Zum Einstellen des Status für das Widget Autostart Priorität in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/color</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/fontServer</code>	Zum Einstellen des Status für das Widget Schriftartenserver in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/hasDesktopIcon</code>	Zum Einstellen des Status für das Widget Symbol auf Desktop anzeigen in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/isInMenu</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/label</code>	Zum Einstellen des Status für das Widget Name in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/refreshRate</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/type</code>	Zum Einstellen des Status für das Widget Typ in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/useFontServer</code>	Zum Einstellen des Status für das Widget Schriftartenserver verwenden in XDMCP Connection Manager. Durch die Einstellung

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

xen

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/xen/authorizations/user/add</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/xen/authorizations/user/general</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/xen/connections/<UUID>/SingleSignOn</code>	Wenn der Wert 1 ist, verwendet die Verbindung die gleichen Anmeldeinformationen wie der Bildschirmschoner.
<code>root/ConnectionType/xen/connections/<UUID>/address</code>	Die Adresse des Remote-Hosts, zu dem die Verbindung hergestellt werden soll. In der Regel ist dies eine URL, wie z. B. <code>http://server.domain.com</code> .
<code>root/ConnectionType/xen/connections/<UUID>/afterStartedCommand</code>	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/xen/connections/<UUID>/afterStoppedCommand</code>	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/xen/connections/<UUID>/appInMenu</code>	Wenn der Wert 1 ist, werden alle Anwendungen für diese Verbindung im Menü der Taskleiste angezeigt.
<code>root/ConnectionType/xen/connections/<UUID>/appOnDashboard</code>	Wenn der Wert 1 ist, werden alle Anwendungen für diese Verbindung in der Taskleiste angezeigt.
<code>root/ConnectionType/xen/connections/<UUID>/appOnDesktop</code>	Wenn der Wert 1 ist, werden alle Anwendungen für diese Verbindung auf dem Desktop angezeigt.
<code>root/ConnectionType/xen/connections/<UUID>/authorizations/user/edit</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
<code>root/ConnectionType/xen/connections/<UUID>/authorizations/user/execution</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/xen/connections/<UUID>/autoLaunchSingleApp</code>	Wenn der Wert 1 ist und wenn nur eine einzige veröffentlichte Anwendung oder Desktop vom Citrix Server zurückgegeben wird, wird diese Ressource automatisch gestartet.
<code>root/ConnectionType/xen/connections/<UUID>/autoReconnect</code>	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
<code>root/ConnectionType/xen/connections/<UUID>/autoReconnectAppsOnLogin</code>	Wenn der Wert 1 ist, versucht das System nach einer Erstanmeldung alle aktiven oder getrennten Citrix Sitzungen wiederherzustellen.
<code>root/ConnectionType/xen/connections/<UUID>/autoReconnectDelay</code>	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn <code>autoReconnect</code> auf 1 eingestellt ist.
<code>root/ConnectionType/xen/connections/<UUID>/autoRefreshInterval</code>	Steuert die Zeit in Sekunden, bevor die Ressourcen gelöscht und vom Server erneut aktualisiert werden. Stellen Sie zum Deaktivieren den Wert -1 ein. Es ist in der Regel nicht erforderlich, die Ressourcen häufig vom Server zu aktualisieren.
<code>root/ConnectionType/xen/connections/<UUID>/autoStartDesktop</code>	Wenn der Wert 1 und <code>autoStartResource</code> leer ist, wird der erste Desktop, der beim Starten der Verbindung zur Verfügung steht, automatisch geöffnet.
<code>root/ConnectionType/xen/connections/<UUID>/autoStartResource</code>	Legt den Namen des Desktops oder der Anwendung fest, der oder die automatisch startet, wenn die Verbindung gestartet wird.
<code>root/ConnectionType/xen/connections/<UUID>/autostart</code>	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
<code>root/ConnectionType/xen/connections/<UUID>/autostartDelay</code>	Gibt die Wartezeit in Sekunden an, bevor die Verbindung beim Systemstart gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Systemstart gestartet. Diese Einstellung wird nur wirksam, wenn <code>autostart</code> auf 1 eingestellt ist.
<code>root/ConnectionType/xen/connections/<UUID>/beforeStartingCommand</code>	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/xen/connections/<UUID>/connectionMode</code>	Legt den Citrix Verbindungsmodus für die Verbindung fest.
<code>root/ConnectionType/xen/connections/<UUID>/connectionStopAction</code>	Definiert die auszuführende Aktion, wenn die Verbindung durch den Connection Manager beendet wird. Die verfügbaren Optionen sind <code>disconnect</code> und <code>logoff</code> .
<code>root/ConnectionType/xen/connections/<UUID>/coord</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xen/connections/<UUID>/credentialsType</code>	Gibt den Anmeldeinformationstyp abhängig davon an, ob die Anmeldeinformationen durch <code>anonymous</code> (nicht authentifizierter Zugriff), <code>sso</code> (einmaliges Anmelden), <code>startup</code> (Anmeldeinformationen werden beim Start abgefragt), <code>password</code> (vorkonfigurierte(r/s) Benutzer/Domäne/Kennwort) oder <code>smartcard</code> (vorkonfigurierte Smart Card) bereitgestellt werden sollen.
<code>root/ConnectionType/xen/connections/<UUID>/dependConnectionId</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

Registrierungsschlüssel	Beschreibung
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	Wenn der Wert 1 ist, wird die Überprüfung 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 <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/xen/connections/<UUID>/logOnMethod	
root/ConnectionType/xen/connections/<UUID>/loginfields/domain	Wenn der Wert 1 ist, wird das Feld 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 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 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 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.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/connections/<UUID>/loginfields/smartcard	Wenn der Wert 1 ist, wird das Kontrollkästchen 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 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>/resListRequest	Wenn der Wert 1 ist, listet eine Verbindung nur die Ressource auf, ohne sie zu starten oder Symbole herunterzuladen.
root/ConnectionType/xen/connections/<UUID>/saveNewUrl	Dies ist ein interner Wert. Wenn der Wert <code>ToBeAsked</code> ist, fragt das Skript den Benutzer. Wenn der Wert <code>Auto</code> ist, fragt das Skript den Benutzer nicht. Ob die URL gespeichert wird, ist fallabhängig. Wenn der Wert <code>Yes</code> ist, hat der Benutzer das Speichern der neuen URL angefordert. Wenn der Wert <code>No</code> ist, hat der Benutzer angefordert, die neue URL nicht zu speichern.
root/ConnectionType/xen/connections/<UUID>/savePassword	
root/ConnectionType/xen/connections/<UUID>/smartCardModuleKey	Gibt das Sicherheitsmodul an, das für eine Smart Card-Verbindung verwendet werden soll.
root/ConnectionType/xen/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/xen/connections/<UUID>/subscribedOnly	Wenn der Wert 1 ist, werden nur abonnierte Ressourcen für die neue Verbindung angezeigt.
root/ConnectionType/xen/connections/<UUID>/unplugSmartCardAction	Legt die Aktion fest, die durchgeführt werden soll, wenn eine Smart Card bei bestehender Verbindung entnommen wird. Mit <code>disconnect</code> wird die Verbindung der aktuellen Sitzung unterbrochen. Mit <code>close</code> werden alle geöffneten Ressourcen geschlossen. Mit <code>noaction</code> wird keine Aktion ausgeführt.
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	Wenn der Wert 1 ist, 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.

Registrierungsschlüssel	Beschreibung
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 Connection Manager 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.
root/ConnectionType/xen/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/xen/coreSettings/retryTimeout	Diese Einstellung kann angewendet werden, wenn ein virtueller Computer nicht neu gestartet wird und noch nicht verfügbar ist, um als Citrix Ressource gestartet zu werden. Wenn der Wert eine negative Zahl ist, wird nicht versucht, die Verbindung erneut herzustellen. Andernfalls gibt er den Zeitraum (in Sekunden) vor,

Registrierungsschlüssel	Beschreibung
	über den HP ThinPro versucht, die Verbindung zum virtuellen Computer erneut herzustellen.
root/ConnectionType/xen/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
root/ConnectionType/xen/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn <code>connection-mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
root/ConnectionType/xen/coreSettings/watchPid	Wenn der Wert 1 ist, wird die unter dem Namen <code>AppName</code> angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/wrapperScript	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/wrapperScriptGeneration	Informiert Connection Manager darüber, welche Parametertypen dem Wrapperskript übergeben werden sollen.
root/ConnectionType/xen/general/CGPAddress	<p>Gibt die CGP-Adresse mithilfe der Syntax <code>hostname:port</code> an.</p> <p>Optional können Sie statt des Hostnamens ein Sternchen (*) eingeben. Dadurch wird der Wert des Registrierungsschlüssels <code>address</code> der Verbindung als Host verwendet. Beispiel: <code>*:2598</code></p> <p>Die Angabe des Anschlusswerts ist optional. Wenn Sie keinen Anschlusswert angeben, wird der Standardwert 2598 verwendet. Wenn die Verbindung am Anschluss 2598 fehlschlägt, versucht der Thin Client, eine Verbindung am Anschluss 1494 herzustellen.</p>
root/ConnectionType/xen/general/TWIMode	Steuert den nahtlosen Modus für veröffentlichte Anwendungen. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>TWIMode</code> direkt zugeordnet.
root/ConnectionType/xen/general/TWIModeResizeType	Diese Einstellung ist der Citrix INI-Dateieinstellung <code>TWIMoveResizeType</code> direkt zugeordnet.
root/ConnectionType/xen/general/allowReadOnA ... allowReadOnZ	Wenn der Wert 1 ist, kann ein Benutzer das zugeordnete Laufwerk lesen.
root/ConnectionType/xen/general/allowWriteOnA ... allowWriteOnZ	Wenn der Wert 1 ist, kann ein Benutzer im zugeordneten Laufwerk auch schreiben.
root/ConnectionType/xen/general/async	Wenn der Wert 1 ist, ist die asynchrone Abfrage aktiviert. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>CommPollSize</code> direkt zugeordnet.
root/ConnectionType/xen/general/autoReconnect	Wenn der Wert 1 ist, ist das automatische Neuverbinden der Sitzung aktiviert. Dies ist nicht identisch mit dem verbindungspezifischen "autoReconnect" (automatisches Neuverbinden). Diese Neuverbindung findet intern statt, innerhalb des Citrix Clients, ohne Neustart der Verbindung. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>TransportReconnectEnabled</code> direkt zugeordnet.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/general/bitmapCacheSize	Legt die minimale Größe für die Bitmap-Zwischenspeicherung fest. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>PersistentCacheMinBitmap</code> direkt zugeordnet.
root/ConnectionType/xen/general/bottomMonitor	Legt fest, dass auf dem Bildschirmbereich des unteren Monitors der virtuelle Desktop angezeigt wird. Wenn der Wert 0 ist, wird der Monitor nicht verwendet, um den virtuellen Desktop anzuzeigen.
root/ConnectionType/xen/general/colorDepth	Erzwingt die Verwendung einer bestimmten Farbtiefe für alle Verbindungen. Dies erfolgt in der Regel entweder in speziellen Umgebungen, in denen die automatische Tiefenauswahl fehlschlägt, oder in sehr langsam Netzwerken, um eine Überlastung zu vermeiden.
root/ConnectionType/xen/general/colorMapping	Bei der Auswahl von <code>Shared - Approximate Colors</code> werden ungefähre Farben aus der Standard-Farbzordnungstabelle verwendet. Bei der Auswahl von <code>Private - Exact Colors</code> werden präzise Farben verwendet. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>ApproximateColors</code> direkt zugeordnet.
root/ConnectionType/xen/general/contentRedirection	Wenn der Wert 1 ist, dann werden Links von Web-Inhalten vom Server an den Client gesendet, so dass der Client versuchen kann, sie lokal zu öffnen.
root/ConnectionType/xen/general/defaultBrowserProtocol	Steuert das Protokoll, das verwendet wird, um den Host für die Verbindung zu finden. Wenn kein Wert angegeben wird, wird der Standardwert vom Abschnitt <code>[WFClient]</code> der <code>wfclient.ini</code> verwendet. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>BrowserProtocol</code> direkt zugeordnet.
root/ConnectionType/xen/general/drivePathMappedOnA ... drivePathMappedOnZ	Legt das Verzeichnis des lokalen Dateisystems zur Zuordnung zum Remote-Host fest. In der Regel ist dies auf <code>/media</code> eingestellt, damit alle angeschlossenen USB-Laufwerke über einen einzigen Laufwerksbuchstaben dem Remote-Host zugeordnet werden können.
root/ConnectionType/xen/general/enableAlertSound	Wenn der Wert 1 ist, sind Windows Warntöne aktiviert. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>DisableSound</code> direkt zugeordnet.
root/ConnectionType/xen/general/enableClipboard	Wenn der Wert 1 ist, wird die Umleitung der Zwischenablage aktiviert.
root/ConnectionType/xen/general/enableConnectionBar	Wenn der Wert 1 ist, wird Citrix Desktop Viewer in der Sitzungsbenutzeroberfläche aktiviert. Standardmäßig lautet der Wert auf der Client-Seite 0 (deaktiviert), da dieser Wert auf dem Client durch die ICA-Datei für eine Desktop-Sitzung festgelegt wird.
root/ConnectionType/xen/general/enableCursorColors	Wenn der Wert 1 ist, werden farbige Cursor aktiviert. Wenn der Wert 0 ist, 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 <code>Compress</code> direkt zugeordnet.
root/ConnectionType/xen/general/enableDriveMapAndRedirect	Wenn der Wert 1 ist, werden Zuordnung und Umleitung von USB-Speichergeräten aktiviert.
root/ConnectionType/xen/general/enableDriveMapping	Wenn der Wert 1 ist, können Verzeichnisse auf dem lokalen Dateisystem über ein virtuelles Laufwerk zum Remote-Host

