HP Smart Zero Core 4.3

Administratorhandbuch

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

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

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

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

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

Zweite Ausgabe: August 2013

Erste Ausgabe: Mai 2013

Teilenummer des Dokuments: 727358-042

Inhaltsverzeichnis

1 Willkommen 1
Zielgruppe 1
Dokumentorganisation 1

2 Einführung 3
Anmelden am Desktop 3
Auswahl eines Verbindungstyps 3
Konfigurieren einer Basisverbindung 3
Arbeiten mit dem Desktop 4

3 In Clients navigieren 5
Verwenden der Client-Symbolleiste 5
Beschreibung des Symbols Systemstatus 5
Verwenden von Client-Informationsbildschirmen 6
Verwenden der Registerkarte Status 6
Verwenden der Registerkarte Netzwerk 7
Verwenden der Registerkarte Net Tools 7
Verwenden der Registerkarte Systeminformationen 8
Verwenden der Registerkarte Systemprotokolle 8
Client-Informationsbildschirme ausblenden 9

4 Cients konfigurieren 10
Verwenden des Client-Bedienfelds 10
Zugriff auf das Client-Bedienfeld 10
Verwenden des Client-Bedienfelds (Benutzermodus) 10
Hauptbedienfeld-Optionen (Benutzermodus) 10
Zusätzliche Bedienfeldoptionen (Benutzermodus) 11
Verwenden des Client-Bedienfelds (Administratormodus) 12
Hauptbedienfeld Optionen (Administratormodus) 12
Zusätzliche Bedienfeldoptionen (Administratormodus) 13
Übersicht über RDP-Verbindungsfunktionen 16
Verwenden des Kioskmodus mit RDP 16
Verwendung von RemoteFX mit RDP 17
Verwenden der Multimedia-Umleitung mit RDP 17
Verwenden von Multi-Monitor-Sitzungen mit RDP 18
Verwenden der Geräteumleitung mit RDP 18

Verwenden einer USB-Umleitung mit RDP ... 18
Verwenden der Massenspeicherumleitung mit RDP ... 19
Verwenden der Druckerumleitung mit RDP ... 19
Audioumleitung mit RDP verwenden ... 20
Smart Card-Umleitung mit RDP verwenden ... 20
Festlegen von RDP-Optionen ... 21
Übersicht über Citrix-Verbindungsfunktionen ... 21
Funktionen der Citrix-Verbindungsverwaltung ... 22
Citrix-Receiver-Funktionen ... 22
HDX MediaStream-Supportmatrix ... 23
Citrix-Verbindung-Supportmatrix ... 23
Übersicht über die VMware Horizon View-Verbindungsfunktionen ... 24
Verwenden des Kiokskmodus mit VMware Horizon View ... 24
Verwenden der Multimedia-Umleitung mit VMware Horizon View ... 25
Verwenden von Multi-Monitor Sitzungen mit VMware Horizon View ... 25
Verwenden von Tastaturkürzeln mit VMware Horizon View ... 25
Geräte-Umleitung mit VMware Horizon View verwenden ... 25
USB-Umleitung mit VMware Horizon View verwenden ... 25
Massenspeicher-Umleitung mit VMware Horizon View verwenden ... 26
Drucker-Umleitung mit VMware Horizon View verwenden ... 26
Audioumleitung mit VMware Horizon View verwenden ... 26
Smart Card-Umleitung mit VMware Horizon View verwenden ... 27
Webcam-Umleitung mit VMware Horizon View verwenden ... 28
Erweiterte Verbindungsoptionen für VMware Horizon View ... 28
Mithilfe erweiterter Befehlszeilenargumente mit VMware mit mehr Komfort anzeigen ... 29
Ein Teradici-beschleunigtes t410-System mit VMware Horizon View verwenden. ... 29
Umschalten zum standardmäßigen VMware Horizon View-Client ... 29
Ändern des VMware Horizon View Protokolltyps ... 30
Zertifikate auf Clients installieren ... 30
Anforderungen für die VMware Horizon View HTTPS- und Zertifizierungsverwaltung ... 31
USB-Geräte umleiten ... 32
Zuordnen eines seriellen oder parallelen Druckers ... 32

5 Fehlerbeseitigung von Clients ... 34
Fehlerbeseitung der Netzwerkverbindung ... 34
Fehlerbeseitigung bei Firmware-Beschädigung ... 35
Re-Imaging der Client-Firmware des Geräts ... 35
Fehlerbeseitigung bei der Konfiguration eines seriellen oder parallelen Druckers ... 35
Fehlerbehebung bei abgelaufenen Citrix-Kennwörtern ... 36
Verwenden Systemdiagnose für die Fehlerbeseitigung ... 36

Speichern von Systemdiagnosedaten 36
Dekomprimieren der Systemdiagnosedateien 36
Dekomprimieren der Systemdiagnosedateien auf Windows-basierten Systemen 37
Dekomprimieren der Systemdiagnosedateien auf Linux- oder Unix-basierten Systemen 37
Anzeigen der Systemdiagnosedateien 37
Anzeigen von Dateien im Ordner Befehle 37
Anzeigen von Dateien im Ordner /var/log 37
Anzeigen von Dateien im Ordner /etc 37

6 HP Smart Zero Client Services 38
Unterstützte Betriebssysteme 38
Vorbereitung zum Installieren von HP Smart Zero Client Services 39
Herunterladen und Installieren von HP Smart Zero Client Services 39

7 Verwenden des Profile Editors 40
Zugriff auf den Profile Editor 40
Laden eines Client-Profils 40
Ändern eines Client-Profils 40
Auswahl der Plattform eines Client-Profils 41
Auswahl des Verbindungstyps eines Client-Profils 41
Ändern der Einstellungen der Registrierung eines Client-Profil 41
Aktivieren oder deaktivieren der Menüoptionen auf Clients 41
Aktivieren oder deaktivieren der Benutzerkonfigurationen auf Clients 42
Hinzufügen von Dateien zu einem Client-Profil 42
Hinzufügen einer Konfigurationsdatei zu einem Client-Profil 42
Zertifikate zu einem Client-Profil hinzufügen 43
Hinzufügen eines symbolischen Links zu einem Client-Profil 43
Speichern des Client-Profils 44
Konfigurieren eines seriellen oder parallelen Druckers 44
Abrufen der Drucker-Baudrate 44
Einrichten von Druckeranschlüssen 44
Drucker auf dem Server installieren 45

8 Automatic Intelligence verwenden 46
Anzeigen der Automatic Update-Website 46
Ein Automatic Update-Profil erstellen 46
Clients aktualisieren 47
Verwenden der Methode Aktualisierung per Übertragung 47
Verwenden der Aktualisierungsmethode mit der DHCP-Kennung 47

Beispiel für die Durchführung DHCP-Kennung 47
Verwenden der Aktualisierungsmethode mit DNS Alias 48
Verwenden der manuellen Aktualisierungsmethode 48
Eine manuelle Aktualisierung durchführen 48
Verwenden des HP Intelligent Delivery-Dienstes 49
Wie der HP Intelligent Delivery-Dienst funktioniert 49
Starten, anhalten und beenden des HP Intelligent Delivery-Dienstes 49
Anzeigen des Anwendungsprotokolls des HP Intelligent Delivery-Dienstes 49
HP Intelligent Delivery Service-Registrierungsschlüssel 50
Verwenden des HP Device Manager 50

Anhang A Client-Tastatursprache 51

Anhang B Anpassen des Client-Anmeldebildschirms 53
Anpassen des Bildschirmhintergrunds 53
Gemeinsame Attribute 53
Elemente 56
Image 58
Text 59
Anpassen des Dialogfeld für die Client-Anmeldung 61
Anpassen des zentralen Rahmen 62
Anpassen des Text für die Kopfzeile 62
Anpassen des Symbold für den Header 63

Anhang C HP Smart Zero Core-Registrierungseinstellungen 64
root > Audio 64
root > ConnectionManager 65
root > ConnectionType 66
root > ConnectionType > freerdp 66
root > ConnectionType > view 72
root > ConnectionType > xen 76
root > Display 87
root > Network 88
root > USB 92
root > keyboard 92
root > logging 93
root > mouse 94
root > printer-mapping-mgr 94
root > printers 94
root > screensaver 95

root > time 95
root > translation 96
root > users 97
root > zero-login 99

Anhang D VMware Horizon View-USB-Konfiguration 102
USB-Optionen in vorhergehenden-Releases 102
VMware Horizon View-USB-Gerätefamilien 102

Index 104

1 Willkommen

Dieses Handbuch ist eine umfassende Referenz zur Beschreibung, wie HP Smart Zero Core auf HP Smart Zero-Clients verwaltet wird. Außerdem enthält es Informationen über die Softwarevoraussetzungen und die Installationsaufgaben im Zusammenhang mit einer Standard- oder benutzerdefinierten Serverinstallation .

Zielgruppe

Dieses Handbuch ist für Administratoren und technische Mitarbeiter vorgesehen, die für die Installation, Konfiguration und Verwaltung von HP Smart Zero-Clientsystemen verantwortlich sind.

Dokumentorganisation

Dieses Handbuch ist in die folgenden Kapitel und Anhänge unterteilt:

- „Einführung“ auf Seite 3 – Beschreibt, wie Sie sich am Desktop anmelden und ihn verwenden und wie eine Basisverbindung konfiguriert wird.
- „In Clients navigieren“ auf Seite 5 – Bietet eine Überblick über die Client-Symbolleiste und Informationsbildschirme.
- „Cients konfigurieren“ auf Seite 10 – Beschreibt die im Client-Bedienfeld verfügbaren Einestellungen, einen Überblick über Verbindungsmerkmale und andere Konfigurationen wie z. B. Geräteumleitungen und Druckeranschlusszuordnung.
- „Fehlerbeseitigung von Clients“ auf Seite 34 – Beschreibt häufige Probleme und Lösungen bei der Fehlerbeseitigung.
- „HP Smart Zero Client Services“ auf Seite 38 – Beschreibt Softwareanforderungen und bietet Informationen zur Verwendung des Installationsassistenten zur Durchführung einer Standardinstallation und einer benutzerdefinierten Installation, sowie zum erstmaligen Start eines HP Smart Zero-Client.
- „Verwenden des Profile Editors“ auf Seite 40 – Beschreibt die Verwendung des Profile Editors zum Einrichten und Bearbeiten von Client-Profilen, die Verbindungsinformationen, Einstellungen und Dateien enthalten, die beim Selbstkonfigurationsvorgang verwendet werden.
- „Automatic Intelligence verwenden“ auf Seite 46 – Definiert die Automatic Intelligence - Verzeichnisstruktur und wie Konfigurationsdateien an ein Profil angehängt werden. Außerdem wird beschrieben, wie Sie die HP Smart Zero Client Services-Website anzeigen und Client-Profile, die auf dem Automatic Intelligence-Server gespeichert sind, remote verwalten können.
- „Client-Tastatursprache“ auf Seite 51 – Liste der Sprachoptionen für die Client-Tastatur.
- „Anpassen des Client-Anmeldebildschirms“ auf Seite 53 – Beschreibt die gängigen Attribute und Elemente, die bei der Anpassung des Bildschirmhintergrunds für die Client-Anmeldung verwendet werden.
- „HP Smart Zero Core-Registrierungseinstellungen“ auf Seite 64 – Liste der HP Smart Zero Core-Registrieungseinstellungen. Die Tabellen in diesem Abschnitt beschreiben den

Registrierungsschlüsselpfad, die Anwendungsfunktionen und Optionen wie sie in der Komponente Registrierungseditor des Profile-Editor vorgestellt werden.

- „VMware Horizon View-USB-Konfiguration“ auf Seite 102 – Beschreibt die USB-Konfiguration für VMware Horizon View.

2 Einführung

In diesem Kapitel werden folgende Themen behandelt:

- Anmelden am Desktop
- Konfigurieren einer Basisverbindung
- Arbeiten mit dem Desktop

Anmelden am Desktop

Während des Systemstarts versucht der Client eine Verbindung zu erkennen und die Einstellungen automatisch zu installieren. Wenn Sie zuvor den Client entweder über HP Smart Zero Client Services oder HP Device Manager, konfiguriert haben, melden Sie sich mithilfe des standardmäßigen Anmeldebildschirm beim Desktop an.

Auswahl eines Verbindungstyps

Für kleine Deployments, bei denen Sie keine Geräteverwaltung brauchen, wird der Bildschirm **Select Connection Type** (Verbindungstyp auswählen) beim ersten Einrichten angezeigt. Verwenden Sie diesen Bildschirm zur Auswahl des zu verwendenden Verbindungstyps.

Die folgenden Standard-Verbindungstypen sind verfügbar:

- Citrix
- Microsoft RDP7
- VMware Horizon View
- Internetbrowser

TIPP: Im Anmeldedialog zeigt ein gelbes Warnsymbol an, dass Sie keinen HP Smart Zero Client Services-Server konfiguriert haben. In diesem Fall kann der Client einen Aktualisierungsserver nicht automatisch erkennen. Um diese Benachrichtigung zu deaktivieren, führen Sie einen der folgenden Schritte aus:

Konfigurieren Sie einen HP Smart Zero Client Services-Server wie in „HP Smart Zero Client Services“ auf Seite 38 beschrieben.

- oder -

Deaktivieren Sie im Menü Konfiguration, im Dialog **Zusätzliche Konfiguration > Automatic Update** die automatischen Updates.

Konfigurieren einer Basisverbindung

So konfigurieren Sie eine Basisverbindung:

1. Klicken Sie im Bildschirm **Connection Selection** (Verbindungsauswahl) auf die Art von Verbindung, die Sie verwenden möchten.
2. Geben Sie im Dialogfeld **Remote Connection Server** (Remote-Verbindungsserver) unter Servername oder Adresse eine der folgenden Optionen ein:

- Server URL (Server-URL)
- Server Hostname (Host-Name des Servers)
- Server-IP-Adresse

3. Klicken Sie auf **OK**.
4. Melden Sie sich mit Hilfe der folgenden Informationen am Desktop an:
   - Benutzername
   - Kennwort
   - Domäne

HINWEIS: Sie müssen die Verbindung nur einmal konfigurieren. Die Konfiguration wird für zukünftige Sitzungen gespeichert. Zum Ändern der Verbindung wählen Sie **Select Connection Type** (Verbindungstyp auswählen) aus dem Konfigurationsmenü.

Arbeiten mit dem Desktop

Desktops starten in der Regel auf allen verfügbaren Monitoren mit Vollbild.

Um von einem Vollbild-Remote-Desktop zu einem lokalen Desktop zurückzukehren, verwenden Sie diese Verknüpfung:

▲ Drücken Sie Strg+Alt+Ende.

Um zwischen Desktop-Systemen umzuschalten, verwenden Sie diese Verknüpfung:

▲ Drücken Sie Strg+Alt+Tab.

TIPP: Zum konfigurieren von Verknüpfungen verwenden Sie die Systemsteuerung,

3 In Clients navigieren

In diesem Kapitel werden folgende Themen behandelt:

- Verwenden der Client-Symbolleiste
- Verwenden von Client-Informationsbildschirmen

Verwenden der Client-Symbolleiste

Verwenden Sie die Client-Symbolleiste, um auf die Client-Menüs zuzugreifen und Informationen über den Systemstatus erhalten.

Tabelle 3-1 Client-Symbolleiste

Element	Beschreibung
	Einschalten, Neu starten oder Ausschalten des Client.
	Zeigt die Client-Systemsteuerung. Nähere Informationen hierzu finden Sie hier: Verwenden des Client-Bedienfelds auf Seite 10.
	Zeigt den Bildschirm **About this Client** (Über diesen Client). Weitere Informationen hierzu finden Sie unter Verwenden von Client-Informationsbildschirmen auf Seite 6.
	Entspricht dem Status Ihres Systems. Weitere Informationen hierzu finden Sie unter Beschreibung des Symbols Systemstatus auf Seite 5.
	Startet oder stoppt die Verbindung oder setzt sie zurück.

Beschreibung des Symbols Systemstatus

Die Client-Symbolleiste zeigt ein Systemstatus-Symbol, das dem Systemstatus entspricht. Um detaillierte Informationen abzurufen, klicken Sie auf das Symbol Systemstatus.

Tabelle 3-2 Informationen über das Symbol Systemstatus

Systemstatus	Beschreibung
Fehler	Ein **X** zeigt an, das ein kritischer Fehler aufgetreten ist, wie beispielsweise eine fehlende Netzwerkverbindung.
Warnung	Ein **yellow triangle** (gelbes Dreieck) zeigt an, dass ein nicht-kritischer Fehler aufgetreten ist, wie z. B. das Unvermögen, einen Client-Service zu kontaktieren. Durch Klicken auf das Symbol wird der Warnungsstatus gelöscht.
Beschäftigt	Ein **spinning circle** (sich drehender Kreis) zeigt an, dass der Client beschäftigt ist und keine Fehler vorhanden sind. Dieser Status wird angezeigt, wenn eine Verbindung gestartet wird oder eine andere Aktivität auftritt.

Tabelle 3-2 Informationen über das Symbol Systemstatus (Fortsetzung)

Systemstatus	Beschreibung
Leerlauf	Ein **question mark** (Fragezeichen) zeigt an, dass sich der Client im Leerlauf befindet und keine Fehler vorliegen. Klicken Sie für weitere Informationen auf das Symbol.
Aktualisieren	**Spinning arrows** (Sich drehende Pfeile) zeigen an, dass der Client ein Update von HP Smart Zero Client Services empfängt oder installiert.

Verwenden von Client-Informationsbildschirmen

So greifen Sie auf die Client-Informationsbildschirme zu

▲ Klicken Sie auf der Client-Symbolleiste auf  .

Weitere Informationen zu den auf dem Bildschirm **About this Client** (Über diesen Client) verfügbaren Registerkarten finden Sie in den folgenden Abschnitten:

- Verwenden der Registerkarte Status
- Verwenden der Registerkarte Netzwerk
- Verwenden der Registerkarte Net Tools
- Verwenden der Registerkarte Systeminformationen
- Verwenden der Registerkarte Systemprotokolle
- Client-Informationsbildschirme ausblenden

Verwenden der Registerkarte Status

Verwenden Sie die Registerkarte **Status**, um Probleme bezüglich des Netzwerks des Systems, des Client-Service und der Client-Konnektivität zu überwachen und zu identifizieren.

Die folgende Tabelle beschreibt die auf dieser Registerkarte angezeigten Elemente.

Tabelle 3-3 Über diesen Client – Status

Element	Beschreibung
Netzwerk	Zeigt ein grünes Häkchen, wenn das System ordnungsgemäß funktioniert, sowie folgende Informationen: • IP-Adresse • Gateway • MAC-Adresse Wenn das Client-Netzwerk nicht ordnungsgemäß funktioniert, zeigt dieses Element möglicherweise eine Warnung oder einen Fehlerstatus und eine Fehlermeldung.
Smart Client Service	Zeigt ein grünes Häkchen, wenn alles normal ist und erzeugt eine Systemmeldung mit dem Namen des konfigurierten HP Smart Zero Client Services-Server an. Wenn HP Smart Zero Client Services nicht richtig konfiguriert ist oder auf einen ungültigen Server zeigt, wird einer der folgenden Fehler angezeigt:

Tabelle 3-3 Über diesen Client – Status (Fortsetzung)

Element	Beschreibung
	• Ein **X** und die Fehlermeldung zeigen an, dass beim Versuch, die Client-Einstellungen vom Server abzurufen, ein Fehler aufgetreten ist. • Ein Warnhinweis zeigt an, dass ein Fehler aufgetreten ist, während versucht wurde, die Client-Einstellungen vom Server abzurufen.
Verbindung	Zeigt ein grünes Häkchen an, wenn der Client mit dem Server verbunden ist. Wenn die Verbindung falsch eingerichtet ist oder auf einen ungültigen Server zeigt, wird einer der folgenden Fehler angezeigt: • Ein **X** zeigt an, dass für Ihr System noch keine eine Verbindung konfiguriert wurde. • Ein Warnhinweis zeigt an, dass beim Versuch, eine Verbindung mit dem Server herzustellen, ein Fehler aufgetreten ist.

Verwenden der Registerkarte Netzwerk

Verwenden Sie die Registerkarte **Netzwerk** zur Anzeige der Netzwerk- und Schnittstellen-Einstellungen in drei unterschiedlichen Bereichen, wie in der folgenden Tabelle beschrieben.

Tabelle 3-4 Über diesen Client – Netzwerk

Bereich	Element
Schnittstelle	• Name • Status • IP-Adresse • Netzwerkmaske • MAC-Adresse • DHCP-Server-Adresse • Schnittstellenstatistik
Netzwerk	• Standard-Gateway
DNS-Einstellungen	• Host-Name • Standarddomäne • Nameserver

Verwenden der Registerkarte Net Tools

Verwenden Sie die Registerkarte **Net Tools** (Netzwerkzeuge), um Optionen für die Überwachung der Systemleistung und zum Beheben von Netzwerkproblemen zu konfigurieren:

1. Wählen Sie auf der Registerkarte **Net Tools** (Netzwerkzeuge) unter **Select Tool** (Werkzeug auswählen) eine der Optionen aus der folgenden Tabelle aus.

Tabelle 3-5 **Über diesen Client – Netzwerkzeuge**

Option	Beschreibung
Ping	Verwenden Sie dieses Werkzeug, um Kontakt mit einem anderen Gerät im Netzwerk aufzubauen und geben Sie dazu eine entsprechende IP-Adresse an. • Wenn diese Verbindung erfolgreich hergestellt werden konnte, gibt das Werkzeug die Gesamtzeit in Millisekunden an, die benötigt wurde, um eine Antwort von diesem Gerät zu empfangen. • Wenn dies fehlschlägt, gibt das Tool keine Daten zurück
DNS-Suche	Verwenden Sie dieses Werkzeug zum Auflösen eines Domänennamens in eine IP-Adresse, mithilfe der DNS-Nameserver, die auf der Registerkarte **Netzwerk** registriert sind. Das Werkzeug gibt die IP eines Servers zurück, wenn die IP aufgelöst werden konnte. Andernfalls werden ein Fehlercode und eine Meldung zurückgegeben.
Trace Route (Route verfolgen)	Verwenden Sie dieses Werkzeug, um den Pfad nachzuverfolgen, auf dem ein Netzwerkpaket von einem Gerät zum anderen gesendet wird. • Falls dies erfolgreich ist, gibt das Werkzeug den Pfad an, auf dem die Daten über alle Router und Netzwerkgeräte bis hin zum Zielgerät gesendet wurden. • Wenn dies fehlschlägt, gibt das Werkzeug eine Fehlermeldung zurück.

2. Geben Sie die Optionen ein oder wählen Sie die Optionen aus, die Sie überwachen wollen.
3. Klicken Sie nach Abschluss auf **Start Process** (Prozess starten).

Verwenden der Registerkarte Systeminformationen

Die Registerkarte **Systeminformationen** bietet die folgenden Informationen über Ihren Client:

- Plattform
- RAM insgesamt
- Seriennummer
- OS Kernel Version (Kernel-Version des Betriebssystems)
- OS Build ID (Build-ID des Betriebssystems)
- Wichtige installierte Software

Verwenden der Registerkarte Systemprotokolle

Die Registerkarte **Systems Logs** (Systemprotokolle) zeigt alle folgenden Protokolle an:

- Systemkernel
- X-Server
- HP Smart Zero Client Services

HINWEIS: Um zusätzliche Diagnoseberichte oder Protokollinformationen zu erzeugen, wählen Sie **Enable Debug Mode** (Debug-Modus aktivieren). Diese Informationen können von HP angefordert werden, um die Fehlerbeseitigung zu starten.