Registrierungsschlüssel	Beschreibung
	weitergeleitet werden. Typischerweise würde <code>/media</code> zu <code>Z</code> zugeordnet werden, um ein Weiterleiten von USB-Laufwerken zum Remote-Host zu ermöglichen. Wenn die USB-Umleitung aktiviert ist, sollte diese deaktiviert werden, um Speicherkonflikte zu verhindern. Um auf diese Weise korrekt dem Remote-Host zugeordnet werden zu können, muss das USB-Gerät eines der folgenden Dateisysteme verwenden: FAT32, NTFS, ext2, ext3.
<code>root/ConnectionType/xen/general/enableDynamicDriveMapping</code>	Wenn der Wert 1 ist, werden USB-Speichergeräte auf dem Citrix Server dynamisch zugeordnet. Wenn der Wert 0 ist, ist die Speichererweiterung für die USB-Speichergeräte deaktiviert.
<code>root/ConnectionType/xen/general/enableH264Compression</code>	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.
<code>root/ConnectionType/xen/general/enableHDXFlashRedirection</code>	<p>HINWEIS: Diese Funktion wird nur für die 32-Bit-Version von HP ThinPro unterstützt.</p> <p>Steuert das Verhalten der HDX Flash-Umleitung. Wenn <code>Always</code> eingestellt ist, dann wird, wenn möglich, die HDX Flash-Umleitung verwendet und der Benutzer wird nicht aufgefordert. Wenn <code>Ask</code> eingestellt ist, dann wird der Benutzer aufgefordert. Durch die Einstellung <code>Never</code> wird diese Funktionalität deaktiviert.</p>
<code>root/ConnectionType/xen/general/enableHDXFlashServerContentFetch</code>	<p>HINWEIS: Diese Funktion wird nur für die 32-Bit-Version von HP ThinPro unterstützt.</p> <p>Steuert das Verhalten des Side Content Fetching (Abrufen der Seiteninhalte) des HDX Flash Servers. Wenn deaktiviert, wird der Client Inhalte abrufen.</p>
<code>root/ConnectionType/xen/general/enableHDXMediaStream</code>	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.
<code>root/ConnectionType/xen/general/enableHWH264</code>	Wenn der Wert 1 ist und auch <code>enableH264Compression</code> 1 ist, wird die Hardwarekomprimierung für H.264 aktiviert. Wenn der Wert 0 ist, wird die H.264 Komprimierung von Software bearbeitet.
<code>root/ConnectionType/xen/general/enableMapOnA ... enableMapOnZ</code>	<p>Wenn hier der Wert 1 eingestellt wird, kann diesem Laufwerk auf dem Remote-Host ein lokales Dateisystem zugeordnet werden. Der entsprechende Registrierungsschlüssel <code>DrivePathMappedOn</code> muss auf ein gültiges lokales Verzeichnis eingestellt sein, damit die Laufwerkszuordnung einwandfrei funktioniert.</p>
<code>root/ConnectionType/xen/general/enableMultiMedia</code>	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 den Multimedia-Inhalten im Abschnitt für virtuelle Kanäle der Citrix INI-Dateieinstellungen direkt zugeordnet. Aktivieren Sie diese Einstellung, wenn HDX MediaStream aktiviert ist.
<code>root/ConnectionType/xen/general/enableOffScreenSurface</code>	Wenn der Wert 1 ist, dann kann der Server das Format <code>X PixMap</code> für Offscreen-Zeichnungen verwenden. Reduziert die Bandbreite in 15-Bit- und 24-Bit-Farbe auf Kosten des X-Serverspeichers und der Prozessorzeit. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>EnableOSS</code> direkt zugeordnet.

Registrierungsschlüssel	Beschreibung
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.
root/ConnectionType/xen/general/enableSmartCard	Wenn der Wert 1 ist, 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/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

Registrierungsschlüssel	Beschreibung
	nur der Local Area Network Linkstatus überwacht. Wenn die Einstellung <code>Server online status</code> gewählt wurde, dann werden sowohl der Local Area Network Linkstatus und die Server-Konnektivität überwacht.
<code>root/ConnectionType/xen/general/mouseClickFeedback</code>	Steuert die Maus-Latenzreduktion. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>ZLMouseMode</code> indirekt zugeordnet.
<code>root/ConnectionType/xen/general/mouseMiddleButtonPaste</code>	Wenn der Wert 1 ist, dann ist die mittlere Maustaste zum Einfügen der Emulation für Windows Sitzungen aktiviert. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>MouseSendsControlV</code> direkt zugeordnet.
<code>root/ConnectionType/xen/general/noInfoBox</code>	Wenn der Wert 1 ist, dann wird der Client Manager (Wfcmgr) nicht angezeigt, wenn eine Clientsitzung beendet wird. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>PopupOnExit</code> direkt zugeordnet.
<code>root/ConnectionType/xen/general/printerAutoCreation</code>	Durch die Einstellung 0 wird die Druckerzuordnung deaktiviert. Wenn der Wert 1 ist, dann werden lokal definierte Drucker der Verbindung zugeordnet. Wenn der Wert 2 ist, werden USB-Drucker entsprechend der Konfiguration im USB-Manager weitergeleitet.
<code>root/ConnectionType/xen/general/proxyAddress</code>	Die zu verwendende Proxy-Adresse, wenn eine manuelle Proxy-Einstellung über <code>proxyType</code> ausgewählt ist.
<code>root/ConnectionType/xen/general/proxyPassword</code>	Das zu verwendende Proxy-Kennwort, wenn eine manuelle Proxy-Einstellung über <code>proxyType</code> ausgewählt ist. Dieses Kennwort wird mithilfe der rc4-Verschlüsselung verschlüsselt.
<code>root/ConnectionType/xen/general/proxyPort</code>	Der zu verwendende Proxy-Port, wenn eine manuelle Proxy-Einstellung über <code>proxyType</code> ausgewählt ist.
<code>root/ConnectionType/xen/general/proxyType</code>	Wählt den Proxy-typ, der für die XenDesktop-Verbindungen verwendet wird. <code>Use Browser settings</code> wird nur unterstützt, wenn ein lokaler Browser installiert ist.
<code>root/ConnectionType/xen/general/proxyUser</code>	Der zu verwendende Proxy-Benutzername, wenn eine manuelle Proxy-Einstellung über <code>proxyType</code> ausgewählt ist.
<code>root/ConnectionType/xen/general/rightMonitor</code>	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.
<code>root/ConnectionType/xen/general/saveLogs</code>	Wenn der Wert 1 ist, werden detaillierte Protokollinformationen gespeichert, nachdem die Sitzung beendet wurde. Diese Protokollinformationen werden im folgenden Verzeichnis gespeichert: <code>/tmp/debug/citrix/<Datum>/</code>
<code>root/ConnectionType/xen/general/serverCheckTimeout</code>	
<code>root/ConnectionType/xen/general/sessionReliabilityTTL</code>	Gibt das Zeitlimit für die Sitzungszuverlässigkeit in Sekunden an. Damit wird die Gültigkeitsdauer der Sitzungszuverlässigkeit konfiguriert.
<code>root/ConnectionType/xen/general/sessionSharingClient</code>	Wenn der Wert 1 ist,, werden Anforderungen zur Sitzungsfreigabe an andere Citrix Sitzungen auf dem gleichen X-Display gesendet. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>EnableSessionSharingClient</code> direkt zugeordnet.

Registrierungsschlüssel	Beschreibung
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.
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	Wenn der Wert 1 ist, 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.

Registrierungsschlüssel	Beschreibung
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 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	Wenn der Wert 1 ist, 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 windowHeight 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.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/gui/XenManager/widgets/domain	Zum Einstellen des Status für das Widget Domäne in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xen/gui/XenManager/widgets/fallBackConnection	Zum Einstellen des Status für das Widget Alternative Verbindung in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xen/gui/XenManager/widgets/folder	
root/ConnectionType/xen/gui/XenManager/widgets/hasDesktopIcon	Zum Einstellen des Status für das Widget Symbol auf Desktop anzeigen in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xen/gui/XenManager/widgets/label	Zum Einstellen des Status für das Widget Name in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xen/gui/XenManager/widgets/password	Zum Einstellen des Status für das Widget Kennwort in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xen/gui/XenManager/widgets/username	Zum Einstellen des Status für das Widget Benutzername in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xen/gui/XenManager/widgets/waitForNetwork	Zum Einstellen des Status für das Widget Vor der Anmeldung auf Netzwerkverbindung warten in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xen/gui/fbpanel/autohide	Wenn der Wert <code>true</code> ist, dann wird automatisch die Taskleiste ausgeblendet.

Registrierungsschlüssel	Beschreibung
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 <code>autoStartResource</code> oder <code>autoStartDesktop</code> aktiviert ist.

DHCP

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

Dashboard



HINWEIS: Das Dashboard entspricht der Taskleiste.

Registrierungsschlüssel	Beschreibung
root/Dashboard/GUI/Clock	Wenn der Wert 1 ist, wird die Uhr in der Taskleiste angezeigt.
root/Dashboard/GUI/ConnectionManager	Wenn der Wert 1 ist, wird der HP Connection Manager in der Taskleiste angezeigt.
root/Dashboard/GUI/ControlPanel	Wenn der Wert 1 ist, wird die Systemsteuerung in der Taskleiste angezeigt.
root/Dashboard/GUI/DomainUser	Wenn der Wert 1 ist, wird das Symbol für den Domänenbenutzer in der Taskleiste angezeigt, wenn sich das System im Domänenanmeldemodus befindet.
root/Dashboard/GUI/PowerButton	Wenn der Wert 1 ist, wird die Schaltfläche „Ein/Aus“ in der Taskleiste angezeigt.
root/Dashboard/GUI/PowerButtonPosition	Wenn der Wert 1 ist, wird die Ein/Aus-Taste rechts in einer horizontalen und unten in einer vertikalen Taskleiste angezeigt. Wenn der Wert 0 ist, wird die Ein/Aus-Taste links in einer horizontalen und oben in einer vertikalen Taskleiste angezeigt.
root/Dashboard/GUI/Search	Wenn der Wert 1 ist, wird die Schaltfläche „Suchen“ in der Taskleiste angezeigt.
root/Dashboard/GUI/SystemInformation	Wenn der Wert 1 ist, wird die Schaltfläche „Systeminformation“ in der Taskleiste angezeigt.
root/Dashboard/GUI/SystemTray	Wenn der Wert 1 ist, wird der Infobereich in der Taskleiste angezeigt.
root/Dashboard/GUI/TaskBar	Wenn der Wert 1 ist, dann wird der Anwendungsbereich in 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.

Registrierungsschlüssel	Beschreibung
root/Dashboard/General/EnterLeaveTimeout	Legt die Dauer in Millisekunden fest, bevor die Taskleiste ausgeblendet bzw. einblendet wird, wenn <code>AutoHide</code> aktiviert ist.
root/Dashboard/General/IconSize	Regelt die Größe der Symbole in der Taskleiste.
root/Dashboard/General/Length	Legt die Länge der Taskleiste fest.
root/Dashboard/General/LengthToScreenSide	Wenn der Wert 1 ist, ist die Länge der Taskleiste fest und entspricht der Länge der Bildschirmseite, an der sie angeheftet ist.
root/Dashboard/General/PanelDockSide	Legt die Seite des Bildschirms fest, an der die Taskleiste angedockt ist.
root/Dashboard/General/RemainPixel	Legt die Anzahl an Pixeln fest, die sichtbar sind, wenn die Taskleiste ausgeblendet ist.
root/Dashboard/General/SlidingTimeout	Legt die Dauer in Millisekunden fest, die benötigt werden, um die Taskleiste ein- oder auszublenden, wenn <code>AutoHide</code> aktiviert ist.
root/Dashboard/General/Width	Legt die Breite der Taskleiste fest.

Display

Registrierungsschlüssel	Beschreibung
root/Display/Configuration/Hotplug/newMonitorPosition	Auf unterstützten Plattformen wird damit festgelegt, wo neue Monitore platziert werden sollten (entweder links oder rechts der bereits angeschlossenen Monitore), wenn sie per Hot-Plug verbunden sind.
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 <code>Standard</code> eingestellt werden.
root/Display/Configuration/quaternarymode	Legt die Position des vierten Monitors im Verhältnis des in <code>Quaternaryrelative</code> angegebenen Monitors fest. Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. Werte sind wie folgt definiert: 0 = identisch; 1 = Oben; 2 = Rechts daneben; 3 = Links daneben; 4 = Unten.
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.

Registrierungsschlüssel	Beschreibung
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 <code>tertiaryrelative</code> angegebenen Monitors fest. Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. Werte sind wie folgt definiert: 0 = identisch; 1 = Oben; 2 = Rechts daneben; 3 = Links daneben; 4 = Unten.
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 <code>ffffff</code> 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, dann wird die Auflösung automatisch erkannt.
root/Display/Profiles/<UUID>/label	Legt den Profilnamen in der Anzeige fest. Für Smart Zero muss dies immer auf <code>Standard</code> eingestellt werden.
root/Display/Profiles/<UUID>/orientation	Legt die Monitorausrichtung wie folgt fest: 0 = Normal; 1 = Nach links drehen; 2 = Nach rechts drehen; 3 = Invertieren.
root/Display/Profiles/<UUID>/refresh	Gibt die gewünschte Bildwiederholungsrate für den Monitor an. Nicht alle Bildwiederholungsrate werden für alle Auflösungen unterstützt. Wenn der Wert 0 ist, dann wird die Aktualisierungsrate automatisch erkannt. Die unterstützten Werte sind abhängig vom Monitor. Das Einrichten einer Aktualisierungsrate, die von dem angeschlossenen Monitor nicht unterstützt wird, wird zu einem schwarzen Bildschirm führen. HP empfiehlt, diese Einstellung auf 0 zu lassen.