Client-Informationsbildschirme ausblenden

1. Klicken Sie auf , wählen Sie **Administrator/User Mode Switch** (Wechsel zwischen Administrator-/Benutzer-Modus) aus, und melden Sie sich dann als Administrator an.
2. Wählen Sie unter die Menüoptionen **Additional Configuration > Advanced > XTerminal** (Zusätzliche Konfiguration > Erweitert > XTerminal) aus.
3. Geben Sie in der Befehlszeile des XTerminal `regeditor` ein, und drücken Sie dann die Eingabetaste.
4. Wählen Sie im Registrierungseditor unter **Smart Client Registry > root/SystemInfo/Pages** das Element entsprechend der Registerkarte aus, die Sie ausblenden möchten.
   - General
   - NetTools
   - Network
   - SoftwareInformation
   - SystemLogs
5. Legen Sie den Wert auf **0**, fest und klicken Sie dann auf **Speichern**.
6. Nach Abschluss starten Sie das System neu.

4 Cients konfigurieren

Für jeden unter „Einführung“ auf Seite 3 beschriebenen Verbindungstyp sind außer dem grundlegenden Setup noch viele zusätzliche Optionen verfügbar. Diese Optionen bieten viele einzigartige Systemkonfigurationen und stellen sicher, dass der Client für die meisten Umgebungen angepasst werden kann.

Dieses Kapitel enthält die folgenden Themen:

- Verwenden des Client-Bedienfelds
- Übersicht über RDP-Verbindungsfunktionen
- Übersicht über Citrix-Verbindungsfunktionen
- Übersicht über die VMware Horizon View-Verbindungsfunktionen
- Zertifikate auf Clients installieren
- USB-Geräte umleiten
- Zuordnen eines seriellen oder parallelen Druckers

Verwenden des Client-Bedienfelds

Das Client-Bedienfeld bietet Benutzern und Administratoren Zugriff auf Optionen, mit denen sie den Client konfigurieren können.

Zugriff auf das Client-Bedienfeld

Um auf das Client-Bedienfeld zuzugreifen, klicken Sie auf der Client-Symbolleiste auf  . Das Client-Bedienfeld unterstützt die folgenden Betriebsmodi:

- Benutzermodus (Standard)
- Administratormodus

Verwenden des Client-Bedienfelds (Benutzermodus)

Dieser Abschnitt beschreibt die Optionen des Client-Bedienfelds, die im Benutzermodus verfügbar sind.

Hauptbedienfeld-Optionen (Benutzermodus)

Tabelle 4-1 Hauptbedienfeld-Optionen (Benutzermodus)

Menüoption	Beschreibung
Verbindungstyp auswählen	Erlaubt die Konfiguration einer der folgenden Verbindungsarten: • Citrix • RDP7 • VMware Horizon View

Tabelle 4-1 Hauptbedienfeld-Optionen (Benutzermodus) (Fortsetzung)

Menüoption	Beschreibung
	• Internetbrowser
Wechsel zwischen Administrator-/Benutzermodus	Autorisierte Administratoren erhalten damit Zugriff auf die Menüs im Administratormodus-Bedienfeld. **HINWEIS:** Vor der Verwendung dieser Option stellen Sie sicher, dass Sie ein Kennwort für die Menüs des Administratormodus-Bedienfelds einrichten,
Sprache	Damit können Sie die Client-Bedienoberfläche in einer anderen Sprache anzeigen.
Tastaturlayout	Damit können Sie das Tastaturlayout ändern, um es der Sprache der Tastatus anzupassen.
Audio	Damit steuern Sie den Audiolevel.
Zusätzliche Konfiguration	Öffnet das Menü mit zusätzlichen Optionen. Weitere Informationen zu den zusätzlich im Benutzermodus verfügbaren Optionen finden Sie unter Zusätzliche Bedienfeldoptionen (Benutzermodus) auf Seite 11

Zusätzliche Bedienfeldoptionen (Benutzermodus)

Tabelle 4-2 Zusätzliche Bedienfeldoptionen (Benutzermodus)

Menüoption	Beschreibung
Datum und Uhrzeit	Damit können Sie das Datum und die Zeitzone mithilfe der folgenden Optionen einrichten: • Zeitzone • Zeit • Datum • Verwenden der von DHCP angegebenen NTP-Zeitserver • Zeitserver Ihrer Wahl verwenden • Keinen Zeitserver verwenden
Einstellungen anzeigen	Damit können Sie die folgenden benutzerdefinierten Optionen für Ihre Anzeigehardware konfigurieren und testen: • Auflösung • Tiefe • Ausrichtung • Primärer Videoanschluss für die Anzeige (DVI-I oder DVI-D) • Sekundärer Monitormodus
Maus	Damit können Sie benutzerdefinierte Optionen für Ihre Maushardware einrichten.
Netzwerk	Damit können Sie die folgenden Netzwerkeinstellungen konfigurieren: • Kabelgebundene Einstellungen ◦ Netzwerkgeschwindigkeit

Tabelle 4-2 Zusätzliche Bedienfeldoptionen (Benutzermodus) (Fortsetzung)

Menüoption	Beschreibung
	◦ Duplex-Einstellungen ◦ Verbindungsmethode • DNS-Einstellungen • IPSec-Einstellungen • VPN-Einstellungen • HP Velocity-Einstellungen • Wireless-Einstellungen ◦ Duplex-Einstellungen ◦ Verbindungsmethode HINWEIS: Viele Funknetzwerke sind gesichert und erfordern eine eigene Authentifizierung und ein Kennwort bzw. einen Schlüssel.
Druckerzuordnung	Damit können Sie einen Drucker einrichten und im gesamten Netzwerk freigeben.

Verwenden des Client-Bedienfelds (Administratormodus)

Dieser Abschnitt beschreibt die Optionen des Client-Bedienfelds, die im Administratormodus verfügbar sind.

So melden Sie sich als Administrator an:

1. Klicken Sie auf der Client-Symbolleiste auf  .
2. Wählen Sie im Menü **Administrator/User Mode Switch** (Wechsel zwischen Administrator-/Benutzermodus).
3. Im Feld **Switch to Admin** (Zu Admin wechseln) unter **Administrative Passwort** (Administratorkennwort) geben Sie Ihr Kennwort ein und klicken dann **auf OK**.

Hauptbedienfeld Optionen (Administratormodus)

Tabelle 4-3 Hauptbedienfeld Optionen (Administratormodus)

Menüoption	Beschreibung
Standardverbindung bearbeiten	Damit bearbeiten Sie die folgenden Standard-Verbindungseinstellungen, je nach dem vorher konfigurierten Verbindungstyp: • Netzwerk • Fenster • Optionen • Lokale Ressourcen • Darstellung • Erweitert
Wechsel zwischen Administrator-/Benutzermodus	Wechselt zurück zum Benutzermodus.

Tabelle 4-3 Hauptbedienfeld Optionen (Administratormodus) (Fortsetzung)

Menüoption	Beschreibung
Audio	Damit können Sie die Wiedergabe- und Aufnahmepegel für das Standardaudiogerät. Das Standardaudiogerät kann geändert werden durch Auswahl der Menüoption **Sound**.
Zusätzliche Konfiguration	Öffnet das Menü mit zusätzlichen Optionen. Weitere Informationen zu den zusätzlich im Administratormodus verfügbaren Optionen finden Sie unter Zusätzliche Bedienfeldoptionen (Administratormodus) auf Seite 13

Zusätzliche Bedienfeldoptionen (Administratormodus)

Die zusätzlichen Optionen, die im Administratormodus unter **Additional Configuration** (Zusätzliche Konfiguration) verfügbar sind, sind in vier Kategorien unterteilt:

- Peripheriegeräte
- Setup
- Verwaltung
- Erweitert

Die folgenden Tabellen beschreiben die verfügbaren Optionen in jeder Kategorie.

Tabelle 4-4 Zusätzliche Bedienfeldoptionen (Administratormodus) – Peripheriegeräte

Menüoption	Beschreibung
Display Preferences (Einstellungen anzeigen)	Damit können ein primäres und sekundäres Anzeigeprofil für mehrere mit dem Client verbundene Displays konfigurieren und testen. Sie können die folgenden Profilinformationen konfigurieren: • Profileinstellungen ◦ Profilname ◦ Auflösung ◦ Tiefe ◦ Ausrichtung des Hauptmonitors • Videoanschluss für primäres Display • Sekundärer Monitormodus
Tastaturlayout	Damit können Sie die folgenden benutzerdefinierten Tastaturlayout-Einstellungen konfigurieren: • Primäres und sekundäres Tastaturlayout • Layouttyp der Standardtastatur • Tastaturmodell • Tastaturvariante • Minimieren lokale Tastenkombinationen
Maus	Damit können Sie benutzerdefinierte Optionen für Ihre Maushardware einrichten.

Tabelle 4-4 Zusätzliche Bedienfeldoptionen (Administratormodus) – Peripheriegeräte (Fortsetzung)

Menüoption	Beschreibung
Druckerzuordnung	Ermöglicht das Hinzufügen, Bearbeiten und Löschen von Druckern. Klicken Sie auf **Hinzufügen**, um einen Druckers hinzuzufügen und definieren Sie die Informationen zum Drucker wie folgt: • Port • Modell • Drucker-IP-Adresse • Name der Remote-Warteschlange • Windowstreiber • Aktivieren oder Deaktivieren des Druckers Zum Bearbeiten oder Löschen eines Druckers wählen Sie einen Drucker, und klicken Sie dann **Bearbeiten** oder **Löschen**.
Sound	Damit können Sie die Audioeingangs- und Wiedergabeeinstellungen für Ihren Client einrichten.
USB-Manager	Damit können Sie die Umleitungsoptionen für USB-Geräte konfigurieren.

Tabelle 4-5 Zusätzliche Administrator-Bedienfeldoptionen – Setup

Menüoption	Beschreibung
Datum und Uhrzeit	Damit können Sie das Datum und die Zeitzone mithilfe der folgenden Optionen einrichten: • Zeitzone • Zeit • Datum • Verwenden der von DHCP angegebenen NTP-Zeitserver • Zeitserver Ihrer Wahl verwenden • Keinen Zeitserver verwenden
Sprache	Damit können Sie die Client-Bedienoberfläche in einer anderen Sprache anzeigen.

Netzwerk	Damit können Sie die folgenden Netzwerkeinstellungen konfigurieren:
	
	• Kabelgebundene Einstellungen
	  ◦ Netzwerkgeschwindigkeit
	  ◦ Duplex-Einstellungen
	  ◦ Verbindungsmethode
	• Wireless-Einstellungen
	  ◦ Verbindungsmethode

Tabelle 4-5 Zusätzliche Administrator-Bedienfeldoptionen – Setup (Fortsetzung)

Menüoption	Beschreibung
	• DNS-Einstellungen • IPSec-Einstellungen • VPN-Einstellungen • HP Velocity-Einstellungen **HINWEIS:** Viele Funknetzwerke sind gesichert und erfordern eine eigene Authentifizierung und ein Kennwort bzw. einen Schlüssel.
Sicherheit	Damit können Sie die Systemkennwörter für Administrator und Benutzer des Client einrichten oder ändern.