Registrierungsschlüssel	Beschreibung
root/Display/Profiles/<UUID>/width	Legt die gewünschte Monitor-Auflösungsbreite fest. Wenn der Wert 0 ist, dann wird die Auflösung automatisch erkannt.
root/Display/userLock	Wenn der Wert 1 ist und die Anzeigeeinstellungen vom Benutzer geändert wurden, werden die Anzeigeeinstellungen beim Import eines Clientprofils beibehalten.
root/Display/userLockEngaged	Dieser Registrierungsschlüssel wird automatisch auf 1 gesetzt, nachdem die Anzeigeeinstellungen vom Benutzer geändert wurden. Sie müssen diese Einstellung in der Regel nicht ändern.

Domain

Registrierungsschlüssel	Beschreibung
root/domain/OU	Gibt die mit der Domänenmitgliedschaft des Thin Client verknüpften Organisationseinheit an.
root/domain/allowSmartcard	Diese Taste ist derzeit nicht nutzbar.
root/domain/cacheDomainLogin	Wenn diese Option aktiviert ist, wird ein Hash mit Domänenanmeldeinformationen auf dem Datenträger gespeichert, sodass spätere Anmeldungen auch dann erfolgen können, wenn kein Zugriff auf den Active Directory Server möglich ist.
root/domain/ddns	Wenn diese Option aktiviert ist, versucht der Thin Client, den DNS-Server während jeder DHCP-Erneuerung über Aktualisierungen seines Hostnamens und seiner IP-Adresse zu informieren.
root/domain/domain	Gibt die Domäne an, der dieser Thin Client beigetreten ist oder mit der er sich authentifiziert.
root/domain/domainAdminGroup	Wenn <code>enableDomainAdmin</code> aktiviert ist, können Mitglieder dieser AD-Gruppe den Thin Client in den Administratormodus versetzen.
root/domain/domainControllers	Gibt eine durch Kommas getrennte Liste von Domänencontrollern an, die mit dieser Domäne verwendet werden sollen. Wenn das Feld leer gelassen wird (empfohlen), wird die automatische Suche nach Domänencontrollern stattdessen mithilfe von DNS durchgeführt.
root/domain/domainJoined	Gibt an, ob der Thin Client formell zur Domäne hinzugefügt wurde.
root/domain/domainUsersGroup	Wenn <code>enableDomainUsers</code> aktiviert ist, werden Domänenanmeldungen auf direkte Mitglieder dieser Gruppe beschränkt. Geschachtelte Gruppen werden für diese Funktion nicht unterstützt.
root/domain/enableDomainAdmin	Wenn der Wert 1 ist, können Mitglieder der Gruppe unter <code>domainAdminGroup</code> den Thin Client in den Administratormodus versetzen. Wenn der Wert 0 ist, muss das lokale Stammkonto verwendet werden, um lokale administrative Aufgaben auszuführen.
root/domain/enableDomainUsers	Wenn der Wert 1 ist, sind Domänenanmeldungen auf Mitglieder der Gruppe unter <code>domainUserGroup</code> beschränkt. Wenn der Wert 0 ist, ist die Anmeldung am Thin Client mit jeglichen gültigen Domänenanmeldeinformationen möglich.

Registrierungsschlüssel	Beschreibung
root/domain/enablePasswordChange	Wenn der Wert 1 ist, kann der Benutzer sein Domänenkennwort direkt über den Thin Client ändern.
root/domain/enableSSO	Wenn diese Option aktiviert ist, werden verschlüsselte aktuelle Anmeldeinformation im Speicher zwischengespeichert. Diese können beim Herstellen von Remoteverbindungen wiederverwendet werden.
root/domain/loginAtStart	Wenn der Wert 1 ist und der Thin Client einer Domäne hinzugefügt wurde, wird beim Start des Thin Client ein Anmeldebildschirm angezeigt. Andernfalls wird beim Systemstart der veraltete freigegebene Desktop von ThinPro angezeigt.
root/domain/retainUserRegistry	Wenn der Wert 1 ist, werden jegliche von den Benutzern vorgenommene Änderungen an den Einstellungen zwischen den Anmeldesitzungen beibehalten.
root/domain/workgroup	Gibt die Arbeitsgruppe oder „kurze Domäne“ an, die der Domänenmitgliedschaft des Thin Client zugeordnet ist. Diese wird während der Erstellung der Active Directory Domäne auch als NetBIOS-Domäne bezeichnet. Dieser Wert wird normalerweise während der Domänenauthentifizierung automatisch erkannt, indem er von einem Domänencontroller bezogen wird.

Network

Registrierungsschlüssel	Beschreibung
root/Network/ActiveDirectory/Domain	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/DynamicDNS	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/Enabled	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/Method	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/Password	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/Username	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/DNSServers	Hier kann ein zusätzlicher DNS-Server für die Auflösung des Domännennamens angegeben werden. Die angegebenen Server werden zusätzlich zu jeglichen über DHCP abgerufenen Servern verwendet. Es können bis zu drei IPv4- oder IPv6-Adressen, durch Kommas getrennt, angegeben werden.
root/Network/DefaultHostnamePattern	Legt das Standard-Hostnamensmuster fest, das zu verwenden ist, wenn neue Hostnamen generiert werden. Dies wird verwendet, wenn sowohl der Registrierungsschlüssel <code>Hostname</code>

Registrierungsschlüssel	Beschreibung
	als auch <code>/etc/hostname</code> leer ist. Verwenden Sie im Muster des Hostnamen <code>%</code> als Trennzeichen. Im Beispiel <code>HPTC%MAC:1-6%</code> wäre <code>HPTC</code> das Präfix und die ersten sechs Zeichen der MAC-Adresse des Thin Client würden folgen. Wenn die MAC-Adresse des Thin Client also <code>11:22:33:44:55:66</code> ist, dann wäre der generierte Hostname <code>HPTC112233</code> . Ist das Muster <code>TC%MAC%</code> , wäre der generierte Hostname <code>TC112233445566</code> . Wenn das Muster <code>HP%MAC:7%</code> ist, dann wäre der generierte Hostname <code>HP1122334</code> .
<code>root/Network/EncryptWpaConfig</code>	Wenn der Wert 1 ist, wird das Kennwort verschlüsselt.
<code>root/Network/FtpProxy</code>	Legt die FTP-Proxy-Adresse fest. HP empfiehlt, dass das folgende Format für diesen Wert verwendet wird, da das <code>http</code> -Präfix besser unterstützt ist: <code>http://ProxyServer:Port</code>
<code>root/Network/Hostname</code>	Legt den Hostnamen des Thin Client fest.
<code>root/Network/HttpProxy</code>	Legt die HTTP-Proxy-Adresse fest. HP empfiehlt die Verwendung des folgenden Format: <code>http://ProxyServer:Port</code>
<code>root/Network/HttpsProxy</code>	Legt die HTTPS-Proxy-Adresse fest. HP empfiehlt, dass das folgende Format für diesen Wert verwendet wird, da das <code>http</code> -Präfix besser unterstützt ist: <code>http://ProxyServer:Port</code>
<code>root/Network/IPSec/IPSecRules/<UUID>/DstAddr</code>	Legt die Zieladresse für die IPSec Regel fest.
<code>root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethod</code>	Legt die Authentifizierungsmethode für die IPSec Regel fest. <code>PSK</code> wird für einen Pre-shared-Schlüssel verwendet und <code>Certificate</code> für die Verwendung der Zertifikat-Dateien.
<code>root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodCACert</code>	Wenn die Authentifizierungsmethode <code>Certificate</code> ist, wird der Dateipfad des CA-Zertifikats in diesem Registrierungsschlüssel gespeichert.
<code>root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodClientCert</code>	Wenn die Authentifizierungsmethode <code>Certificate</code> ist, wird der Dateipfad des Client-Zertifikats in diesem Registrierungsschlüssel gespeichert.
<code>root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPresharedKey</code>	Wenn die Authentifizierungsmethode <code>PSK</code> ist, wird der Pre-shared-Key-Wert in diesem Registrierungsschlüssel gespeichert.
<code>root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPrivateKey</code>	Wenn die Authentifizierungsmethode <code>Certificate</code> ist, wird der private Schlüsseldatei-Pfad, der dem Client-Zertifikat entspricht, in diesem Registrierungsschlüssel gespeichert.
<code>root/Network/IPSec/IPSecRules/<UUID>/MMDHGroup</code>	Legt die Phase 1 der Diffie-Hellman-Gruppe fest.
<code>root/Network/IPSec/IPSecRules/<UUID>/MMEncryptionAlg</code>	Legt die Phase 1 des Verschlüsselungsalgorithmus fest.
<code>root/Network/IPSec/IPSecRules/<UUID>/MMIntegrityAlg</code>	Legt die Phase 1 des Integritätsalgorithmus fest.
<code>root/Network/IPSec/IPSecRules/<UUID>/MMLifetimeMinutes</code>	Legt die Phase 1 der Lebensdauer fest.
<code>root/Network/IPSec/IPSecRules/<UUID>/QMAHEnable</code>	Ermöglicht Phase 2 AH.
<code>root/Network/IPSec/IPSecRules/<UUID>/QMAHIntegrityAlg</code>	Legt die Phase 2 AH des Integritätsalgorithmus fest.

Registrierungsschlüssel	Beschreibung
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	Wenn der Wert 1 ist, 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 Netzwerk-Manager generiert wurden, in resolv.conf aufbewahrt. Wenn der Wert 0 ist, dann wird resolv.conf komplett überschrieben.
root/Network/SearchDomains	Zusätzliche Suchdomänen für die FQDN-Auflösung können hier angegeben werden. Die angegebenen Domänen werden an alle unvollständigen Definitionen angehängt werden, als Versuch, einen FQDN zu erzeugen, der über DNS aufgelöst werden kann. Zum Beispiel wird eine Suchdomäne <code>mydomain.com</code> die Serverdefinition <code>Myserver</code> ordnungsgemäß zu <code>myserver.mydomain.com</code> lösen, auch wenn der DNS-Server <code>Myserver</code> nicht in seinem Namenslösungsverzeichnis hat. Bis zu fünf zusätzliche Suchdomänen können angegeben werden.
root/Network/VPN/AutoStart	Wenn der Wert 1 ist, startet VPN automatisch beim Systemstart.
root/Network/VPN/PPTP/Domain	Legt die PPTP-Domäne fest.
root/Network/VPN/PPTP/Gateway	Legt das PPTP-Gateway fest.
root/Network/VPN/PPTP/Password	Legt das PPTP-Benutzerkennwort fest.
root/Network/VPN/PPTP/Username	Legt den PPTP-Benutzernamen fest.
root/Network/VPN/Type	Legt den VPN-Typ fest.
root/Network/VPN/VPNC/DPDEndianess	Legt die Bytereihenfolge der DPD-Sequenznummer fest (siehe rfc3706). 0: Big Endian; 1: Little Endian. Versuchen Sie, diese Option zu aktivieren bzw. deaktivieren, wenn die Sitzung zwischenzeitlich ohne offensichtliche Gründe abgebrochen wird.
root/Network/VPN/VPNC/DPDInterval	Legt das DPD-Intervall in Sekunden fest (siehe rfc3706).

Registrierungsschlüssel	Beschreibung
root/Network/VPN/VPNC/DebugLevel	Legt die Debugebene auf 0, 1, 2, 3 oder 99 fest. Dadurch wird eine große Anzahl von Protokollen erstellt. Aktivieren Sie diese Option nur, wenn Sie ein VPN-Problem beheben müssen.
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 (NATMode) auf <code>cisco-udp</code> festgelegt ist.
root/Network/VPN/VPNC/NATMode	Legt den NAT-Traversal-Modus für VPNC fest.
root/Network/VPN/VPNC/Password	Legt das VPNC-Benutzerkennwort fest.
root/Network/VPN/VPNC/PerfectForwardSecrecy	Legt für die VPNC Diffie-Hellman-Gruppe fest, dass Perfect Forward Secrecy (PFS) verwendet werden soll.
root/Network/VPN/VPNC/Security	Legt die VPNC-Sicherheitsstufe fest.
root/Network/VPN/VPNC/Username	Legt den VPNC-Benutzernamen fest.
root/Network/Wired/DefaultGateway	Legt das Standard-Gateway fest, das vom Gerät für die Kommunikation mit dem Internet verwendet wird. In der Regel ist dies die IP-Adresse des Routers. Diese Einstellung wird nur wirksam, wenn <code>Method</code> auf <code>Static</code> eingestellt ist.
root/Network/Wired/EnableDefGatewayAsDNS	Wenn der Wert 1 ist, dann wird der Standard-Gateway auch als Namensservers benutzt.
root/Network/Wired/EthernetSpeed	Legt die Verbindungsgeschwindigkeit der primären Ethernet-Netzwerkschnittstelle fest. <code>Automatic</code> ermöglicht, dass die schnellste verfügbare Verbindungsgeschwindigkeit verwendet wird, die in der Regel 1 Gbit/s oder 100 Mbit/s/Full je nach Switch ist. Die Verbindungsgeschwindigkeit kann auch erzwungen werden, um eine einzige Geschwindigkeit (100 Mbit/s oder 10 Mbit/s) und einen Duplexmodus (Voll oder Halb) zu verwenden, sodass Switches oder Hubs unterstützt werden, die keine angemessene Autonegotiation durchführen.
root/Network/Wired/IPAddress	Legt die IPv4-Adresse des Thin Client fest. Diese Einstellung wird nur wirksam, wenn <code>Method</code> auf <code>Static</code> eingestellt ist.
root/Network/Wired/IPv6Enable	Wenn der Wert 1 ist, dann ist IPv6 aktiviert.
root/Network/Wired/Interface	Legt die Standard-Ethernet-Schnittstelle oder NIC fest.
root/Network/Wired/MTU	Legt die MTU fest. Es spielt dabei keine Rolle, wenn die IP-Adresse statisch oder DHCP-erworben wird.
root/Network/Wired/Method	Wenn <code>Automatic</code> eingestellt ist, verwendet der Thin Client DHCP, um die Netzwerkeinstellungen abzurufen. Wenn <code>Static</code> eingestellt ist, werden die Werte der Registrierungsschlüssel <code>IP-Adresse</code> , <code>SubnetMask</code> und <code>DefaultGateway</code> verwendet. HP rät, in einem generischen Clientprofil <code>Static</code> nicht zu verwenden, da es dazu führt, dass alle Thin Clients die gleiche IP-Adresse erhalten.

Registrierungsschlüssel	Beschreibung
root/Network/Wired/Profiles/<UUID>/AutoConnect	Wenn der Wert 1 ist, wird das automatische Herstellen der Netzwerkverbindung aktiviert.
root/Network/Wired/Profiles/<UUID>/EthernetSpeed	Legt die Verbindungsgeschwindigkeit der primären Ethernet-Netzwerkschnittstelle fest. <code>Automatic</code> ermöglicht, dass die schnellste verfügbare Verbindungsgeschwindigkeit verwendet wird, die in der Regel 1 Gbit/s oder 100 Mbit/s/Full je nach Switch ist. Die Verbindungsgeschwindigkeit kann auch erzwungen werden, um eine einzige Geschwindigkeit (100 Mbit/s oder 10 Mbit/s) und einen Duplexmodus (<code>Full</code> oder <code>Half</code>) zu verwenden, sodass Switches oder Hubs unterstützt werden, die keine Autonegotiation durchführen.
root/Network/Wired/Profiles/<UUID>/IPv4/Address	Legt die IPv4-Adresse des Client fest. Diese Einstellung ist nur wirksam, wenn <code>Method</code> auf <code>Static</code> festgelegt ist.
root/Network/Wired/Profiles/<UUID>/IPv4/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 ist nur wirksam, wenn <code>Method</code> auf <code>Static</code> festgelegt ist.
root/Network/Wired/Profiles/<UUID>/IPv4/Enabled	Wenn der Wert 1 ist, wird IPv4 für dieses Profil aktiviert.
root/Network/Wired/Profiles/<UUID>/IPv4/Method	Wenn <code>Automatic</code> festgelegt ist, dann verwendet der Client DHCP, um die Netzwerkeinstellungen abzurufen. Wenn <code>Static</code> festgelegt ist, werden die Werte der Registrierungsschlüssel <code>Address</code> , <code>SubnetMask</code> und <code>DefaultGateway</code> verwendet. HP rät von der Verwendung von <code>Static</code> in einem generischen Client-Profil ab, da dies dazu führt, dass alle Clients dieselbe IP-Adresse verwenden.
root/Network/Wired/Profiles/<UUID>/IPv4/SubnetMask	Legt die Subnetzmaske des Geräts fest, z. B. 255.255.255.0 (für ein Standard-Klasse C Subnetz). Diese Einstellung ist nur wirksam, wenn <code>Method</code> auf <code>Static</code> festgelegt ist.
root/Network/Wired/Profiles/<UUID>/IPv6/Address	Legt die IPv6-Adresse des Clients fest. Diese Einstellung ist nur wirksam, wenn <code>Method</code> auf <code>Static</code> festgelegt ist.
root/Network/Wired/Profiles/<UUID>/IPv6/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 ist nur wirksam, wenn <code>Method</code> auf <code>Static</code> festgelegt ist.
root/Network/Wired/Profiles/<UUID>/IPv6/Enabled	Wenn der Wert 1 ist, wird IPv6 für dieses Profil aktiviert.
root/Network/Wired/Profiles/<UUID>/IPv6/Method	Wenn <code>Automatic</code> festgelegt ist, dann verwendet der Client DHCP, um die Netzwerkeinstellungen abzurufen. Wenn <code>Static</code> festgelegt ist, werden die Werte der Registrierungsschlüssel <code>Address</code> , <code>SubnetMask</code> und <code>DefaultGateway</code> verwendet. HP rät von der Verwendung von <code>Static</code> in einem generischen Client-Profil ab, da dies dazu führt, dass alle Clients dieselbe IP-Adresse verwenden.
root/Network/Wired/Profiles/<UUID>/IPv6/SubnetMask	Legt die Subnetzmaske des Geräts fest, die in der Regel der Länge des IPv6-Präfixes entspricht. Diese Einstellung ist nur wirksam, wenn <code>Method</code> auf <code>Static</code> festgelegt ist.
root/Network/Wired/Profiles/<UUID>/MTU	Legt die MTU fest. Es spielt dabei keine Rolle, ob die IP-Adresse statisch ist oder mittels DHCP abgerufen wird.
root/Network/Wired/Profiles/<UUID>/Priority	Für ein kabelgebundenes Netzwerk reserviert.

Registrierungsschlüssel	Beschreibung
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/AnonyIdentity	Legt die anonyme Identität für die PEAP-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/EAPPEAP/CACert	Legt den Pfad der CA-Zertifikatsdatei für die PEAP-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/InnerAuth	Legt das PEAP innere Authentifizierung-Protokoll fest.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/PEAPVer	Legt die PEAP-Version fest.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/Password	Legt das Kennwort für die PEAP-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/Username	Legt den Benutzernamen für die PEAP-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/Security/EAPTLS/CACert	Legt den Pfad der CA-Zertifikatsdatei für die TLS-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/Security/EAPTLS/Identity	Legt die Identität für die TLS-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/EAPTLS/PrivateKey	Legt den Pfad zu einer Datei des privaten Schlüssels für die TLS-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/Security/EAPTLS/PrivateKeyPassword	Legt das Kennwort für eine Datei des privaten Schlüssels für die TLS-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/EAPTLS/UserCert	Legt den Pfad zu einer Benutzerzertifikatsdatei für die TLS-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTL/AnonyIdentity	Legt die anonyme Identität für die TTLS-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTL/CACert	Legt den Pfad zu einer CA-Zertifikatsdatei für die TTLS-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTL/InnerAuth	Legt das TTLS innere Authentifizierung-Protokoll fest.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTL/Password	Legt das Kennwort für die TTLS-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTL/Username	Legt den Benutzernamen für die TTLS-Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/Security/Type	Legt den Typ der kabelgebundenen Authentifizierung fest.
root/Network/Wired/Profiles/<UUID>/WiredInterface	Legt die kabelgebundene Schnittstelle für das Profil fest.
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.

Registrierungsschlüssel	Beschreibung
root/Network/Wired/Security/MachineAuthName	Speichert den Namen des Computerkontos, wenn die Computerauthentifizierung aktiviert ist.
root/Network/Wired/Security/MachineAuthPassword	Speichert das Kennwort des Computerkontos, wenn die Computerauthentifizierung aktiviert ist.
root/Network/Wired/Security/PEAPVersion	Legt die PEAP-Version fest.
root/Network/Wired/Security/Password	Legt das Kennwort fest.
root/Network/Wired/Security/PrivateKey	Legt den Pfad zu einer privaten Schlüsseldatei fest. Dies dient nur der TLS-Authentifizierung.
root/Network/Wired/Security/Type	Legt den 802.1x-Authentifizierungstyp fest.
root/Network/Wired/Security/UserCert	Legt den Pfad zu einer Benutzer-Zertifikatsdatei fest. Dies dient nur der TLS-Authentifizierung.
root/Network/Wired/Security/Username	Legt den Benutzernamen fest.
root/Network/Wired/SubnetMask	Legt die Subnetzmaske des Geräts fest, z. B. 255.255.255.0 (für ein Standard-Klasse C Subnetz). Diese Einstellung wird nur wirksam, wenn Method auf Static eingestellt ist.
root/Network/Wired/UseWiredProfiles	Wenn der Wert 1 ist, wird die kabelgebundene Verbindung im Profilmodus konfiguriert, in dem Verbindungen zu mehreren kabelgebundenen Netzwerken hergestellt werden können. Wenn der Wert 0 ist, kann nur eine Verbindung zu einem kabelgebundenen Netzwerk hergestellt werden.
root/Network/WiredWirelessSwitch	Wenn der Wert 0 ist, können gleichzeitig Verbindungen zu einem kabelgebundenen Netzwerk und einem Wireless-Netzwerk hergestellt werden. Wenn der Wert 1 ist, wird dem kabelgebundenen Netzwerk eine höhere Priorität als dem Wireless-Netzwerk zugewiesen. Falls keine Verbindung zum kabelgebundenen Netzwerk hergestellt werden kann, wird also ein konfiguriertes Wireless-Netzwerk verwendet.
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/EnableWireless	Wenn der Wert 1 ist, wird die Wireless-Funktionalität aktiviert. Wenn der Wert 0 ist, wird die Wireless-Funktionalität deaktiviert.
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 Wireless-Netzwerkadapter fest.
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 Clientprofil Static nicht zu verwenden, da es dazu führt, dass alle Thin Clients die gleiche IP-Adresse erhalten.

Registrierungsschlüssel	Beschreibung
root/Network/Wireless/PowerEnable	Wenn der Wert 1 ist, dann ist das Energiemanagement der Wireless-Netzwerkkarte aktiviert.
root/Network/Wireless/Profiles/<UUID>/AutoConnect	Wenn der Wert 1 ist, wird das automatische Herstellen einer Verbindung zum SSID aktiviert.
root/Network/Wireless/Profiles/<UUID>/IPv4/Address	Legt die IPv4-Adresse des Client fest. Diese Einstellung ist nur wirksam, wenn Method auf Static festgelegt ist.
root/Network/Wireless/Profiles/<UUID>/IPv4/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 ist nur wirksam, wenn Method auf Static festgelegt ist.
root/Network/Wireless/Profiles/<UUID>/IPv4/Enabled	Wenn der Wert 1 ist, wird IPv4 für dieses Profil aktiviert.
root/Network/Wireless/Profiles/<UUID>/IPv4/Method	Wenn Automatic festgelegt ist, dann verwendet der Client DHCP, um die Netzwerkeinstellungen abzurufen. Wenn Static festgelegt ist, werden die Werte der Registrierungsschlüssel Address, SubnetMask und DefaultGateway verwendet. HP rät von der Verwendung von Static in einem generischen Client-Profil ab, da dies dazu führt, dass alle Clients, die dieses Profil verwenden, dieselbe IP-Adresse verwenden.
root/Network/Wireless/Profiles/<UUID>/IPv4/SubnetMask	Legt die Subnetzmaske des Geräts fest, z. B. 255.255.255.0 (für ein Standard-Klasse C Subnetz). Diese Einstellung ist nur wirksam, wenn Method auf Static festgelegt ist.
root/Network/Wireless/Profiles/<UUID>/IPv6/Address	Legt die IPv6-Adresse des Clients fest. Diese Einstellung ist nur wirksam, wenn Method auf Static festgelegt ist.
root/Network/Wireless/Profiles/<UUID>/IPv6/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 ist nur wirksam, wenn Method auf Static festgelegt ist.
root/Network/Wireless/Profiles/<UUID>/IPv6/Enabled	Wenn der Wert 1 ist, wird IPv6 für dieses Profil aktiviert.
root/Network/Wireless/Profiles/<UUID>/IPv6/Method	Wenn Automatic festgelegt ist, dann verwendet der Client DHCP, um die Netzwerkeinstellungen abzurufen. Wenn Static festgelegt ist, werden die Werte der Registrierungsschlüssel Address, SubnetMask und DefaultGateway verwendet. HP rät von der Verwendung von Static in einem generischen Client-Profil ab, da dies dazu führt, dass alle Clients dieselbe IP-Adresse verwenden.
root/Network/Wireless/Profiles/<UUID>/IPv6/SubnetMask	Legt die Subnetzmaske des Geräts fest, die in der Regel der Länge des IPv6-Präfixes entspricht. Diese Einstellung ist nur wirksam, wenn Method auf Static festgelegt ist.
root/Network/Wireless/Profiles/<UUID>/PowerEnable	Wenn der Wert 1 ist, dann ist das Energiemanagement der Wireless-Netzwerkkarte aktiviert.
root/Network/Wireless/Profiles/<UUID>/Priority	Definiert die Priorität des Netzwerks. Im Fall eines Wireless-Netzwerks bedeutet eine größere Zahl eine höhere Priorität. Eine höhere Priorität ist für eine Wireless-Verbindung zu einem Netzwerk vorzuziehen.
root/Network/Wireless/Profiles/<UUID>/SSID	Legt den WLAN-Access Point fest, der über SSID verwendet wird.
root/Network/Wireless/Profiles/<UUID>/SSIDHidden	Gibt an, ob der SSID des WLAN-Access Point ausgeblendet ist.

Registrierungsschlüssel	Beschreibung
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/AnonyIdentity	Legt die anonyme Identität für die EAP-FAST-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/FastProvision	Legt die bereitgestellte Option für die EAP-FAST-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/PACFile	Legt den Pfad der PAC-Datei für die EAP-FAST-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/Password	Legt das Kennwort für die EAP-FAST-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/Username	Legt den Benutzernamen für die EAP-FAST-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/AnonyIdentity	Legt die anonyme Identität für die EAP-PEAP-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/CACert	Legt den Pfad zur CA-Zertifikatsdatei für die EAP-PEAP-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/InnerAuth	Legt das PEAP innere Authentifizierungsprotokoll fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/PEAPVer	Legt die PEAP-Version fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/Password	Legt das Kennwort für die EAP-PEAP-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/Username	Legt den Benutzernamen für die EAP-PEAP-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/CACert	Legt den Pfad der CA-Zertifikatsdatei für die TLS-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/Identity	Legt die Identität für die TLS-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/PrivateKey	Legt den Pfad zu einer Datei des privaten Schlüssels für die TLS-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/PrivateKeyPassword	Legt das Kennwort für eine Datei des privaten Schlüssels für die TLS-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/UserCert	Legt den Pfad zu einer Benutzerzertifikatsdatei für die TLS-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTL/AnonyIdentity	Legt die anonyme Identität für die TTLS-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTL/CACert	Legt den Pfad zu einer CA-Zertifikatsdatei für die TTLS-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTL/InnerAuth	Legt das TTLS innere Authentifizierungsprotokoll fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTL/Password	Legt das Kennwort für die TTLS-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTL/Username	Legt den Benutzernamen für die TTLS-Authentifizierung fest.
root/Network/Wireless/Profiles/<UUID>/Security/PSK/PreSharedKey	Legt das Kennwort für die PSK-Authentifizierung fest.