Tabelle 4-6 Zusätzliche Administrator Bedienfeldoptionen – Verwaltung

Menüoption	Beschreibung
Automatic Update	Damit können Sie den Automatic Update-Server manuell zurücksetzen.
Rücksetzung auf Werkseinstellungen	Damit können Sie den Client auf seine Standard-Werkseinstellungen wiederherstellen.
VNC-Shadow	Damt können Sie das VNC-Shadowing verwenden. Virtual Network Computing (VNC) ist ein Fernsteuerungsprogramm, mit dem Sie den Desktop eines Remotecomputers anzeigen und mit der lokalen Maus und der lokalen Tastatur genauso steuern können, als würden Sie direkt an diesem Computer sitzen. Verwenden Sie VNC-Shadowing für folgende Funktionen: • Einem anderen System von einem Remote-Standort Zugriff auf den Client zu ermöglichen • VNC-Sitzungen mit einem Schreibschutz zu versehen • Ein Kennwort für den Zugriff auf den Client fordern, wenn VNC verwendet wird • Einem Benutzer zu ermöglichen den Zugriff auf den VNC-Client zu verweigern • Den VNC-Server zurücksetzen

Tabelle 4-7 Zusätzliche Administrator Bedienfeldoptionen – Erweitert

Menüoption	Beschreibung
Zertifikate	Damit können Sie den **Zertifikat-Manager** für Folgendes verwenden: • Eine lokale vertrauenswürdigen Zertifizierungsstelle und persönliche Zertifikate anzeigen • Zertifikate mithilfe der folgenden Methoden zum Client importieren:

Tabelle 4-7 Zusätzliche Administrator Bedienfeldoptionen – Erweitert (Fortsetzung)

Menüoption	Beschreibung
	◦ Das Zertifikat von einem USB-Schlüssel importieren ◦ Das Zertifikat von einer URL impoprtieren
Tastenkombinationen	Mithilfe des **Keyboard Shortcuts Manager** (Tastenkombinations-Manager) können Sie vorhandene Verknüpfungen ändern und neue Verknüpfungen erstellen, mit denen benutzerdefinierte Befehle ausgeführt werden.
Task-Manager	Damit können Sie die CPU-Auslastung und den CPU-Nutzungsverlauf für den Client überwachen.
Textbearbeitung	Damit können Sie Konfigurationsdateien oder Skripte direkt im Client bearbeiten.
X-Terminal	Damit können Sie Linux-Befehle außerhalb der Client-Benutzeroberfläche ausführen.

Übersicht über RDP-Verbindungsfunktionen

Der RDP-Client basiert auf FreeRDP 1.0 und erfüllt die folgenden Anforderungen für RDP 7.1:

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

Verwenden des Kioskmodus mit RDP

Standardmäßig ist nur der Host-Name des Servers erforderlich, um eine Verbindung herzustellen. Der Anmeldebildschirm identifiziert und authentifiziert den Benutzer. Zusätzliche Anmeldungsinformationen können im Dialogfeld Verbindungseinstellungen im Administratormodus eingerichtet werden.

Um den Kioskmodus zu aktivieren, in dem der Client beim Booten unter Verwendung vordefinierter Benutzer-Anmeldeinformationen eine automatische Anmeldung zum Remote-Desktop durchführt, gehen Sie wie folgt vor:

1. Klicken Sie im Administratormodus auf der Client-Symbolleiste auf  .
2. Klicken Sie auf **Edit Default Connection** (Standardverbindung bearbeiten).
3. Geben Sie einen Benutzernamen und ein Kennwort für den Kioskbenutzer ein.

TIPP: Der Benutzername ist ein allgemeiner Ausdruck mit eingeschränkten Domänen-Zugriffsrechten.

4. Führen Sie unter **Erweitert** einen der folgenden Schritte aus:

a. Legen Sie die **Autostart Priority** (Autostart-Priorität) auf **1** fest.

b. Wählen Sie **Autoreconnect** (Automatische Neuverbindung).

5. Klicken Sie auf **Speichern**.

6. Klicken Sie auf **Neu verbinden**.

Dies führt dazu, dass die RDP-Sitzung automatisch beim Booten angemeldet wird. Darüber hinaus wird die Verbindung, wenn sie aufgrund einer Abmeldung, einer Trennung oder eines Netzwerkausfalls verloren gegangen ist, automatische neu hergestellt, sobald sie wiederhergestellt ist. Der Remote-Host kann so konfiguriert werden, dass er alle gewünschten Anwendungen bei der Anmeldung automatisch startet.

Um zum Anmeldebildschirm zurückzukehren und die Sitzung zu minimieren, drücken Sie Strg+Alt +Ende. Dies ermöglicht es Ihnen, die Client-Einstellungen zu ändern.

Verwendung von RemoteFX mit RDP

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

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

Um RFX zu deaktivieren, richten Sie den Wert des Registrierungsschlüssels folgendermaßen ein:

- `root/ConnectionType/freerdp/connections/{UUID}/remoteFx to '0'`

TIPP: HP empfiehlt, dass Sie RFX auf dem Remote-Host aktivieren oder deaktivieren.

Verwenden der Multimedia-Umleitung mit RDP

Die Multimedia Umleitung (MMR) ist eine Technologie, die mit Windows Media Player auf dem Remote-Host integriert ist. Sie streamt die codierten Medien zum Client anstatt sie auf dem Remote-Host wiederzugeben und über RDP neu zu codieren. Diese Technologie verringert die Serverlast und den Netzwerkverkehr und verbessert das Multimedia-Erlebnis in höchstem Maße. Unterstützt die 24 FPS-Wiedergabe von 1080p-Videos mit automatischer Audiosynchronisierung. MMR ist standardmäßig aktiviert. Ein Client verhandelt mit jedem RDP-Server, den er kontaktiert, und wenn MMR verfügbar ist, wird es verwendet.

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

Um MMR auf dem Client für alle RDP-Verbindungen zu deaktivieren, richten Sie den Wert des Registrierungsschlüssel folgendermaßen ein:

- `root/ConnectionType/freerdp/general/enableMMR to '0'`

Da RemoteFX bereits akzeptable Multimedia-Leistung bietet, können Sie MMR mit RFX deaktivieren, indem Sie den Registrierungsschlüssel folgendermaßen einrichten:

- `root/ConnectionType/freerdp/connections/{UUID}/disableMMRwithRFX to '1`

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

Verwenden von Multi-Monitor-Sitzungen mit RDP

Echter Multi-Monitor-Support benötigt keine spezielle Konfiguration durch den Administrator oder Benutzer. Der RDP-Client identifiziert automatisch, welcher Monitor in den lokalen Einstellungen als Hauptmonitor angegeben ist und platziert die Taskleiste und die Desktop-Symbole auf diesem Monitor. Wenn ein anderer Hauptmonitor gewünscht wird, kann er über die lokalen Einstellungen für die **Anzeige** eingerichtet werden, die im Menü **Konfiguration** verfügbar sind. Wenn ein Fenster innerhalb der Remotesitzung maximiert wird, wird das Fenster nur den Monitor abdecken, auf dem es maximiert wurde.

Die Bildschirmeinstellungen und Monitorauflösungen können innerhalb der Remotesitzung angezeigt, aber nicht geändert werden. Zum Ändern der Sitzungsauflösung melden Sie sich von der Sitzung ab und änderndie die Auflösung auf dem lokalen Client. Die empfohlene Einstellung **Autom.** verwendet DDC für die Kommunikation mit dem Monitor und richtet automatisch die Auflösung auf die bevorzugte native Auflösung des Monitors ein.

Standardmäßig sind alle RDP-Sitzungen Vollbildsitzungen und umfassen alle Monitore,um die Virtualisierungserfahrung zu verbessern. Zusätzliche Fensteroptionen stehen über die Option **Edit Default Connection** (Standardverbindung bearbeiten) im Menü **Konfiguration** zur Verfügung. Normalerweise werden diese Optionen nur auf Systemen verwendet, die mehrere gleichzeitige Verbindungen unterstützen, wie z. B. HP ThinPro.

HINWEIS: Der HP t410 All-in-One Smart Zero Client unterstützt nur eine Bildschirmauflösung von 1366x768.

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

Verwenden der Geräteumleitung mit RDP

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

Verwenden einer USB-Umleitung mit RDP

Bei Systemen, die an einen Windows 7 SP1-Host angeschlossen sind, unterstützt RDP die Umleitung für eine Vielzahl von USB-Geräten, die in einer Hyper-V Virtual Machine ausgeführt werden.

Bei Systemen, die an einen Windows 8- oder Windows Server 2012-Host angeschlossen sind, ermöglicht HP Smart Zero Core eine USB-Umleitung auf sämtlichen Installationen.

Die USB-Umleitung erfolgt durch Übermittlung von Low-Level-USB-Protokoll-Anrufen über das Netzwerk an den Remote-Host. Alle am lokalen Host angeschlossenen USB-Geräte werden innerhalb des Remote-Hosts als native USB-Geräte angezeigt, als wären sie lokal angeschlossen. Standard-Windows-Treiber unterstützen das Gerät in der Remotesitzung, und alle Gerätetypen werden unterstützt, ohne dass zusätzliche Treiber auf dem Client erforderlich sind.

Nicht alle Geräte können standardmäßig mit der USB-Umleitung verwendet werden. Zum Beispiel können USB-Tastaturen, Mäuse und anderen Eingabegeräte in der Regel nicht umgeleitet werden,

da die Remotesitzung eine Eingabe com Client erwartet. Einige Geräte wie z. B. Massenspeicher, Drucker und Audiogeräte verwenden zusätzliche Optionen für die Umleitung.

Verwenden der Massenspeicherumleitung mit RDP

Standardmäßig leitet die RDP-Sitzung alle Massenspeichergeräte an den Remote-Host weiter und verwendet dabei eine Laufwerksumleitung höchster Ebene. Wenn ein Gerät wie ein USB-Flash-Laufwerk, ein USB-DVD-ROM-Laufwerk oder eine externe USB-Festplatte am System angeschlossen wird, erkennt der Client diese Geräte und stellt diese im lokalen Dateisystem bereit. RDP erkennt dann ein bereitgestelltes Laufwerk und leitet es zum Remote-Host um. Innerhalb des Remote-Host erscheint es als neue Festplatte im Windows-Explorer und erhält den Namen `<device label> auf <client hostname>`; beispielsweise `Bill_USB auf 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 ist weniger als eine Sekunde nachdem der Dialog Datei kopieren beendet ist, aber es können bis zu 10 Sekunden erforderlich sein, je nach der Schreibgeschwindigkeit des Geräts und der Netzwerklatenz.
- Nur vom Client unterstützte Dateisysteme werden bereitgestellt. Die unterstützten Dateisysteme sind FAT32, NTFS, ISO9660 (CD-ROMs), UDF (DVD-ROMs) und ext3.
- Das Gerät wird als Verzeichnis behandelt. Häufige Laufwerksaufgaben wie die Formatierung und die Änderung der Festplattenbezeichnung stehen nicht zur Verfügung.

  Bei Bedarf können Sie die Umleitung von Massenspeichern deaktivieren. Schalten Sie die USB-Umleitung aus. Ändern Sie danach die Einträge für den Registrierungsschlüssel wie in der folgenden Tabelle beschrieben.

Tabelle 4-8 USB-Umleitung deaktivieren

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

Um die lokale Bereitstellung von USB-Massenspeichergeräten vollständig zu deaktivieren oder die Umleitung von USB-Massenspeichergeärten zu deaktivieren, jedoch andere Geräte zur Umleitung zuzulassen, löschen Sie im Client-Dateisystem die udev-Regel `/etc/udev/rules.d/010_USBDRIVE.Regeln`.

Verwenden der Druckerumleitung mit RDP

Standardmäßig hat RDP zwei Methoden der Druckerumleitung aktiviert:

- **USB-Umleitung** – Alle am Gerät angeschlossenen USB-Drucker werden in der Remote-Sitzung als lokale Drucker angezeigt. Der Standardvorgang für die Druckerinstallation muss in der

Remote-Sitzung durchgeführt werden, falls der Drucker noch nicht am Remote-Host installiert ist. Es müssen lokal keine Einstellungen vorgenommen werden.

- **High-level redirection** (High-Level-Umleitung) – Wenn entweder keine USB-Umleitung verfügbar auf dem Remote-Host ist oder der Drucker ein paralleler oder serieller Drucker ist, verwenden Sie die High-Level-Umleitung. Konfigurieren Sie den Drucker für die Verwendung eines lokalen Druckerspoolers und der RDP-Client wird automatisch einen Remote-Drucker einrichten, der Druckspoolingbefehle über einen virtuellen Kanal vom Remote-Host an den Client sendet.

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

HINWEIS: Weitere Informationen finden Sie unter Konfigurieren eines seriellen oder parallelen Druckers auf Seite 44.

Audioumleitung mit RDP verwenden

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

- 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.
- Wenn USBR aktiviert ist, empfiehlt HP, dass alle USB-Audiogeräte über USBR umgeleitet werden. Dies stellt sicher, dass Audio lokal gemischt wird, um die Qualität zu verbessern. Wenn die USB-Umleitung eines Audiogeräts erforderlich ist, stellen Sie sicher, dass die RDP-Einstellung für **Sound** auf **Leave at remote computer** (Auf Remote-Computer lassen) eingerichtet ist, anstelle von **Bring to this computer** (Zu diesem Computer bringen). Konfigurieren Sie diese Einstellung mithilfe der Seite **Local Resources** (Lokale Ressourcen) in den **Verbindungseinstellungen** im Administratormodus.

Deaktivieren Sie MMR, falls alle Audiogeräte auf Lokal eingerichtet sind, da sonst Multimedia nur über die Standard-Audiogeräte wiedergegeben wird.

- Die Mikrofon-Umleitung ist standardmäßig aktiviert. Die Standard-Mikrofonlautstärke muss möglicherweise auf dem Client angepasst werden. Dies kann über das Menü **Konfiguration** ausgeführt werden.
- Sowohl die lokalen wie die Remote-Lautstärkeeinstellungen haben Auswirkungen auf die endgültige Lautstärke. HP empfiehlt, die lokale Lautstärke auf das Maximum einzustellen und die Lautstärke innerhalb des Remote-Host anzupassen.

Smart Card-Umleitung mit RDP verwenden

Standardmäßig werden Smart Cards mithilfe der High-Level-Umleitung umgeleitet. Damit können sie zum Anmelden bei der Sitzung und anderen Remote-Anwendungen verwendet werden. Um die Smart Card-Anmeldung zu aktivieren, markieren Sie das Feld **Allow Smarcard login** (Smart Card-Anmeldung zulassen) im Anmeldebildschirm oder innerhalb der **Connection settings** (Verbindungseinstellungen). Damit kann der Benutzer eine Verbindung herstellen, ohne zuerst die

Anmeldedaten angeben zu müssen. Anschließend startet der RDP-Client die RDP-Sitzung und der Benutzer wird aufgefordert, sich per Smart Card zu authentifizieren.

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

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

Festlegen von RDP-Optionen

Für eine optimale Benutzererfahrung verwenden Sie die Registerkarte **Erfahrung** in den **Verbindungseinstellungen** und legen Sie die **Verbindungsgeschwindigkeit** zum **LAN** fest. Ist eine Bandbreitenreduzierung erforderlich ist, kann die Verbindungsgeschwindigkeit auf **Modem** eingestellt werden, wodurch alle Erfahrungsoptionen deaktiviert werden.

Die zusätzlichen Optionen, die in der folgenden Tabelle beschrieben werden, können über die Kontrollkästchen auf der Registerkarte **Options** (Optionen) konfiguriert werden.

Tabelle 4-9 Allgemeine Verbindungsoptionen

Verbindungsoptionen	Beschreibung
Enable motion events (Senden von Bewegungen aktivieren)	Die Funktion ist standardmäßig aktiviert. Sendet jedes Mal eine Meldung an den RDP-Server, wenn das Zeigegerät verschoben wird. Ist diese Option deaktiviert, werden Hover-Optionen wie Quickinfos häufigt nicht angezeigt.
Enable data compression (Datenkomprimierung aktivieren)	Die Funktion ist standardmäßig aktiviert. Die Datenkomprimierung kann deaktiviert werden, um die Server- und Client-CPU-Nutzung zu reduzieren, aber dies resultiert in einer drastischen Anstieg der Bandbreite im Netzwerk.
Enable encryption (Verschlüsselung aktivieren)	Die Funktion ist standardmäßig aktiviert. Verursacht eine Codierung des gesamten Datenverkehrs mit TLS- oder RC4-Verschlüsselung. Kann deaktiviert werden, um die Client- und Host-CPU-Nutzung zu reduzieren.
Force bitmap updates (Bitmap-Aktualisierungen erzwingen)	Die Funktion ist standardmäßig aktiviert. Führt dazu, dass Bitmaps gespeichert werden, auch wenn sie nicht angezeigt werden. Dadurch wird die Nutzung des Client-Speichers erhöht, jedoch die Aktualisierung der Hintergrundbilder verbessert.
Attach to console (Zu Konsole hinzufügen)	Standardmäßig deaktiviert. Wenn diese Option aktiviert ist, kann RDP dazu verwendet werden, eine Verbindung zu den Servern herzustellen, bei denen RDP deaktiviert ist und bei denen nur die Administrator-Konsole aktiv ist. Wird primär für das Debuggen verwendet.
Send hostname (Host-Namen senden)	Sendet die angegebene Textzeichenfolge als Client-Host-Name statt System-Host-Name.

Übersicht über Citrix-Verbindungsfunktionen

Eine Citrix Verbindung greift auf die Citrix SBC (Server-Based Computing)- und VDI (Virtual Desktop Infrastructure)-Dienste zu.

Konfigurieren einer Citrix Remote-Verbindung mit dem Verbindungsassistenten. Wenn die Standardwerte nicht Ihren Anforderungen entsprechen, verwenden Sie die erweiterten Optionen, um den Einrichtungsvorgang für die Verbindung abzuschließen.

Funktionen der Citrix-Verbindungsverwaltung

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

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

Citrix-Receiver-Funktionen

Citrix-Receiver-Funktionen:

- Neueste Version zum Zeitpunkt des Release:
  - 12.1.5 für x86
  - 12.5 für ARM/SoC
- Einstellungen für die Fenstergröße und -tiefe
- Nahtloser Fenstersupport
- Einstellungen für die Soundqualität
  - Niedrig
  - Mittel
  - Hoch
  - Deaktiviert
- Zuordnung von statischen Laufwerken
- Zuordnung von dynamischen Laufwerken
- USB-Umleitung für XenDesktop und VDI-in-a-Box
- Smart Card Virtual Channel-Aktivierung

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

- Druckerzuordnung

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

HINWEIS: Weitere Informationen finden Sie unter HDX MediaStream-Supportmatrix auf Seite 23.

- HDX Flash-Umleitung (nur x86)
- HDX Webcam-Komprimierung
- HDX RealTime (MS Lync-Optimierung) (nur x86)

HDX MediaStream-Supportmatrix

Tabelle 4-10 HDX MediaStream-Supportmatrix

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

Citrix-Verbindung-Supportmatrix

Die folgende Tabelle beschreibt die unterstützten Citrix-Backends.

Tabelle 4-11 Citrix-Verbindung-Supportmatrix

		Backend		
		XenApp	XenDesktop	VDI-in-a-Box
Zugriffstyp	Direkt (Betriebssystemunabhängig)	4,5/5/6/6.4		
	Nativ (PNAgent)	4.5/5/6/6.5	4.5/5.5/5.6.5	5.x
	Internetbrowser	4.5/5/6/6.5	4.5/5.5/5.6.5	5.x

Übersicht über die VMware Horizon View-Verbindungsfunktionen

Verwenden des Kiokskmodus mit VMware Horizon View

Im Kioskmodus führt der Client beim Start mithilfe vordefinierter Benutzer-Anmeldeinformationen eine automatische Anmeldung zu einem Remote-Desktop durch. Wenn Sie wegen einer Abmeldung, einer Verbindungstrennung oder eines Netzwerkausfalls eine Verbindung verlieren, wird die Verbindung bei Rückkehr der Konnektivität automatisch wiederhergestellt.

Um die Sitzung zu minimieren und zum Anmeldebildschirm zurückzukehren, verwenden Sie die Tastenkombination Strg+Alt+Ende.

So richten Sie ein Kioskmodus-Anmeldung ein:

1. Klicken Sie als Administrator auf , und wählen Sie **Edit Connection Settings** (Verbindungseinstellungen bearbeiten) aus.
2. Geben Sie unter **Netzwerk** die folgenden Einstellungen ein:
   - Benutzername
   - Kennwort
   - Domäne
   - Desktop (falls zutreffend)
3. Klicken Sie auf **OK**.
4. Klicken Sie auf , und wählen Sie **Advanced Configuration > Advanced > Xterminal** (Zusätzliche Konfiguration > Erweitert > X-Terminal) aus.
   a. Geben Sie in der Eingabeaufforderung `regeditor` und drücken Sie die **Eingabetaste**.
   b. In den Client-Registrierung legen Sie den Wert wie folgt fest:

Wert	Eintrag
Connection Type/view/connections/UUID/autostart	1
Connection Type/view/connections/UUID/autoreconnect registry	1

WICHTIG: Klicken Sie **Speichern** nach jedem Eintrag.

5. Klicken Sie nach Abschluss auf **Beenden**.
6. Starten Sie das System neu.

Verwenden der Multimedia-Umleitung mit VMware Horizon View

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

Weitere Informationen hierzu finden Sie unter Verwenden der Multimedia-Umleitung mit RDP auf Seite 17.

Verwenden von Multi-Monitor Sitzungen mit VMware Horizon View

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

Verwenden von Tastaturkürzeln mit VMware Horizon View

Windows-Tastenkombinationen

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

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

Die Windows-Tastaturkürzel werden an die Remote-Desktop-Sitzung weitergeleitet. Daraus resultiert, dass lokale Tastaturkürzel wie z. B. Strg+Alt+Tab und Strg+Alt+F4 innerhalb der Remote-Sitzung nicht funktionieren. Zum Umschalten von Sitzungen kann die obere Leiste aktiviert werden, indem die Markierung **Hide top menu bar** (Obere Menüleiste ausblenden) auf der Registerkarte **Allgemein** in den **Verbindungseinstellungen** aufgehoben wird, oder über den Registrierungsschlüssel `root/ConnectionType/view/connections/{UUID}/hideMenuBar`.

Medientasten

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

Geräte-Umleitung mit VMware Horizon View verwenden

USB-Umleitung mit VMware Horizon View verwenden

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

Weitere Informationen zu USBR, einschließlich Geräte- und klassenspezifische Umleitung finden Sie unter Verwenden einer USB-Umleitung mit RDP auf Seite 18

HINWEIS: Informationen zum Konfigurieren einer USB-Umleitung für Versionen von HP Smart Zero Core, die den USB-Manager nicht verwenden, finden Sie unter USB-Optionen in vorhergehenden-Releases auf Seite 102.

Massenspeicher-Umleitung mit VMware Horizon View verwenden

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

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

▲ Deaktivieren Sie USBR mithilfe des USB-Managers, um das **Remote-Protokoll** auf **Lokal** festzulegen.

Dies erstellt ein einem Netzwerk zugeordnetes Laufwerk in der virtuellen Desktop-Sitzung für jedes interne und externe Massenspeichergerät, das mit dem Client verbunden ist. Das Dateisystemformat der Remote-Speicher spielt keine Rolle. Beispielsweise kann ein mit ext3 formatierter USB-Schlüssel mit einer Windows-Verbindung verwendet werden.

Weitere Einzelheiten finden Sie unter Verwenden der Massenspeicherumleitung mit RDP auf Seite 19.

Drucker-Umleitung mit VMware Horizon View verwenden

Für Verbindungen mit dem PCoIP-Protokoll unterstützt USBR Drucker. Für Verbindungen mit dem RDP-Protokoll siehe Verwenden der Druckerumleitung mit RDP auf Seite 19 für weitere Informationen.

Audioumleitung mit VMware Horizon View verwenden

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

Der VMware Horizon View-Client unterstützt keine High-Level-Aufzeichnungsumleitung über den Verbindungstyp PCoIP. Wenn Sie Unterstützung bei der Audio-Aufzeichnung benötigen, verwenden Sie eine der folgenden Methoden:

- Wenn Sie den Teradici-PCoIP-Client auf dem t410 System verwenden, installieren Sie den Teradici-Audiotreiber von http://techsupport.teradici.com auf dem virtuellen Desktop. Dies ermöglicht High-Level-Audioumleitung über entweder eine 3,5-mm-Buchse oder ein USB-Headset.

HINWEIS: Nur Systeme mit Teradici-PCoIP-Client 1.2 oder höher unterstützen High-Level-Audioumleitung über ein USB-Headset. Systeme mit älteren Client-Versionen leiten das Headset durch das USBR ujder Client wird durch das Headset USBR umleiten.

- 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 Client muss Windows 7 oder höher ausführen. Sie müssen außerdem sicherstellen, dass der Registrierungsschlüssel `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\fDisableAudioCapture` auf `0` eingestellt ist.