Registrierungsschlüssel	Beschreibung
root/Network/Wireless/Profiles/<UUID>/Security/Type	Legt den drahtlosen Authentifizierungstyp fest.
root/Network/Wireless/Profiles/<UUID>/Security/WEP/AuthType	Legt den WEP-Authentifizierungstyp fest.
root/Network/Wireless/Profiles/<UUID>/Security/WEP/Key	Legt das WEP-Kennwort fest.
root/Network/Wireless/Profiles/<UUID>/Security/WEP/KeyIndex	Legt den WEP-Kennwortindex fest.
root/Network/Wireless/Profiles/<UUID>/Security/WirelessBand	Legt die Frequenzbereichsauswahl fest. Wählen Sie <code>Auto</code> , um alle Wireless-Kanäle zu überprüfen, wählen Sie <code>2</code> , <code>4</code> GHz, um nur 2,4-GHz-Kanäle zu überprüfen und wählen Sie <code>5</code> GHz, um nur 5-GHz-Kanäle zu überprüfen.
root/Network/Wireless/Profiles/<UUID>/Security/WirelessInterface	Legt die Wireless-Schnittstelle für das Profil fest.
root/Network/Wireless/Roaming/enableRoamingOptions	Wenn der Wert 1 ist, können die Optionen für Wireless-Roaming konfiguriert werden.
root/Network/Wireless/Roaming/roamingThreshold	Legt die zulässige minimale Signalstärke in dBm vor dem Wechsel zu einem Access Point mit größerer Signalstärke fest. Beachten Sie, dass dieser Wert negativ ist.
root/Network/Wireless/Roaming/scanInterval	Legt fest, wie oft (in Sekunden) nach einem Access Point mit größerer Signalstärke gesucht werden soll, wenn die Signalstärke den Roaming-Grenzwert unterschreitet.
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/InnerAuthTLS	Legt das TLS 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.

Registrierungsschlüssel	Beschreibung
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/Wireless/UseWirelessProfiles	Wenn der Wert 1 ist, wird die Wireless-Verbindung im Profilmodus konfiguriert, in dem Verbindungen zu mehreren Wireless-Netzwerken hergestellt werden können. Dies ist für die mobile Computernutzung nützlich. Wenn der Wert 0 ist, kann nur zu einem Wireless-Netzwerk eine Verbindung hergestellt werden.
root/Network/Wireless/WirelessBand	Legt die Frequenzbereichsauswahl fest. Wählen Sie Auto, um alle Wireless-Kanäle zu überprüfen, wählen Sie 2, 4 GHz, um nur 2,4-GHz-Kanäle zu überprüfen und wählen Sie 5 GHz, um nur 5-GHz-Kanäle zu überprüfen.
root/Network/Wireless/WpaDriver	Gibt den Treiber an, der von wpa_supplicant verwendet wird (standardmäßig wext). nl80211 ist der einzige Treiber, der aktuell unterstützt wird.
root/Network/Wireless/bcmwlCountryOverride	Überschreibt den Wert für das Land aus dem BIOS, wenn der erforderliche Wert im BIOS nicht vorhanden ist. Der bcmwl-Treiber akzeptiert die wl_country-Option, die bei Bedarf aus BIOS-Werten abgerufen wird (gegenwärtig wird nur Indonesien unterstützt). Ein Systemneustart ist erforderlich, damit die Änderungen wirksam werden.
root/Network/Wireless/disableUserCreateWirelessProfile	Wenn der Wert 1 ist, können mit Benutzerkonten keine Wireless-Profile über die Taskleiste erstellt werden.
root/Network/Wireless/disableUserWirelessProfileTrayMenu	Wenn der Wert 1 ist, wird das Wireless-Menü, das über das Wireless-Symbol in der Taskleiste geöffnet wird, für das Benutzerkonto deaktiviert.
root/Network/Wireless/disableWirelessProfileTrayMenu	Wenn der Wert 1 ist, wird das Wireless-Menü deaktiviert, das über das Wireless-Symbol in der Taskleiste geöffnet wird.
root/Network/Wireless/tryAutoWirelessIfUserFailed	Wenn der Wert 1 ist und der Versuch eines Benutzers fehlschlägt, eine Verbindung zu einem WLAN-Access Point herzustellen, versucht das Wireless-Modul, mithilfe aller verfügbaren Profile eine Wireless-Verbindung herzustellen. Wenn der Wert 0 ist und der Versuch eines Benutzers fehlschlägt, eine Verbindung zu einem WLAN-Access Point herzustellen, wird der Wireless-Status als getrennt angezeigt. Dies ist eine alternative Funktion.
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.
root/Network/enableVPNMenu	Wenn der Wert 1 ist, wird das VPN-Menü aktiviert, das sich per Linksklick über das Netzwerksymbol in der Taskleiste aufrufen lässt.

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/SingleSidedAccelerate	Wenn der Wert 1 ist, wird die HP Velocity Funktion zur einseitigen Beschleunigung aktiviert. Wenn der Wert 0 ist, wird die Funktion deaktiviert. HP Velocity wird auf dem HP t420 und HP mt20 nicht unterstützt.
root/Network/iPeak/Status	Wenn der Wert 1 ist, wird HP Velocity aktiviert. Wenn der Wert 2 ist, dann ist HP Velocity im Monitor-Modus aktiviert. Durch die Einstellung 0 wird HP Velocity deaktiviert. HP Velocity wird auf HP t420 nicht unterstützt.
root/Network/userLock	Wenn der Wert 1 ist und die Netzwerkeinstellungen vom Benutzer geändert wurden, werden die Netzwerkeinstellungen beim Import eines Clientprofils beibehalten.
root/Network/userLockEngaged	Dieser Registrierungsschlüssel wird automatisch auf 1 gesetzt, nachdem die Netzwerkeinstellungen vom Benutzer geändert wurden. Sie müssen diese Einstellung in der Regel nicht ändern.

Power

Registrierungsschlüssel	Beschreibung
root/Power/currentPowerPlan	Mit diesem Registrierungsschlüssel wird der zu verwendende Energiesparplan ausgewählt. Die Standardeinstellung wird automatisch ausgewählt.
root/Power/AC/brightness	Legt den standardmäßige Helligkeitsstufe (in Prozent) bei angeschlossenem mobilen Thin Client fest.
root/Power/default/AC/cpuMode	Legt den CPU-Modus für einen Energiesparplan fest, wenn der Computer an den Netzstrom angeschlossen ist. Standardmäßig ist dieser Wert auf „Leistung“ festgelegt.
root/Power/default/AC/lidAction	Legt die Aktion fest, die beim Schließen des Displays ausgeführt werden soll, wenn der Computer an den Netzstrom angeschlossen ist. Standardmäßig ist der Wechsel in den Standbymodus festgelegt.
root/Power/default/AC/powerButtonAction	Legt die Aktion fest, die beim Drücken der Ein/Aus-Taste ausgeführt werden soll, wenn der Computer an den Netzstrom angeschlossen ist. Standardmäßig ist festgelegt, dass der Computer heruntergefahren wird.
root/Power/default/AC/sleep	Legt die Zeit (in Minuten) fest, die verstreicht, bevor der Computer in den Standbymodus wechselt, wenn der Computer an den Netzstrom angeschlossen ist. Standardmäßig ist dieser Wert auf 30 festgelegt. Wenn der Wert 0 ist, wechselt der Computer gar nicht in den Standbymodus.
root/Power/default/AC/standby	Legt die Zeit (in Minuten) fest, die verstreicht, bevor die Anzeige ausgeschaltet wird, wenn der Computer an den Netzstrom angeschlossen ist. Standardmäßig ist dieser Wert auf 15 festgelegt. Wenn der Wert 0 ist, wechselt der Computer nie in den Standbymodus.
root/Power/default/AC/timeoutDim	Diese Taste wird derzeit nicht verwendet.

Registrierungsschlüssel	Beschreibung
root/Power/default/battery/brightness	Legt den standardmäßige Helligkeitsstufe (in Prozent) fest, wenn der mobile Thin Client nicht angeschlossen ist.
root/Power/default/battery/cpuMode	Legt den CPU-Modus für einen Energiesparplan fest, wenn der Computer nicht an den Netzstrom angeschlossen ist. Standardmäßig ist dieser Wert auf die bedarfsgesteuerte Ausführung festgelegt.
root/Power/default/battery/critical/criticalBatteryAction	Legt die Aktion fest, die durchgeführt werden soll, wenn der Akkuladestand kritisch ist, definiert durch criticalBatteryLevel.
root/Power/default/battery/critical/criticalBatteryLevel	Legt den Grenzwert (in Prozent) für den verbleibenden Akkuladestand fest, der als kritischer Akkuladestand angesehen werden soll.
root/Power/default/battery/lidAction	Legt die Aktion fest, die beim Schließen des Displays ausgeführt werden soll, wenn der Computer nicht an den Netzstrom angeschlossen ist. Standardmäßig ist der Wechsel in den Standbymodus festgelegt.
root/Power/default/battery/low/brightness	Legt den standardmäßige Helligkeitsstufe (in Prozent) bei niedrigem Akkustand fest.
root/Power/default/battery/low/cpuMode	Legt den CPU-Modus fest (leistungs- oder bedarfsbezogen).
root/Power/default/battery/low/lowBatteryLevel	Legt den Prozentwert für den verbleibenden Akkuladestand fest, der als niedriger Akkuladestand angesehen werden soll.
root/Power/default/battery/low/sleep	Legt die Zeit (in Minuten) fest, die verstreicht, bevor der Computer in den Standbymodus wechselt, wenn der Computer nicht an den Netzstrom angeschlossen ist. Standardmäßig ist dieser Wert auf 30 festgelegt. Wenn der Wert 0 ist, wechselt der Computer gar nicht in den Standbymodus.
root/Power/default/battery/low/standby	Legt die Zeit (in Minuten) fest, die verstreicht, bevor das Display ausgeschaltet wird, wenn der Computer nicht an den Netzstrom angeschlossen ist. Standardmäßig ist dieser Wert auf 15 festgelegt. Wenn der Wert 0 ist, wechselt der Computer nie in den Standbymodus.
root/Power/default/battery/low/timeoutDim	Diese Taste wird derzeit nicht verwendet.
root/Power/default/battery/powerButtonAction	Gibt an, was geschehen soll, wenn die Ein/Aus-Taste gedrückt wird.
root/Power/default/battery/sleep	Legt fest, wie viele Minuten bis zum Wechsel in den Standbymodus verstreichen sollen. 0 = niemals.
root/Power/default/battery/standby	Legt fest, wie viele Minuten bis zum Ausschalten des Displays verstreichen sollen. 0 = niemals.
root/Power/default/battery/timeoutDim	Diese Taste wird derzeit nicht verwendet.

SCIM

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

ScepMgr

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

Search

Registrierungsschlüssel	Beschreibung
root/Search/Category/Applications/ConnectionManager/checked	

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

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 Flusststeuerung des seriellen Geräts fest, die das Starten und Anhalten der seriellen Kommunikation kommuniziert.
root/Serial/<UUID>/name	Legt den Windows Geräteanschluss fest, der für die Kommunikation mit dem seriellen Gerät verwendet wird.
root/Serial/<UUID>/parity	Legt die Paritätsbit des seriellen Geräts fest. Der Paritätsbit wird für die Fehlererkennung verwendet. Die Einstellung <code>none</code> bedeutet, es gibt keine Paritätserkennung.

SystemInfo

Registrierungsschlüssel	Beschreibung
root/SystemInfo/Pages/General	Wenn der Wert 0 ist, wird die Registerkarte Allgemein im Fenster mit den Systeminformationen für Endbenutzer ausgeblendet.
root/SystemInfo/Pages/NetTools	Wenn der Wert 0 ist, wird die Registerkarte Netzwerktools im Fenster mit den Systeminformationen für Endbenutzer ausgeblendet.
root/SystemInfo/Pages/Network	Wenn der Wert 0 ist, wird die Registerkarte Netzwerk im Fenster mit den Systeminformationen für Endbenutzer ausgeblendet.
root/SystemInfo/Pages/SoftwareInformationTab/ServicePacks	Wenn der Wert 0 ist, wird die Registerkarte Service Packs im Abschnitt Softwareinformationen im Fenster „Softwareinformationen“ für Endbenutzer ausgeblendet.
root/SystemInfo/Pages/SoftwareInformationTab/SoftwareInformation	Wenn der Wert 0 ist, wird die Registerkarte Softwareinformationen im Fenster mit den Systeminformationen für Endbenutzer ausgeblendet.
root/SystemInfo/Pages/SoftwareInformationTab/SoftwareInstalled	Wenn der Wert 0 ist, wird die Registerkarte Installierte Software im Abschnitt Softwareinformationen im Fenster „Softwareinformationen“ für Endbenutzer ausgeblendet.
root/SystemInfo/Pages/SystemLogs	Wenn der Wert 0 ist, wird die Registerkarte Systemprotokolle im Fenster „Systeminformationen“ für Endbenutzer ausgeblendet.
root/SystemInfo/authorized	Wenn der Wert 0 ist, ist die Schaltfläche „Systeminformationen“ in der Taskleiste für Endbenutzer deaktiviert.