- Wenn Sie ein USB-Headset mit einem Mikrofon haben, verwenden Sie USBR. Stellen Sie das USB-Headset so ein, dass es in die Sitzung umgeleitet wird. Das Headset wird als ein Audiogerät angezeigt. Standardmäßig verwendet USB-Audiogeräte nicht weitergeleitet werden und der Blick auf Client hoher Ebene Audio Umleitung verwendet wird. Zur Umleitung des USB-Headsets verwenden Sie den USB-Manager des Client und wählen das USB-Headset aus, das umgeleitet werden soll. Vergewissern Sie sich, dass **VMware Horizon View** als das USBR-Protokoll ausgewählt ist und stellen Sie sicher, dass das Headset unter **Geräte** als umzuleitend markiert ist.

HINWEIS: VMware empfiehlt nicht, USBR für Headsets zu verwenden. Zum Streamen von Audiodaten über das USBR-Protokoll ist eine große Menge Netzwerkbandbreite erforderlich. Sie könnten mit dieser Methode auch schlechte Audioqualität erhalten.

Smart Card-Umleitung mit VMware Horizon View verwenden

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

1. Im Dialogfeld **Verbindungseinstellungen** unter **Allgemein** wählen Sie **Allow Smartcard login**. (Smart Card-Anmeldung zulassen)

   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 erneuter Eingabe einer PIN.

HINWEIS: Zur Anmeldung am VMware Horizon View Manager-Administratorserver mit einer Smartcard müssen der lokale Smart Card-Treiber auf dem Client installiert sein. Weitere Informationen über die Smart Card Treiberinstallation finden Sie unter: Smart Card-Umleitung mit RDP verwenden auf Seite 20. Nachdem Sie sich am Remote-Host angemeldet haben, wird die Smart Card über einen virtuellen Kanal an den Remote-Host weitergeleitet, nicht über USBR: Diese Weiterleitung über einen virtuellen Kanal stellt sicher, dass die Smart Card für Aufgaben wie E-Mail-Unterschriften, Bildschimsperren usw. verwendet werden kann. Es könnte aber passieren, dass die Smart Card im Geräte-Manager von Windows nicht als Smart Card-Gerät erkannt wird.

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

Webcam-Umleitung mit VMware Horizon View verwenden

Die VMware mit mehr Komfort Anzeigen Client unterstützt keine hoher Ebene Webcam Umleitung verwendet wird. Webcams können nur verwendet werden, wenn sie mithilfe von USBR weitergeleitet werden. Die Webcam könnte schlecht oder gar nicht funktionieren. Weitere Informationen finden Sie unter Verwenden einer USB-Umleitung mit RDP auf Seite 18.

Erweiterte Verbindungsoptionen für VMware Horizon View

Für den Zugriff auf zusätzliche VMware Horizon View-Verbindungsoptionen im Client wählen Sie **Verbindungseinstellungen bearbeiten > Allgemeine** im VMware Horizon View-Verbindungsmanager.

Die folgende Tabelle beschreibt die allgemeinen Anmeldeoptionen im VMware Horizon View-Verbindungsmanager.

Tabelle 4-12 Login options (Anmeldeoptionen)

Option	Beschreibung
Automatic login (Automatische Anmeldung)	Wählen Sie **Automatic login** (Automatische Anmeldung), um sicherzustellen, dass der Client bei der Anmeldung beim Broker die folgenden Anmeldeinformationen verwendet: • Host-Name • Benutzername • Passwort Wenn das Feld Automatische Anmeldung aktiviert ist, werden diese Informationen in die richtigen Felder eingegeben, wenn der VMware Horizon View-Client startet. Zum Starten der Verbindung müssen Sie jedoch auf **Verbinden** klicken. **HINWEIS:** HP empfiehlt, das Fls die die automatische Login Box klicken.
Allow Smartcard login (Smart Card-Anmeldung zulassen)	Wählen Sie **Allow Smartcard login** (Smart Card-Anmeldung zulassen), um die Smart Card-Anmeldung zu aktivieren. **HINWEIS:** Weitere Informationen zu HP SAM finden Sie unter .
Nach Verbindungsunterbrechung schließen	Zum beenden des VMware mit mehr Komfort Anzeigen Client nach Benutzer anmelden ihre Desktops oder die Sitzung beendet mit einem Fehler, wählen Sie **Schließen , Nachdem Trennen**. Diese Option ist eine Sicherheitsfunktion so konzipiert, dass ein Benutzer nicht vollständig melden Sie sich ein weiterer Schritt zu treffen müssen, nachdem sie mit ihrem Desktop Sitzung abgeschlossen sind. **Schließen Sie nach dem Trennen Sie** die Option ist standardmäßig aus Sicherheitsgründen, sind jedoch geändert werden, wenn sie werden häufig Benutzer Wechsel zu einem neuen Desktop Pool nach Abmelden von einer Sitzung und nicht vollständig wieder einloggen.
Hide Top Menu Bar (Obere Menüleiste ausblenden)	, Damit der oberen Menüleiste unsichtbar für Benutzer, wählen Sie **Ausblenden oberen Menüleiste**. Diese Option ist standardmäßig aktiviert. Können Sie dieses deaktivieren, wenn Benutzer Optionen für den Zugriff auf

Tabelle 4-12 Login options (Anmeldeoptionen) (Fortsetzung)

Option	Beschreibung
	lieber für das Fenster- oder Desktop Pool Auswahl in einem VMware mit mehr Komfort Session anzeigen.
Connection Security Levels (Verbindungs-Sicherheitsstufen)	Verwenden Sie die **Sicherheitsstufe Verbindung** zum Einstellen der Sicherheitsstufe anzeigen, dass die VMware mit mehr Komfort beim Herstellen einer Verbindung zum Client benutzt den Server. **HINWEIS:** Weitere Informationen finden Sie unter Anforderungen für die VMware Horizon View HTTPS- und Zertifizierungsverwaltung auf Seite 31 weitere Informationen Verbindung Sicherheitsstufen verhalten.

Mithilfe erweiterter Befehlszeilenargumente mit VMware mit mehr Komfort anzeigen

Erweiterte Befehlszeilenargumente zu verwenden:

1. Navigieren Sie in the VMware Horizon View zu **Edit Connection Settings > General** (Verbindungseinstellungen bearbeiten > Allgemein).
2. Unter **Befehlszeilenargumente**, geben Sie Argumente ein, die an den VMware Horizon View-Client weitergeleitet werden, wenn er gestartet wird

Wenn Sie weitere Hilfe zur Verwendung der erweiterten Befehlszeilenoptionen benötigen, führen Sie einen der folgenden Schritte aus:

- Geben Sie in der Befehlszeile `vmware-view--help` ein und drücken Sie dann Eingabe.
- Siehe die Linux Horizon View-Client-Dokumentation von VMware unter http://www.vmware.com.

HINWEIS: Die Informationen in diesem Abschnitt gelten nicht für den Teradici-beschleunigten PCoIP Client.

Ein Teradici-beschleunigtes t410-System mit VMware Horizon View verwenden.

Ein Teradici-beschleunigtes t410-System verwendet einen Teradici PCoIP-Client zur Verbindung mit dem VMware Horizon View-Desktop. Um zu überprüfen, ob Ihr System Teradici-beschleunigt ist, suchen Sie nach der Bezeichnung **teradici-pcoip-Client**, die im Bereich **Systeminformationen** aufgelistet ist.

HINWEIS: Teradici-beschleunigte Einheiten können das RDP-Protokoll nicht dazu verwenden, eine Verbindung mit einer Remote-Desktop-Sitzung herzustellen.

HINWEIS: Der Teradici PCoIP-Client unterstützt keine Weiterleitung des Datenverkehrs über einen HTTP-Proxy. Um eine Verbindung über einen Proxy herzustellen, müssen Sie zum standardmäßigen VMware Horizon View-Client wechseln. Weitere Informationen finden Sie unter Umschalten zum standardmäßigen VMware Horizon View-Client auf Seite 29.

Umschalten zum standardmäßigen VMware Horizon View-Client

So wechseln Sie zum standardmäßigen VMware Horizon View-Client:

1. Öffnen Sie ein Xterminal, und führen Sie den folgenden Befehl aus:

```
mv /usr/bin/teradici_signature_check /usr/bin/
teradici_signature_check.bak
```

WICHTIG: Der Befehl sollte in einer einzigen Zeile mit jeweils einem Leerzeichen vor jedem Dateipfad eingegeben werden.

2. Starten Sie den Client neu.

So wechseln Sie wieder zum Teradici PCoIP-optimierten Client:

1. Öffnen Sie ein Xterminal, und führen Sie den folgenden Befehl aus:

```
mv /usr/bin/teradici_signature_check.bak /usr/bin/
teradici_signature_check
```

WICHTIG: Der Befehl sollte in einer einzigen Zeile mit jeweils einem Leerzeichen vor jedem Dateipfad eingegeben werden.

2. Starten Sie den Client neu.

Ändern des VMware Horizon View Protokolltyps

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

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

So ändern Sie den Verbindungstyp:

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

HINWEIS: Verwenden Sie den VMware Horizon View-Manager, um zu konfigurieren, welches Verbindungsprotokoll für jeden Desktop-Pool verwendet werden soll.

TIPP: HP empfiehlt, das PCoIP-Protokoll zu verwenden, umd die Desktop-Erfahrung zu verbessern. Das RDP-Protokoll bietet jedoch mehr Optionen für die Anpassung und funktioniert bei langsamen Verbindungen möglicherweise besser. Für den Zugriff auf die Optionen **Experience** (Erfahrung) verwenden Sie das Dialogfeld **Connection Settings** (Verbindungseinstellungen).

Weitere Informationen über bestimmte Optionen für RDP-Verbindungen finden Sie unter Festlegen von RDP-Optionen auf Seite 21.

Zertifikate auf Clients installieren

Verwenden Sie den Zertifikat-Manager, wenn Sie eine Zertifikat der Zertifizierungsbehörde (Certificate Authority, CA) installieren. Diese Aktion kopiert das Zertifikat in den lokalen Zertifikatsspeicher des Benutzers (/usr/local/share/ca-certificates) und konfiguriert OpenSSL, das Zertifikat zur Verbindungsverifizierung zu verwenden.

Bei Bedarf können Sie die HP Smart Zero Client Services dazu verwenden, das Zertifikat an ein Profil anzuhängen, wie unter Zertifikate zu einem Client-Profil hinzufügen auf Seite 43 beschrieben.

HINWEIS: Weitere Informationen hierzu finden Sie unter http://linux.die.net/man/1/x509.

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

Anforderungen für die VMware Horizon View HTTPS- und Zertifizierungsverwaltung

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 Zertifizierungsbehörde (CA, Certificate Authority) signiert wird und die CA nicht vertrauenswürdig ist, gibt die Verbindung einen Fehler zurück und dem Benutzer wird es nicht gestattet. eine Verbindung herzustellen.

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

- Im Administratormodus greifen Sie auf das Client-Bedienfeld zu und wählen **Zusätzliche Konfiguration > Erweitert > Zertifikate**, um den Zertifikatsmanager zu öffnen. Importieren Sie dann das Zertifikat von einer Datei oder URL.
- Verwenden Sie eine Remote-Profilaktualisierung zum Importieren eines Zertifikats.
- Im VMware Horizon View Manager wählen Sie **Edit Connection Settings > General** (Verbindungseinstellungen bearbeiten > Allgemein). Legen Sie die **Connection Security Level** (Verbindungssicherheitsstufe) auf **Allow all Connections** (Alle Verbindungen zulassen) fest und klicken Sie anschließend auf **Übernehmen**.