TaskMgr

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

USB

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

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/LockScreenTimeout	Gibt das Zeitlimit (in Minuten) an, nach dem der Bildschirm während eines automatischen Updates entsperrt wird. Wenn der Wert 0 ist, wird der Bildschirm während des gesamten automatischen Updates bis zu dessen Abschluss entsperrt.
root/auto-update/ManualUpdate	Wenn der Wert 1 ist, sind die DHCP-Kennung, die DNS-Alias und die Aktualisierungsmethoden der Übertragung für Automatic Update deaktiviert. Wenn eine manuelle Aktualisierung durchgeführt wird, müssen die Registrierungsschlüssel <code>password</code> , <code>path</code> , <code>protocol</code> , <code>user</code> und <code>ServerURL</code>

Registrierungsschlüssel	Beschreibung
	eingestellt werden, um sicherzustellen, dass der Updateserver bekannt ist.
root/auto-update/ScheduledScan/Enabled	Wenn der Wert 1 ist, prüft der Thin Client in regelmäßigen Abständen den Automatic Update-Server, um nach Aktualisierungen zu suchen. Wenn der Wert 0 ist, wird vom Thin Client nur beim Systemstart auf Aktualisierungen geprüft.
root/auto-update/ScheduledScan/Interval	Legt die Zeit fest, die zwischen geplanten Updates gewartet wird. Dies sollte im Format 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/enableLockScreen	Wenn der Wert 1 ist, wird der Bildschirm während eines automatischen Updates gesperrt.
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 Manuelle Konfiguration aktivieren im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/auto-update/gui/auto-update/ServerURL	Zum Einstellen des Status für das Widget Server im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/auto-update/gui/auto-update/enableLockScreen	Zum Einstellen des Status für das Widget Sperrbildschirm bei automatischem Update aktivieren im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der

Registrierungsschlüssel	Beschreibung
	Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/auto-update/gui/auto-update/enableOnBootup</code>	Zum Einstellen des Status für das Widget Automatic Update beim Systemstart aktivieren im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/auto-update/gui/auto-update/password</code>	Zum Einstellen des Status für das Widget Kennwort im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/auto-update/gui/auto-update/protocol</code>	Zum Einstellen des Status für das Widget Protokoll im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/auto-update/gui/auto-update/tag</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/auto-update/gui/auto-update/user</code>	Zum Einstellen des Status für das Widget Benutzername im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/auto-update/password</code>	Legt das Kennwort fest, das verwendet wird, wenn <code>ManualUpdate</code> aktiviert ist. Dies wird nur verwendet, wenn das <code>protocol</code> auf <code>ftp</code> eingestellt ist. Dieser Wert ist normalerweise verschlüsselt.
<code>root/auto-update/path</code>	Legt den relativen Pfad von der Standard-Server-URL fest, wenn <code>ManualUpdate</code> aktiviert ist. Dies ist normalerweise leer oder auf <code>auto-update</code> eingestellt.
<code>root/auto-update/preserveConfig</code>	Wenn der Wert 1 ist, dann werden die aktuellen Einstellungen der Thin Client-Konfiguration bei einem Image-Update über Automatic Update beibehalten.
<code>root/auto-update/protocol</code>	Legt das Protokoll fest, das verwendet wird, wenn <code>ManualUpdate</code> aktiviert ist.
<code>root/auto-update/tag</code>	Der Registrierungsschlüssel ist veraltet. Er hat zuvor die für DHCP (137) verwendete Tag-Nummer festgelegt. Dies wird jetzt über den Tag-Namen <code>Auto-Update</code> erkannt.
<code>root/auto-update/user</code>	Legt den Benutzernamen fest, der verwendet wird, wenn <code>ManualUpdate</code> aktiviert ist. Dies wird nur verwendet, wenn 'Protocol' auf 'ftp' eingestellt ist.

background

Registrierungsschlüssel	Beschreibung
<code>root/background/bginfo/alignment</code>	Legt die Textausrichtung für die Hintergrundsysteminformationen fest.
<code>root/background/bginfo/enabled</code>	Wenn der Wert <code>1</code> ist, werden Systeminformationen auf dem Desktophintergrund angezeigt (Hintergrundsysteminformationen).
<code>root/background/bginfo/horizontalLocation</code>	Legt die Position der Hintergrundsysteminformationen auf der X-Achse als Prozentsatz fest.
<code>root/background/bginfo/interval</code>	Legt das Intervall für die Textaktualisierung der Hintergrundsysteminformationen in Sekunden fest.
<code>root/background/bginfo/preset</code>	Legt für die Voreinstellungsdatei der Hintergrundsysteminformationen <code>use</code> fest. Wenn dieser Wert auf <code>none</code> festgelegt ist, können Sie die Einstellungen im Hintergrund-Manager anpassen.
<code>root/background/bginfo/shadowColor</code>	Legt die Schattenfarbe für die Hintergrundsysteminformationen fest.
<code>root/background/bginfo/shadowOffset</code>	Legt den Schattenoffset für die Hintergrundsysteminformationen fest. Wenn der Wert <code>0</code> ist, wird der Schatten deaktiviert.
<code>root/background/bginfo/text</code>	Legt den Text für die Hintergrundsysteminformationen fest. Weitere Informationen finden Sie im HP ThinPro-Whitepaper <i>nur auf Englisch verfügbar</i> .
<code>root/background/bginfo/textColor</code>	Legt die Textfarbe für die Hintergrundsysteminformationen fest.
<code>root/background/bginfo/textSize</code>	Legt die Textgröße für die Hintergrundsysteminformationen fest.
<code>root/background/bginfo/verticalLocation</code>	Legt die Position der Hintergrundsysteminformationen auf der Y-Achse als Prozentsatz fest.
<code>root/background/desktop/color</code>	Durch die Einstellung von <code>theme</code> auf <code>none</code> für das Design, speichert dieser Schlüssel die Standardfarbe, die das benutzerdefinierte Design verwendet.
<code>root/background/desktop/imagePath</code>	Durch die Einstellung von <code>theme</code> auf <code>none</code> für das Design, speichert dieser Schlüssel den Image-Pfad des Desktop-Hintergrunds, die das benutzerdefinierte Design verwendet.
<code>root/background/desktop/lastBrowseDir</code>	Durch die Einstellung von <code>theme</code> auf <code>none</code> für das Design, speichert dieser Schlüssel das zuletzt verwendete Verzeichnis.
<code>root/background/desktop/style</code>	Durch die Einstellung von <code>theme</code> auf <code>none</code> , speichert dieser Schlüssel, wie das Hintergrundbild auf dem Desktop erscheint (wie z.B. <code>center</code> , <code>tile</code> , <code>stretch</code> , <code>fit</code> und <code>fill</code>).
<code>root/background/desktop/theme</code>	Legt die System-Design-Einstellung fest. Dieser Wert wird über den Hintergrund-Manager in der Systemsteuerung festgelegt. Die gültigen Werte hängen von den Designs ab, die auf dem System vorhanden sind. Dieser Schlüssel kann auf <code>none</code> eingestellt werden, damit die Benutzer das Design definieren können, auf <code>auto</code> , damit das System automatisch das Design des entsprechenden Protokolls für Smart Zero festlegt, oder auf <code>default</code> , damit das Standard-Design für ThinPro verwendet wird.

config-wizard

Registrierungsschlüssel	Beschreibung
root/config-wizard/FirmwareUpdate/firmwareUpdateTimeout	Legt die Timeout-Dauer in Sekunden fest, wenn nach Updates gesucht wird. Bei Auswahl -1 gibt es keine Zeitüberschreitung.
root/config-wizard/FirmwareUpdate/firmwareUpdateURL	Legt die FTP-URL für Image-Aktualisierungen fest.
root/config-wizard/FirmwareUpdate/preserveConfig	Wenn der Wert 1 ist, werden die aktuellen Einstellungen der Thin Client-Konfiguration beibehalten, wenn ein Image-Update über den Erstkonfigurationsassistenten erfolgt.
root/config-wizard/SelfUpdate/selfUpdateTimeout	Legt das Zeitlimit (in Sekunden) für die Suche nach Updates zur automatischen Aktualisierung fest. Bei Auswahl -1 gibt es keine Zeitüberschreitung.
root/config-wizard/SelfUpdate/selfUpdateURL	Legt die FTP-URL für den Konfigurationsassistenten fest.
root/config-wizard/disableAllChecksAtStartup	Wenn der Wert 1 ist, werden alle Prüfungen beim Systemstart deaktiviert. Wenn der Wert 0 ist, können Sie jede Art von Prüfung einzeln mithilfe der Registrierungsschlüssel <code>enableConnectionCheck</code> , <code>enableNetworkCheck</code> und <code>enableUpdateCheck</code> aktivieren/deaktivieren.
root/config-wizard/enableConfigWizard	Wenn der Wert 1 ist, wird der Konfigurationsassistent beim Systemstart aktiviert.
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/enableUpdateCheck	Wenn der Wert 1 ist, ist die Update-Prüfung beim Systemstart aktiviert.
root/config-wizard/enableUpdateCheckGui	Wenn der Wert 1 ist, wird die Prüfung der grafischen Benutzeroberfläche beim Systemstart aktiviert.
root/config-wizard/showNetworkSettingsButton	Wenn der Wert 1 ist, wird die Schaltfläche „Netzwerkeinstellungen“ im Fenster für die Netzwerkprüfung angezeigt.

desktop

Registrierungsschlüssel	Beschreibung
root/desktop/shortcuts/<action>/command	Legt den Befehl fest, der durch die Verknüpfung ausgeführt wird.
root/desktop/shortcuts/<action>/enabled	Wenn der Wert 1 ist, wird die Verknüpfung aktiviert.
root/desktop/shortcuts/<action>/shortcut	Gibt den Verknüpfungsnamen an.

entries

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

keyboard

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

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

logging

Registrierungsschlüssel	Beschreibung
root/logging/general/debug	Wenn der Wert 1 ist, dann ist Debugging für alle unterstützten Debug-Subsysteme aktiviert. Dies wird gewöhnlich in Verbindung mit <code>generateDiagnostic.sh</code> oder dem 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 Debugebene auf der Registerkarte Systemprotokolle im Fenster Systeminformationen für Endbenutzer verfügbar. Wenn der Wert 0 ist, ist die Option nur für Administratoren verfügbar.

login

Registrierungsschlüssel	Beschreibung
root/login/buttons/configure/authorized	Wenn der Wert 1 ist, steht auf dem Anmeldebildschirm die Schaltfläche „Konfiguration“ zur Verfügung.
root/login/buttons/info/authorized	Wenn der Wert 1 ist, steht auf dem Anmeldebildschirm die Schaltfläche „Systeminformationen“ zur Verfügung.
root/login/keyboard/authorized	Wenn der Wert 1 ist, können auf dem Anmeldebildschirm die Tastaturlayout-Einstellungen konfiguriert werden.
root/login/locale/authorized	Wenn der Wert 1 ist, können auf dem Anmeldebildschirm die Spracheinstellungen konfiguriert werden.
root/login/mouse/authorized	Wenn der Wert 1 ist, können auf dem Anmeldebildschirm die Mauseinstellungen konfiguriert werden.

Registrierungsschlüssel	Beschreibung
<code>root/login/onscreenKeyboard/authorized</code>	Wenn der Wert 1 ist, steht auf dem Anmeldebildschirm die Bildschirmtastatur zur Verfügung.
<code>root/login/power/authorized</code>	Wenn der Wert 1 ist, steht auf dem Anmeldebildschirm die Ein/Aus-Taste zur Verfügung.
<code>root/login/poweroff/authorized</code>	Wenn der Wert 1 ist, steht auf dem Anmeldebildschirm die Funktion zum Herunterfahren zur Verfügung.
<code>root/login/reboot/authorized</code>	Wenn der Wert 1 ist, steht auf dem Anmeldebildschirm die Neustartfunktion zur Verfügung.
<code>root/login/show/authorized</code>	Wenn der Wert 1 ist, steht auf dem Anmeldebildschirm der Schaltflächen-Drawer mit zusätzlichen Optionen zur Verfügung.
<code>root/login/sleep/authorized</code>	Wenn der Wert 1 ist, steht auf dem Anmeldebildschirm die Standbyfunktion zur Verfügung.
<code>root/login/touchscreen/authorized</code>	Wenn der Wert 1 ist, können auf dem Anmeldebildschirm die Touchscreen-Einstellungen konfiguriert werden. Der Registrierungsschlüssel <code>root/touchscreen/enabled</code> muss ebenfalls aktiviert werden.

mouse

Registrierungsschlüssel	Beschreibung
<code>root/mouse/MouseHandedness</code>	Wenn der Wert 0 ist, dann ist die Maus für Rechtshänder. Wenn der Wert 1 ist, dann ist die Maus für Linkshänder.
<code>root/mouse/MouseSpeed</code>	Legt die Beschleunigung des Mauszeigers fest. In der Regel ist ein Wert von 0 bis 25 der nutzbare Bereich. Ein Wert von 0 deaktiviert die Beschleunigung vollständig, wodurch die Maus sich in einem konstant langsamen, aber messbaren Tempo bewegt.
<code>root/mouse/MouseThreshold</code>	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.
<code>root/mouse/disableTrackpadWhileTyping</code>	Wenn der Wert 1 ist, wird das Trackpad während der Eingabe vorübergehend deaktiviert. Wenn der Wert 0 ist, wird das Trackpad während der Eingabe nicht vorübergehend deaktiviert.
<code>root/mouse/enableTrackpad</code>	Wenn der Wert 1 ist, wird das Trackpad aktiviert. Wenn der Wert 0 ist, wird das Trackpad deaktiviert.

restore-points

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

screensaver

Registrierungsschlüssel	Beschreibung
<code>root/screensaver/SlideShowAllMonitors</code>	Wenn der Wert 1 ist, wird die Bildschirmschoner-Diashow auf allen Monitoren angezeigt. Wenn der Wert 0 ist, wird die Diashow nur auf dem primären Monitor angezeigt.
<code>root/screensaver/SlideShowInterval</code>	Legt das Intervall in Sekunden für Bilderwechsel in der Bildschirmschoner-Diashow fest.
<code>root/screensaver/SlideShowPath</code>	Gibt das Verzeichnis an, das die Bilder für die Bildschirmschoner-Diashow enthält.
<code>root/screensaver/buttons/configure/authorized</code>	Wenn der Wert 1 ist, steht bei gesperrtem Bildschirm die Schaltfläche „Konfiguration“ zur Verfügung.
<code>root/screensaver/buttons/info/authorized</code>	Wenn der Wert 1 ist, steht bei gesperrtem Bildschirm die Schaltfläche „Systeminformationen“ zur Verfügung.
<code>root/screensaver/buttons/keyboard/authorized</code>	Wenn der Wert 1 ist, können bei gesperrtem Bildschirm die Tastaturlayout-Einstellungen konfiguriert werden.
<code>root/screensaver/buttons/locale/authorized</code>	Wenn der Wert 1 ist, können bei gesperrtem Bildschirm die Spracheinstellungen konfiguriert werden.
<code>root/screensaver/buttons/mouse/authorized</code>	Wenn der Wert 1 ist, können bei gesperrtem Bildschirm die Mauseinstellungen konfiguriert werden.
<code>root/screensaver/buttons/onscreenKeyboard/authorized</code>	Wenn der Wert 1 ist, steht bei gesperrtem Bildschirm die Bildschirmtastatur zur Verfügung.
<code>root/screensaver/buttons/power/authorized</code>	Wenn der Wert 1 ist, steht bei gesperrtem Bildschirm die Ein/Aus-Taste zur Verfügung.
<code>root/screensaver/buttons/poweroff/authorized</code>	Wenn der Wert 1 ist, steht bei gesperrtem Bildschirm die Funktion zum Herunterfahren zur Verfügung.
<code>root/screensaver/buttons/reboot/authorized</code>	Wenn der Wert 1 ist, steht bei gesperrtem Bildschirm die Neustartfunktion zur Verfügung.
<code>root/screensaver/buttons/show/authorized</code>	Wenn der Wert 1 ist, steht bei gesperrtem Bildschirm der Schaltflächen-Drawer mit zusätzlichen Optionen zur Verfügung.
<code>root/screensaver/buttons/sleep/authorized</code>	Wenn der Wert 1 ist, steht bei gesperrtem Bildschirm die Standbyfunktion zur Verfügung.
<code>root/screensaver/buttons/touchscreen/authorized</code>	Wenn der Wert 1 ist, können bei gesperrtem Bildschirm die Touchscreen-Einstellungen konfiguriert werden. Der Registrierungsschlüssel <code>root/touchscreen/enabled</code> muss ebenfalls aktiviert werden.
<code>root/screensaver/enableCustomLogo</code>	Wenn der Wert 1 ist, dann werden die in <code>LogoPath</code> definierten, benutzerdefinierten Image für den Bildschirmschoner verwendet.
<code>root/screensaver/enableDPMS</code>	Wenn der Wert 0 ist, dann ist die Monitor-Energieverwaltung deaktiviert. Dies bewirkt, dass der Monitor eingeschaltet bleibt, bis er manuell ausgeschaltet wird.
<code>root/screensaver/enableScreensaver</code>	Wenn der Wert 1 ist, wird der Bildschirmschoner aktiviert.
<code>root/screensaver/enableSleep</code>	Wenn der Wert 1 ist, dann ist der Standbymodus aktiviert.
<code>root/screensaver/lockScreen</code>	Wenn der Wert 1 ist, ist ein Kennwort erforderlich, um vom Bildschirmschoner zum Desktop zurückkehren.

Registrierungsschlüssel	Beschreibung
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. <code>Center</code> , <code>Tile</code> und <code>Stretch</code>). Bei Auswahl von <code>Default</code> (Standard), wird das Bild ohne jegliche Verarbeitung angezeigt. Wenn der Wert <code>SlideShow</code> ist, durchläuft der Bildschirmschoner die Bilder im Verzeichnis, das von <code>SlideShowPath</code> angegeben 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 <code>mode</code> auf <code>Default</code> eingestellt ist.
root/screensaver/standby	Legt die Zeitüberschreitung-Zeitverzögerung in Minuten fest, bevor der Monitor in den Standbymodus 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 Standbymodus wechselt.

security

Registrierungsschlüssel	Beschreibung
root/security/authenticationFailDelay	Legt die ungefähre Zeit für die Verzögerung nach einem fehlgeschlagenen Anmeldeversuch in Millisekunden fest. Die tatsächliche Zeit kann um 25 % von diesem Wert abweichen. Verwenden Sie beispielsweise einen Wert von 3000, um eine Verzögerung von ca. 3 Sekunden zu erreichen.
root/security/domainEntryMode	Wenn der Wert 1 ist, muss die Domäne in einem eigenen Textfeld mit der Bezeichnung Domäne eingegeben werden. Wenn der Wert 0 ist, muss die Domäne in einem Bereich des Felds Benutzer eingegeben werden.
root/security/enableLockOverride	Wenn der Wert 1 ist, können Administratoren die Bildschirmsperre eines lokalen Desktops überschreiben.
root/security/enableSecretPeek	Wenn der Wert 1 ist, weisen Kennwort- und PIN-Dialogfelder eine Schaltfläche auf, mit der sich das eingegebene Kennwort bzw. die PIN im Klartext anzeigen lassen.
root/security/encryption/identity/encryptedSecretCipher	Legt den Algorithmus für symmetrische Verschlüsselung eines geheimen Schlüssels fest. Alle Algorithmen verwenden eine angemessene Menge von zufällig gewählten Zeichenfolgen („Salt“), die jedes Mal generiert werden, wenn ein geheimer Schlüssel gespeichert wird. Der Verschlüsselungsschlüssel ist auf jedem Thin Client anders und die Verschlüsselung und Entschlüsselung ist nur durch autorisierte Programme möglich. Die Liste der unterstützten Verschlüsselungsverfahren umfasst die meisten OpenSSL-Verschlüsselungsverfahren und ChaCha20-Poly1305.

Registrierungsschlüssel	Beschreibung
root/security/encryption/identity/encryptedSecretTTL	Legt die Anzahl von Sekunden für die Gültigkeit von gespeicherten verschlüsselten geheimen Schlüsseln nach der letzten erfolgreichen Anmeldung fest. Wenn der Wert eine negative Zahl ist, gibt es kein Zeitlimit für verschlüsselte geheime Schlüssel.
root/security/encryption/identity/secretHashAlgorithm	Legt den Algorithmus zur Erstellung eines Hash mit einem geheimen Schlüssel fest. Schlüsselableitungsfunktionen wie scrypt oder Argon2 sind besser als einfache Hashes, weil damit Rainbow-Wörterbücher mithilfe einer Schlüsselableitungsfunktion nicht schnell berechnet werden können. Alle Algorithmen verwenden eine angemessene Menge von zufällig gewählten Zeichenfolgen („Salt“), die jedes Mal generiert werden, wenn ein geheimer Schlüssel hashcodiert wird. Die Liste der unterstützten Funktionen umfasst scrypt, Argon2, SHA-256 und SHA-512 (allerdings handelt es sich bei den beiden letztgenannten nicht um Schlüsselableitungsfunktionen).
root/security/encryption/identity/secretHashTTL	Legt die Anzahl von Sekunden für die Gültigkeit eines gespeicherten Hashes mit geheimen Schlüssel nach der letzten erfolgreichen Anmeldung fest. Wenn der Wert eine negative Zahl ist, gibt es kein Zeitlimit für Hashes mit geheimen Schlüsseln.
root/security/mustLogin	Stellen Sie den Wert 1 ein, um eine Anmeldung aller Benutzer vor dem Zugriff auf den Desktop zu erzwingen.

shutdown

Registrierungsschlüssel	Beschreibung
root/shutdown/enableAutomaticShutdownTimeout	Wenn der Wert 1 ist, erscheint im Bestätigungsdialogfeld zum Herunterfahren/Neustarten/Abmelden eine Statusanzeige. Wird die Frage nicht rechtzeitig beantwortet, erfolgt das Herunterfahren/Neustarten/Abmelden automatisch.
root/shutdown/timeOfAutomaticShutdownTimeout	Legt die Wartezeit für das automatische Herunterfahren fest.

sshd

Registrierungsschlüssel	Beschreibung
root/sshd/disableWeakCipher	Wenn der Wert 1 ist, wird die Verschlüsselung im CBC-Modus deaktiviert und andere als schwach bekannte Verschlüsselungsverfahren wie 3DES und arcfour ebenfalls.
root/sshd/disableWeakHmac	Wenn der Wert 1 ist, wird 96-Bit-HMAC deaktiviert, ebenso jegliche SHA1-basierte und MD5-basierte HMAC-Algorithmen.
root/sshd/disableWeakKex	Wenn der Wert 1 ist, werden Algorithmen für den DH-Schlüsselaustausch mit SHA1 deaktiviert.
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 Endbenutzer über SSH eine Verbindung mit dem Thin Client herstellen.

Registrierungsschlüssel	Beschreibung
<code>root/time/NTPServers</code>	Gibt zu verwendende NTP-Server über eine Liste mit Kommas als Trennzeichen an. Private NTP-Server oder große virtuelle NTP-Cluster wie <code>pool.ntp.org</code> sind die beste Auswahl, um die Serverlast zu minimieren. Deaktivieren Sie dieses Feld, um die Verwendung von DHCP-Servern (Tag 42) anstelle einer festen Liste zurückzukehren.
<code>root/time/dateFormatLong</code>	Eine optionale Methode zum Überschreiben des langen Datumsformats, das in verschiedenen ThinPro Tools verwendet wird. Führen Sie zur Formatierung einer Websuche nach <code>QDate::toString</code> durch. Wenn das Feld leer gelassen wird, wird normalerweise eine gebietsschemaspezifische Zeichenfolge verwendet.
<code>root/time/dateFormatShort</code>	Eine optionale Methode zum Überschreiben des kurzen Datumsformats, das in verschiedenen ThinPro Tools verwendet wird. Führen Sie zur Formatierung einer Websuche nach <code>QDate::toString</code> durch. Wenn das Feld leer gelassen wird, wird normalerweise eine gebietsschemaspezifische Zeichenfolge verwendet.
<code>root/time/dateTimeFormatLong</code>	Eine optionale Methode zum Überschreiben des langen Datums- und Uhrzeitformats, das in verschiedenen ThinPro Tools verwendet wird. Führen Sie zur Formatierung einer Websuche nach <code>QDate::toString</code> durch. Wenn das Feld leer gelassen wird, wird normalerweise eine gebietsschemaspezifische Zeichenfolge verwendet.
<code>root/time/dateTimeFormatShort</code>	Eine optionale Methode zum Überschreiben des langen Datums- und Uhrzeitformats, das in verschiedenen ThinPro Tools verwendet wird. Führen Sie zur Formatierung einer Websuche nach <code>QDate::toString</code> durch. Wenn das Feld leer gelassen wird, wird normalerweise eine gebietsschemaspezifische Zeichenfolge verwendet.
<code>root/time/hideCountries</code>	Eine durch Semikolons getrennte Liste der Länder, die in der grafischen Benutzeroberfläche für die Auswahl der Zeitzone verborgen werden sollen.
<code>root/time/hideWinZones</code>	Eine durch Semikolons getrennte Liste der Zeitzonen im Windows Format (beispielsweise „(UTC+2:00) Tripoli“), die in der grafischen Benutzeroberfläche für die Auswahl der Zeitzone verborgen werden sollen.
<code>root/time/hideZones</code>	Eine durch Semikolons getrennte Liste der Zeitzonen im Linux Format (beispielsweise „America/Denver“), die in der grafischen Benutzeroberfläche für die Auswahl der Zeitzone verborgen werden sollen.
<code>root/time/timeFormatLong</code>	Eine optionale Methode zum Überschreiben des langen Uhrzeitformats, das in verschiedenen ThinPro Tools verwendet wird. Führen Sie zur Formatierung einer Websuche nach <code>QDate::toString</code> durch. Wenn das Feld leer gelassen wird, wird normalerweise eine gebietsschemaspezifische Zeichenfolge verwendet.
<code>root/time/timeFormatShort</code>	Eine optionale Methode zum Überschreiben des kurzen Uhrzeitformats, das in verschiedenen ThinPro Tools verwendet wird. Führen Sie zur Formatierung einer Websuche nach <code>QDate::toString</code> durch. Wenn das Feld leer gelassen wird,

Registrierungsschlüssel	Beschreibung
	wird normalerweise eine gebietsschemaspezifische Zeichenfolge verwendet.
<code>root/time/timezone</code>	Legt die Zeitzone fest. Zeitzonen sollten angegeben werden, wie von Linux Zeitzone im Tool für Datum und Uhrzeit in der Systemsteuerung definiert und sollten folgendes Format aufweisen: <Region>/<Teilregion>.
<code>root/time/use24HourFormat</code>	Wenn der Wert -1 ist, wählt das System das Format automatisch entsprechend dem Gebietsschema. Wenn der Wert 0 ist, wird das englische Format a.m./p.m. verwendet. Wenn der Wert 1 ist, wird das 24-Stunden-Format verwendet.
<code>root/time/useADNSTimeServers</code>	Wenn der Wert 1 ist, versucht er Thin Client die Zeitzone über die Active Directory Domänencontroller festzulegen, die im lokalen Netzwerk automatisch erkannt wurden. Dies erfolgt mithilfe der folgenden DNS-Abfrage für SRV-Einträge: _ldap._tcp.dc._msdcs.domain.
<code>root/time/useDHCPTimezone</code>	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 <code>tcode</code> weiterleitet (was normalerweise die Kennung 101 ist, jedoch auch 100 und 2 sein kann).
<code>root/time/useNTPServers</code>	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 <code>NTPServers</code> angegeben ist.

touchscreen

Registrierungsschlüssel	Beschreibung
<code>root/touchscreen/beep</code>	Definiert, ob der Thin Client piept, wenn der Touchscreen verwendet wird.
<code>root/touchscreen/calibrated</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/touchscreen/enabled</code>	Wenn der Wert 1 ist, wird die Eingabe per Touchfunktion deaktiviert.
<code>root/touchscreen/maxx</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/touchscreen/maxy</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/touchscreen/minx</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

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

translation

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

usb-update

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

users

Registrierungsschlüssel	Beschreibung
root/users/gui/hptc-user-rights/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/gui/hptc-user-rights/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/gui/hptc-user-rights/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/root/enablePassword	Wenn diese Option aktiviert ist, werden Anmeldungen beim lokalen Administratorstammkonto ermöglicht. Wenn diese Option deaktiviert ist, können nur Active Directory Administratoren den Wechsel des Thin Client in den Administratormodus initiieren.
root/users/root/password	Legt das Administrator Kennwort fest. Wenn kein Wert angegeben ist, ist der Administratormodus gesperrt.
root/users/root/timeout	Gibt die Leerlaufzeitüberschreitung (in Minuten) an, nach der die Ausführung im Administratormodus beendet wird. Wenn der Wert 0 oder eine negative Zahl ist, wird die Ausführung im Administratormodus nicht automatisch beendet.
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	Wenn der Wert 1 ist, können Endbenutzer auf das Element AD/DDNS Manager in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-agent-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element HPDM Agent in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-auto-update/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Automatic Update in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-background-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Hintergrund-Manager in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-cert-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Zertifikat-Manager in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-clientaggregation-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Clientaggregation in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-date-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Datum und Uhrzeit in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-dhcp-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element DHCP-Optionen in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-display-prefs/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Anzeigeeinstellungen in der Systemsteuerung zugreifen.