Tabelle 4-13 VMware Horizon View Sicherheitsstufen für Zertifikate

		Sicherheitsstufen		
		Unsichere Verbindungen verweigern	**Warnen**	**Alle Verbindungen erlauben**
Zertifikatsvertrauen	**Vertrauenswürdig**	Vertrauenswürdig	Vertrauenswürdig	Vertrauenswürdig
	Selbst signierte	Fehler	Warnung	Nicht vertrauenswürdig
	Abgelaufen	Fehler	Warnung	Nicht vertrauenswürdig
	Nicht vertrauenswürdig	Fehler	Fehler	Nicht vertrauenswürdig

Tabelle 4-14 Definitionen für Sicherheitsstufe der Zertifikate

Stufe	Beschreibung
Vertrauenswürdig	Stellt ohne den Dialog für eine Zertifikatswarnung eine Verbindung her und zeigt ein grünes Schloßsymbol an.
Nicht vertrauenswürdig	Stellt ohne den Dialog für eine Zertifikatswarnung eine Verbindung her und zeigt ein rotes entsperrtes Schloßsymbol an.

Tabelle 4-14 Definitionen für Sicherheitsstufe der Zertifikate (Fortsetzung)

Stufe	Beschreibung
Warnung	Stellt mit dem Dialog für eine Zertifikatswarnung eine Verbindung her und zeigt ein rotes entsperrtes Schloßsymbol an.
Fehler	Erlaubt die Verbindung nicht

USB-Geräte umleiten

1. Melden Sie sich im Client als Administrator an.
2. Klicken Sie auf , und wählen Sie **Additional Configuration > Peripherals > USB Manager** (Zusätzliche Konfiguration > Peripheriegeräte > USB-Manager) aus.
3. Wählen Sie eines der folgenden Remoteprotokolle aus:
   - Citrix
   - RDP7
   - Lokal
   - VMware Horizon View
4. Wenn die Einstellung **Lokal** lautet, können Sie außerdem die folgenden Optionen angeben: **allow devices to be mounted** (Gerätebereitstellung zulassen) und **mount devices read-only** (Geräte schreibgeschützt bereitstellen).
5. Im Bildschirm **USB-Manager** unter **Geräte** zeigen Sie die an das System angeschlossenen Geräte an.
6. Um diese Standard-Umleitungseinstellungen zu überschreiben, wählen Sie die Geräte aus, die Änderungen erfordern.
7. Für die ausgewählten Geräte wählen Sie eine der folgenden Umleitungsoptionen:
   - Standard
   - Umleiten
   - Nicht umleiten
8. Nach Abschluss wählen Sie **Übernehmen**, und klicken Sie dann **auf OK**.

Zuordnen eines seriellen oder parallelen Druckers

1. Klicken Sie auf der Client-Symbolleiste auf .
2. Wählen Sie **Zusätzliche Konfigurationen** > Druckerzuordnung.
3. Im Bildschirm **Druckerzuordnung** klicken Sie auf **Hinzufügen**, um einen Drucker hinzuzufügen.
4. Im Dialogfeld **HP-Druckererstellung** unter **Anschluss** wählen Sie eine der folgenden Optionen:
   - Parallel
   - Seriennummer 1
   - Seriennummer 2

HINWEIS: Wählen Sie **Seriennummer 1** wenn Sie nur einen seriellen Drucker haben.

5. Unter **Modell**, geben Sie den Namen und die Modellnummer Ihres Druckers an.

HINWEIS: Dies ist ein optionaler Schritt. HP empfiehlt jedoch, dass Sie dies tun, damit der Druckername im Bildschirm **Zuordnung** angezeigt wird.

6. Unter **Windows-Treiber** geben Sie den Namen des Windows-Druckertreibers für den Drucker ein.

HINWEIS: Dies ist ein optionaler Schritt. HP empfiehlt, dass Sie jedoch mindestens den Windows-Treiber Allgemein/Nur Text installieren, um den Drucker auf dem Server zu verwenden. Ohne Treiber kann Windows den Drucker unter Umständen nicht korrekt verwenden.

7. Wählen Sie **Aktiv**, um den neuen Drucker zu aktivieren.

8. Zum Erstellen des neuen Druckers wählen Sie **Erstellen**.

Nach Abschluss wird der neue Drucker im Dialogfeld **HP-Druckererstellung** angezeigt.

5 Fehlerbeseitigung von Clients

In diesem Kapitel werden folgende Themen behandelt:

- Fehlerbeseitung der Netzwerkverbindung
- Fehlerbeseitigung bei Firmware-Beschädigung
- Fehlerbeseitigung bei der Konfiguration eines seriellen oder parallelen Druckers
- Fehlerbehebung bei abgelaufenen Citrix-Kennwörtern
- Verwenden Systemdiagnose für die Fehlerbeseitigung

Fehlerbeseitung der Netzwerkverbindung

1. "Ping" zusammen mit der IP-Adresse des Client Server indem Sie Folgendes durchführen:

   a. Klicken Sie auf der Client-Symbolleiste auf  , um auf den Bildschirm **About this Client** (Über diesen Client) zuzugreifen, und klicken Sie dann auf die Registerkarte **NetTools** (Netzwerktools).

   b. Unter **Select Tool** (Tool auswählen) wählen Sie **Ping**.

   c. Im Feld **Target Host** (Zielhost) geben Sie die Server-Adresse ein und klicken Sie dann **Start Process** (Prozess starten).