Registrierungsschlüssel	Beschreibung
root/users/user/apps/hptc-easy-update/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Easy Update in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-energy-star/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Energy Star in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-il8n-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Sprache in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-keyboard-layout/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Tastaturlayout in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-mixer/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Sound in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-mouse/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Maus in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-network-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Netzwerk-Manager in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-power-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Energieverwaltung in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-printer-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Drucker in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-restore/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Schnappschüsse in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-screenlock/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Energieverwaltung in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-security/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Sicherheit in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-shortcut-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Tastenkombinations-Manager in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-sshd-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element SSHD-Manager in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-task-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Task-Manager in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-text-editor/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Text-Editor in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-thinstate/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element ThinState in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-touchscreen/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Touchscreen in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-usb-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element USB-Manager in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-user-rights/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element Anpassungscenter in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-vncshadow/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element VNC-Shadow in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-xterm/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element X-Terminal in der Systemsteuerung zugreifen.

Registrierungsschlüssel	Beschreibung
	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	Wenn der Wert 1 ist, können Endbenutzer auf das Element Einrichten der SCIM-Eingabemethode in der Systemsteuerung zugreifen.
root/users/user/enablePassword	Wenn diese Option aktiviert ist, werden Anmeldungen beim lokalen freigegebenen Konto Benutzer ermöglicht.
root/users/user/hideDesktopPanel	Wenn der Wert 1 ist, 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, wird Connection Manager 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	Wenn der Wert 1 ist, ist der Wechsel in den 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.

vncserver

Registrierungsschlüssel	Beschreibung
root/vncserver/coreSettings/enableVncShadow	Wenn der Wert 1 ist, dann ist der VNC-Shading-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/vncAllowLoopbackOnly	Wenn der Wert 1 ist, sind nur localhost- oder Loopbackadresse für VNC-Verbindungen zulässig.
root/vncserver/coreSettings/vncDefaultNumLockStatus	Wenn der Wert 1 ist, ist num-Modus standardmäßig aktiviert. Wenn der Wert 0 ist, ist num-Modus standardmäßig deaktiviert.
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.

Registrierungsschlüssel	Beschreibung
<code>root/vncserver/coreSettings/vncNotifyTimeout</code>	Legt die Zeitüberschreitung in Sekunden für das Dialogfeld für die Benachrichtigung fest, die dem Benutzer angezeigt wird, wenn jemand versucht, sich via VNC mit dem Thin Client zu verbinden.
<code>root/vncserver/coreSettings/vncNotifyUser</code>	Wenn der Wert 1 ist, wird dem Benutzer eine Benachrichtigung angezeigt, wenn jemand versucht, sich via VNC mit den Thin Client zu verbinden.
<code>root/vncserver/coreSettings/vncPassword</code>	Legt das Kennwort für VNC-Shadowing fest. Der Schlüssel <code>VncUsePassword</code> muss ebenfalls aktiviert werden.
<code>root/vncserver/coreSettings/vncReadOnly</code>	Wenn der Wert 1 ist, dann wird VNC-Shadowing im nur-Ansicht-Modus arbeiten.
<code>root/vncserver/coreSettings/vncRefuseInDefault</code>	Wenn der Wert 1 ist, werden VNC-Anforderungen automatisch abgelehnt, wenn der Benutzer nicht vor Ablauf des Zeitlimits mit dem Benachrichtigungsdialog interagiert.
<code>root/vncserver/coreSettings/vncStopButton</code>	Wenn der Wert 1 ist, wird in der linken Ecke des Bildschirms eine Immer-im-Vordergrund-Schaltfläche angezeigt. Durch Klicken auf diese Schaltfläche, wird die Verbindung zur VNC-Sitzung unterbrochen.
<code>root/vncserver/coreSettings/vncTakeEffectRightNow</code>	Wenn der Wert 1 ist, dann werden VNC-Einstellungen sofort wirksam, nachdem sie geändert wurden.
<code>root/vncserver/coreSettings/vncUsePassword</code>	Wenn der Wert 1 ist, dann ist das in <code>VncPassword</code> angegebene Kennwort für VNC-Shadowing erforderlich.
<code>root/vncserver/coreSettings/vncUseSSL</code>	Wenn der Wert 1 ist, dann wird SSL für VNC-Verbindungen verwendet.
<code>root/vncserver/gui/VNCShadowManager/name</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/vncserver/gui/VNCShadowManager/status</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/vncserver/gui/VNCShadowManager/title</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/vncserver/gui/VNCShadowManager/widgets/enableVncShadow</code>	Zum Einstellen des Status für das Widget VNC-Shadow aktivieren im VNC Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/userNotificationMessage</code>	Zum Einstellen des Status für das Widget Benutzerbenachrichtigung im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/vncAllowLoopbackOnly</code>	Zum Einstellen des Status für das Widget Nur Loopbackverbindungen zulassen im VNC-Shadow-Dienstprogramm. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das

Registrierungsschlüssel	Beschreibung
	Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncNotifyShowTimeout</code>	Zum Einstellen des Status für das Widget VNC-Zeitlimit für Benachrichtigung anzeigen im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncNotifyTimeout</code>	Zum Einstellen des Status für das numerische Widget im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncNotifyUser</code>	Zum Einstellen des Status für das Widget VNC: Benutzer benachrichtigen, um Ablehnung zuzulassen im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncPassword</code>	Zum Einstellen des Status für das Widget Kennwort festlegen im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncReadOnly</code>	Zum Einstellen des Status für das Widget VNC: Schreibgeschützt im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncRefuseInDefault</code>	Zum Einstellen des Status für das Widget Verbindungen standardmäßig verweigern im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/vncStopButton</code>	Zum Einstellen des Status für das Widget VNC: Schaltfläche „Shadowing stoppen“ im VNC Shadow-Dienstprogramm. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncTakeEffectRightNow</code>	Zum Einstellen des Status für das Widget VNC-Server jetzt zurücksetzen im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung

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

Index

A

- Active Directory 59
- Add-Ons 1
- Administratormodus 3
- Aktualisieren von Thin Clients
 - Aktualisieren per DHCP-Kennung 73
 - Aktualisieren per DNS-Alias 74
 - Aktualisierung per Übertragung 73
 - Manuelle Aktualisierung 74
- Anzeigeeinstellungen 50
- Anzeigeprofile 50
- Audioeinstellungen 47
- Audioumleitung
 - RDP 25
 - VMware Horizon View 32
- Auslieferungszustand 60

B

- Background Manager 52
- Benutzermodus 3
- Benutzeroberfläche
 - Connection Manager (nur ThinPro) 8
 - Desktop 5
 - Taskleiste 6
 - Übersicht 5
- Betriebssystemkonfiguration, Auswählen 2
- Bildschirmschoner-Einstellungen 52

C

- Certificate Manager 67
- Citrix
 - Einstellungen, allgemeine 11
 - Einstellungen, pro Verbindung 14
 - HP True Graphics 42
- Clientaggregation 48
 - Clientkonfiguration 49
 - Serverkonfiguration 50
- Clientprofil
 - Anpassung 76

- Hinzufügen eines symbolischen Links 78
- Hinzufügen von Dateien 77
- Laden 76
- Registrierungseinstellungen 77
- Speichern 79
- Zertifikate 77
- Custom-Verbindungen 41

D

- Datums- und Uhrzeiteinstellungen 52
- DHCP-Optionen 68
- Drucker 51
- Druckerkonfiguration 79
- Druckerumleitung
 - RDP 24
 - VMware Horizon View 32

E

- Einführung 1
- Energieverwaltung 52
- Energieverwaltungseinstellungen 52

F

- Fehlerbeseitigung 81
 - Netzwerkverbindung 81
 - verwenden der Systemdiagnose 82

G

- Geräteumleitung
 - RDP 23
 - VMware Horizon View 31

H

- HP Device Manager. *Siehe* HPDM Agent
 - Siehe auch* Remoteverwaltungsdienst
- HPDM Agent 59
- HP Smart Client Services
 - Installation 71
 - Profile Editor. *Siehe* Profile Editor

- Übersicht 71
- unterstützte Betriebssysteme 71
- Siehe auch* Remoteverwaltungsdienst
- HP TeemTalk. *Siehe* TeemTalk
- HP True Graphics 42
- HP Velocity 57

I

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

K

- Kennwörter, ändern 52
- Kioskmodus 10
- Komponenten-Manager 60
- Konfiguration eines parallelen Druckers 79
- Konfiguration eines seriellen Druckers 79

M

- Massenspeicherumleitung
 - RDP 23
 - VMware Horizon View 31
- Mauseinstellungen 47
- MMR. *Siehe* Multimedia-Umleitung
- Multimedia-Umleitung
 - RDP 22
 - VMware Horizon View 31

N

- Netzwerkeinstellungen
 - DNS 55
 - drahtgebunden 53
 - HP Velocity 57
 - IPSec 56
 - VPN 56
 - Wireless 54
 - Zugreifen 52

P

- Profile Editor 76

R

RDP

- Audioumleitung 25
 - Druckerumleitung 24
 - Einstellungen, allgemeine 16
 - Einstellungen, pro Verbindung 16
 - Geräteumleitung 23
 - Massenspeicherumleitung 23
 - Multimedia-Umleitung 22
 - RemoteFX 22
 - Sitzungen mit mehreren Monitoren 22
 - Smart Card-Umleitung 26
 - USB-Umleitung 23
- Registrierungsschlüssel 87
- RemoteFX 22
- Remoteverwaltungsdienst, Auswählen 3

S

- SCEP-Manager 67, 68
- Schnappschüsse 60
- SCIM 47
- Serial Manager 67
- Sicherheitseinstellungen 52
- Smart Card-Umleitung
- RDP 26
 - VMware Horizon View 33
- Smart Zero. *Siehe* Betriebssystemkonfiguration
- Snipping Tool 67
- Spracheinstellungen 52
- SSH 39
- SSHD-Manager 60
- Standbymodus 52
- Systemdiagnose 82
- Systemsteuerung
- Active Directory 59
 - Anpassungscenter 52
 - Anzeigeeinstellungen 50
 - Auslieferungszustand 60
 - Clientaggregation 48
 - Datum und Uhrzeit 52
 - DHCP Options Manager 68
 - Dienstprogramme, ausblenden 52
 - Einrichten der SCIM-Eingabemethode 47
 - Energieverwaltung 52

- Hintergrundeinstellungen 52
- Komponenten-Manager 60
- Maus 47
- Netzwerk 52
- SCEP-Manager 67
- Schnappschüsse 60
- Serial Manager 67
- Sicherheit 52
- Snipping Tool 67
- Sound 47
- Sprache 52
- SSHD-Manager 60
- Task-Manager 67
- Tastenkombinationen 67
- Text-Editor 67
- ThinState. *Siehe* HP ThinState
- Touchscreen 47
- Übersicht 47
- VNC-Shadow 66
- Wireless-Statistiken 60
- X-Terminal 67

T

- Task-Manager 67
- Tastenkombinationen 67
- TeamTalk 36
- Telnet 39
- Text-Editor 67
- Thin Clients
- Aktualisieren. *Siehe* Aktualisieren von Thin Clients
- ThinPro. *Siehe* Betriebssystemkonfiguration
- ThinState. *Siehe* HP ThinState
- Touchscreen-Einstellungen 47

U

- USB-Umleitung
- RDP 23
 - USB-Manager 51
 - VMware Horizon View 31

V

- Verbindungen
- Ausblenden 52
 - Erweiterte Einstellungen 9
 - Konfiguration 9
- VMware Horizon View
- Ändern von Protokollen 34
 - Audioumleitung 32
 - Druckerumleitung 32

- Einstellungen, pro Verbindung 26
- Geräteumleitung 31
- Massenspeicherumleitung 31
- Multimedia-Umleitung 31
- Sitzungen mit mehreren Monitoren 30
- Smart Card-Umleitung 33
- Tastenkombinationen 31
- USB-Umleitung 31
- Webcam-Umleitung 33
- Zertifikate 34
- VNC-Shadowing 66

W

- Web Browser
- Einstellungen, allgemeine 35
 - Einstellungen, pro Verbindung 36
- Webcam-Umleitung
- VMware Horizon View 33
- Websites
- Citrix Support 1
 - HP Support 1
 - Microsoft Support 1
 - VMware Support 1
- Weitere Informationen 1
- Wireless-Statistiken 60

X

- XDMCP 38
- X-Terminal 67

Z

- Zertifikate
- Installation 67
 - VMware Horizon View 34