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

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

   64 bytes from 10.30.8.52: icmp_seq-1 ttl=64 time=0.81 5 ms 64 bytes
   from 10.30.8.52: icmp_seq=2 ttl=64 time=0.735 ms
   ```

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

2. Falls der Client nicht auf den Ping reagiert, gehen Sie wie folgt vor:

   a. Prüfen Sie das Netzwerkkabel und überprüfen Sie die Netzwerkeinstellungen der Client Bedienfeld.

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

   c. Wenn Sie andere Netzwerk-Clients erreichen, überprüfen Sie, ob Sie die richtige Server-Adresse eingegeben haben.

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

3. Überprüfen Sie die Systemprotokolle indem Sie Folgendes durchführen:

a. Klicken Sie auf der Client-Symbolleiste auf  , um auf den Bildschirm **About this Client** (Über diesen Client) zuzugreifen, und klicken Sie dann auf die Registerkarte **System Logs** (Systemprotokolle).

b. Überprüfen Sie die Protokolle auf Fehler.

c. Wenn ein Fehler aufgetreten ist, dann wird die Benachrichtigung **Server is not set up** (Server ist nicht eingerichtet) angezeigt. Überprüfen Sie, dass der Server richtig eingerichtet ist und dass die HP Smart Zero Client Services ausgeführt werden..

Fehlerbeseitigung bei Firmware-Beschädigung

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

Re-Imaging der Client-Firmware des Geräts

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

Fehlerbeseitigung bei der Konfiguration eines seriellen oder parallelen Druckers

Vor der Konfiguration des Druckers benötigen Sie die Information über die Baudrate des Druckers von der Dokumentation des Druckers. Wenn Sie die erforderliche Dokumentation nicht besitzen, suchen Sie die Baudrate durch Ausführen der folgenden Schritte:

1. Schalten Sie den Drucker ein, während Sie die Taste **Feed** gedrückt halten.
2. Lassen Sie die **Feed**-Taste los und warten Sie 30 Sekunden. Der Drucker geht in einen Selbsttestmodus und druckt die erforderlichen Informationen aus.

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

HINWEIS: Die meisten seriellen Drucker drucken eine Diagnoseseite, wenn Sie diesen Vorgang durchführen. Wenn Ihr Drucker nicht in die Diagnoseseite zu drucken, finden Sie in der Dokumentation des Druckers.

Zur Eingabe des Druckers Baudrate:

1. Mit dem **Profile Editor** unter **Registrierung**, wählen Sie **root/printer-mapping-mgr/{UUID}/BaudRate**.
2. Geben Sie die Baudrate Ihres Druckers ein.

HINWEIS: Die UUID stimmt mit der UUID des Druckers im Verzeichnis **root/printer** überein. Schauen Sie dort nach und gleichen Sie den Drucker mit der UUID unter **root/printer-mapping-mgr** ab.

3. Klicken Sie auf **Speichern**.
4. Klicken Sie mit der rechten Maustaste auf UUID und danach auf **Änderungen übernehmen**.

Fehlerbehebung bei abgelaufenen Citrix-Kennwörtern

Wenn Benutzer nicht dazu aufgefordert werden, abgelaufene Citrix-Kennwörter zu ändern, sollten Sie sicherstellen, dass die XenApp Services-Site (Pnagent-Site) für die Authentifizierungsmethode **Prompt** konfiguriert ist, um es Benutzern zu ermöglichen, abgelaufene Kennwörter zu ändern. Wenn Sie Benutzern erlauben, ihre Passwörter über eine direkte Verbindung zum Domänencontroller zu ändern, sollten Sie außerdem die Synchronizität der Systemzeit von Client und Domänencontroller sicherstellen und darauf achten, dass bei der Eingabe von Citrix-Anmeldeinformationen der vollständige Domänenname (z. B. `domain_name.com`) verwendet wird. Weitere Informationen finden Sie in der Citrix-Dokumentation.

Verwenden Systemdiagnose für die Fehlerbeseitigung

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

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

Speichern von Systemdiagnosedaten

1. Stecken Sie ein USB-Flash-Laufwerk am Thin Client ein.
2. Klicken Sie auf der Client-Symbolleiste auf , um auf den Bildschirm **About this Client** (Über diesen Client) zuzugreifen, und klicken Sie dann auf die Registerkarte **System Logs** (Systemprotokolle).
3. Klicken Sie auf **Diagnose**, und speichern Sie dann die komprimierte Diagnosedatei **Diagnose.tgz** auf demm USB-Flash-Laufwerk.

Dekomprimieren der Systemdiagnosedateien

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

Dekomprimieren der Systemdiagnosedateien auf Windows-basierten Systemen

1. Laden Sie eine Kopie der Windows-Version von **7-Zip** herunter und installieren Sie sie.

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

2. Stecken Sie das USB-Flash-Laufwerk, das die gespeicherte Systemdiagnosedatei enthält, ein, und kopieren Sie anschließend **Diagnose.tgz** zum Desktop.
3. Klicken Sie mit der rechten Maustaste auf **Diagnostic.tgz** und wählen Sie **7-Zip** > **Dateien entzippen ...**.
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 **Diagnose.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 Befehle

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

Tabelle 5-1 Dateien im Ordner Befehle

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

Anzeigen von Dateien im Ordner /var/log

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

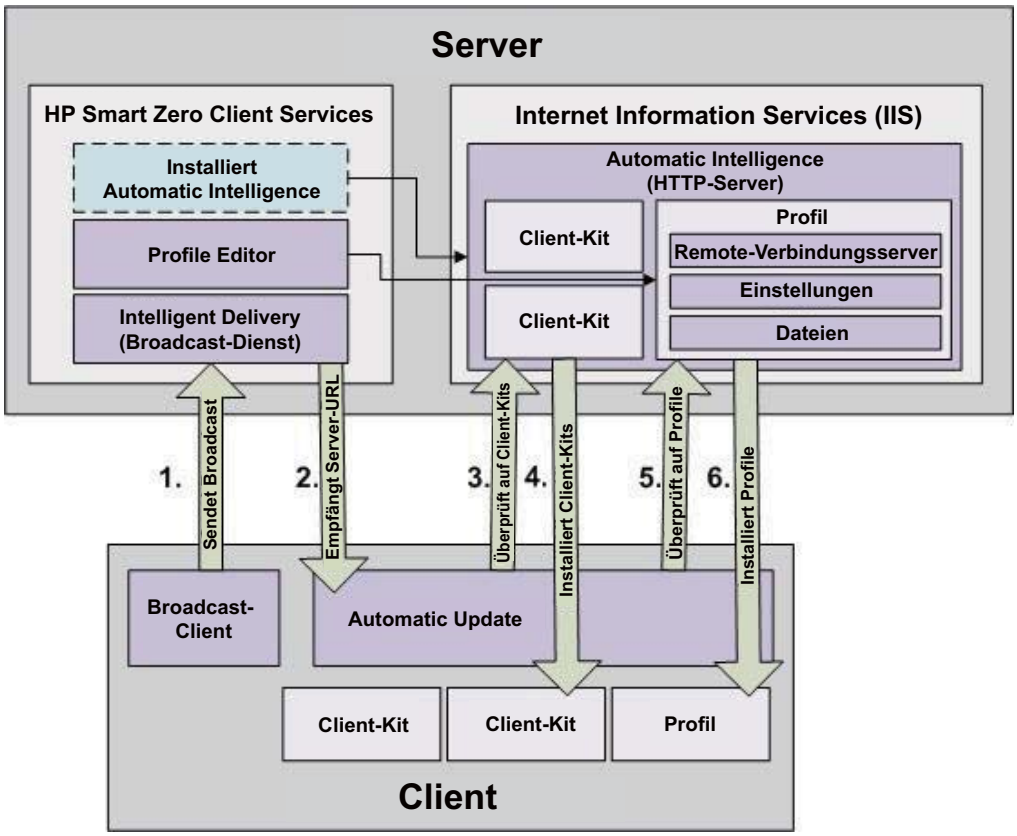
Anzeigen von Dateien im Ordner /etc

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

6 HP Smart Zero Client Services

Clients erkennen einen Update Server automatisch und konfigurieren sich selbst beim ersten Booten. Dadurch werden die Installation und die Wartung von Geräten vereinfacht.

Im Diagramm unten wird beschrieben, wie die Clients mit dem Server kommunizieren, wenn sie Profile und Client-Aktualisierungskits empfangen.



Unterstützte Betriebssysteme

HP Smart Zero 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.

Vorbereitung zum Installieren von HP Smart Zero Client Services

Vor der Installation der HP Smart Zero Client Services überprüfen Sie 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.

Herunterladen und Installieren von HP Smart Zero Client Services

So laden Sie die HP Smart Zero Client Services herunter und installieren sie:

1. Navigieren Sie zur Webseite http://www.hp.com/support.
2. Klicken Sie auf **Drivers & Software** (Treiber und Software), geben Sie den Namen Ihres Client-Modells in das Feld ein und klicken Sie dann **SUCHEN**.
3. Klicken Sie in der Liste der Suchergebnisse auf Ihr Client-Modell.
4. Unter **Select operating system** (Betriebssystem auswählen) klicken Sie auf **HP Smart Zero Client**.
5. Unter **Software-Systemmanagement** suchen Sie **Smart Zero Client Services** und klicken Sie dann auf die Schaltfläche **Herunterladen**.
6. Starten Sie den Installationsassistenten und befolgen Sie die Anleitungen auf dem Bildschirm, um die Installation abzuschließen.

HINWEIS: Der Installationsassistent kann auch dazu verwendet werden, Komponenten der HP Smart Zero Client Services hinzuzufügen, zu ändern, zu reparieren und zu entfernen.

7 Verwenden des Profile Editors

HP Smart Zero Client Services enthält den Profile Editor, mit dem Administratoren Client-Profile erstellen und diese zum Automatic Update-Server hochladen können. Das Client-Profil enthält Verbindungsinformationen sowie Einstellungen und Dateien, die Smart Clients herunterladen und zur Selbstkonfiguration verwenden.

Dieser Abschnitt enthält die folgenden Themen:

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

HINWEIS: Im Anhang C finden Sie „HP Smart Zero Core-Registrierungseinstellungen“ auf Seite 64 eine umfassende Liste und Beschreibung der Registrierungsschlüssel.

Zugriff auf den Profile Editor

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

Laden eines Client-Profils

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

So laden Sie ein Profil:

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

Ändern eines Client-Profils

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

- Auswahl der Plattform eines Client-Profils
- Auswahl des Verbindungstyps eines Client-Profils
- Ändern der Einstellungen der Registrierung eines Client-Profil
- Hinzufügen von Dateien zu einem Client-Profil
- Speichern des Client-Profils

Auswahl der Plattform eines Client-Profils

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

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

So richten Sie die Client-Profilplattform ein:

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

TIPP: Erstellen Sie für jeden Hardwaretyp ein eigenes Profil.

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

2. Klicken Sie nach Abschluss auf **Weiter**.

Auswahl des Verbindungstyps eines Client-Profils

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

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

Ändern der Einstellungen der Registrierung eines Client-Profil

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

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

Aktivieren oder deaktivieren der Menüoptionen auf Clients

1. In der Struktur **Registrierungseinstellungen** navigieren Sie zu **root > zero-login > controls**.
2. Erweitern Sie den Ordner für das Menüelement, das aktiviert oder deaktiviert werden soll und klicken Sie auf die Einstellung **autorisiert**.
3. Geben Sie die entsprechende Zahl im Feld **Wert** ein:
   - 0 (deaktivieren)
   - 1 (aktivieren)

Aktivieren oder deaktivieren der Benutzerkonfigurationen auf Clients

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

Hinzufügen von Dateien zu einem Client-Profil

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

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

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

Hinzufügen einer Konfigurationsdatei zu einem Client-Profil

1. Klicken Sie im Bereich **Zusätzliche Konfigurationsdateien** auf **Eine Datei hinzufügen**.
2. Klicken Sie auf **Datei importieren**, suchen Sie die Datei an, die importiert werden soll, und klicken Sie dann **Öffnen**.

   HINWEIS: Dateien können auch über die **Exportdatei** exportiert werden , wenn weitere Einzelheiten über die Datei erforderlich sind.
3. Im Feld **Pfad** legen Sie den Pfad fest, wo die Datei auf dem Client installiert wird.
4. Im Bereich **Dateidetails** geben Sie in den Feldern **Eigentümer**, die Gruppe **Gruppe**, und die **Berechtigungen** die entsprechenden Werte ein.

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

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

Zertifikate zu einem Client-Profil hinzufügen

Client-Profile für HP Smart Zero Core 4.1.1 und neuere Versionen enthalten automatisch Zertifikate, die für die folgenden Anwendungen in einen Standard-Client-Zertifikatsspeicher importiert werden:

- VMware Horizon View, Citrix, RDP
- Automatic Update
- HP Smart Zero Client Services
- Internetbrowser-Speicher (falls installiert)

So importieren Sie andere Zertifikate zu einem Client-Profile für HP Smart Zero Core 4.1.1 oder höhere Versionen:

1. Klicken Sie im Bereich **Zusätzliche Konfigurationsdateien** auf **Eine Datei hinzufügen**.
2. Klicken Sie auf **Datei importieren**, ermitteln Sie das Zertifikat, und klicken Sie dann auf **Öffnen**.

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

3. Im Feld **Pfad** legen Sie den Pfad auf Folgendes fest:

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

4. Klicken Sie auf **Speichern**, um das Hinzufügen des Zertifikats zum Client-Profil abzuschließen.
5. Nach der Installation des Client-Profile verwenden Sie den **Zertifikat-Manager** um zu bestätigen, dass das Zertifikat ordnungsgemäß importiert wurde.

Installieren von Citrix-Zertifikaten auf HP Smart Zero Core 4.1.0 und früheren Versionen

HP Smart Zero Core 4.1.0 und frühere Versionen haben das Zertifikat-Manger-Add-on nicht, und der einzige im Profile Editor unterstützte Zertifikatsspeicher ist der Citrix-Zertifikatsspeicher. Bei anderen Speichern müssen Sie nach dem Importieren von Zertifikaten Client-Skripts ausführen. Außerdem ist für sie eine benutzerdefinierte Aktualisierung erforderlich.

Führen Sie diese Schritte aus, um ein Zertifikat zu installieren, das in einer Citrix-Browsersitzung zu installieren:

1. Klicken Sie im Bereich **Zusätzliche Konfigurationsdateien** auf **Eine Datei hinzufügen**.
2. Klicken Sie auf **Datei importieren**, ermitteln Sie das Zertifika, das Sie importieren möchten, und klicken Sie dann **Öffnen**.

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

3. Im Feld **Pfad** legen Sie den Pfad auf Folgendes fest:

   `/usr/lib/ICAClient/keystore/cacerts/<cert>`

4. Klicken Sie auf **Speichern**, um das Hinzufügen des Zertifikats zum Client-Profil abzuschließen.

Hinzufügen eines symbolischen Links zu einem Client-Profil

1. Klicken Sie im Bereich **Zusätzliche Konfigurationsdateien** auf **Eine Datei hinzufügen**.
2. Wählen Sie in der Dropdown-Liste **Typ** die Option **Link**.
3. Im Bereich **Symbolische Link-Details** legen Sie den **Link** auf den Pfad der gewünschten Datei, die bereits auf dem Client installiert ist, fest.
4. Klicken Sie auf **Speichern** zum Hinzufügen des symbolischen Links.

Speichern des Client-Profils

1. Klicken Sie im **Profile Editor** auf den Link **Beenden** im linken Bereich, um auf den Bereich **Aktuelles Profil** zuzugreifen.
2. Klicken Sie auf **Profil speichern** zum Speichern des aktuellen Client-Profils oder klicken Sie auf **Profil speichern unter**, um es neues Client-Profil zu speichern.

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

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

Konfigurieren eines seriellen oder parallelen Druckers

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

Dieser Abschnitt enthält die folgenden Themen:

- Abrufen der Drucker-Baudrate
- Einrichten von Druckeranschlüssen
- Drucker auf dem Server installieren

Abrufen der Drucker-Baudrate

Vor der Konfiguration des Druckeranschlusses rufen Sie die Baudrate des Druckers ab. Falls verfügbar, überprüfen Sie die Druckerdokumentation bevor Sie fortfahren. Falls diese nicht verfügbar ist, gehen Sie wie folgt vor:

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

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

Einrichten von Druckeranschlüssen

1. Wählen Sie im **Profile Editor** (Profil-Editor) **Registry** (Rgeistrierung) aus, und klicken Sie dann auf **Show all settings** (Alle Einstellungen anzeigen).
2. Aktivieren Sie die Druckerportzuordnung für Ihren Verbindungstyp:
   - Citrix – Navigieren Sie zu **root > Connectiontype > xen > general**, und legen Sie den Registrierungsschlüssel **lastcomportnum** auf einen der Werte `1 bis 4` fest, je nachdem, wie viele zugeordnete Druckerports erforderlich. sind
   - RDP – Navigieren Sie zu **root > ConnectionType > freerdp**. Klicken Sie mit der rechten Maustaste auf den Ordner **connections**, wählen Sie **New connection** (Neue Verbindung) aus und klicken Sie auf **OK**. Legen Sie den Registrierungsschlüssel **portMapping** auf den Wert `1` fest, um die Druckerportzuordnung zu aktivieren.
   - VMware Horizon View – Navigieren Sie zu **root > ConnectionType > view**. Klicken Sie mit der rechten Maustaste auf den Ordner **connections**, wählen Sie **New connection** (Neue

Verbindung) aus und klicken Sie auf **OK**. Legen Sie unter dem Ordner **xfreerdpOptions** den Registrierungsschlüssel **portMapping** auf den Wert `1` fest, um die Druckerportzuordnung zu aktivieren.

3. Navigieren Sie zu **root > Serial**.
4. Legen Sie den Registrierungsschlüssel **Baud** auf die Baudrate Ihres seriellen oder parallelen Druckers fest.

Drucker auf dem Server installieren

1. Auf dem Windows-Desktop wählen Sie **Start > Drucker und Faxgeräte**.
2. Wählen Sie **Drucker hinzufügen** und klicken Sie anschließend auf **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 nach Abschluss 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 aufgefordert werden, den vorhandenen Treiber beizubehalten und dieser funktioniert, dann behalten Sie diesen Treiber bei und klicken Sie auf **Weiter**.
8. Weisen Sie dem Drucker einen Namen zu. Um ihn als Standarddrucker zu verwenden, wählen Sie **Ja**, und klicken Sie dann **Weiter**.
9. Wenn Sie den Drucker freigeben möchten, wählen Sie **Freigabename** und weisen Sie dem Drucker einen Freigabenamen zu. Klicken Sie anderenfalls auf **Weiter**.
10. Auf der nächsten Seite können Sie einen Testdruck anfordern. HP empfiehlt dies, weil Sie dadurch überprüfen können, ob der Drucker korrekt eingerichtet ist. Falls der Drucker nicht korrekt eingerichtet ist, überprüfen Sie die Einstellungen und versuchen Sie es erneut.

HINWEIS: Wenn der Client die Verbindung zum Server trennt, muss der Drucker beim nächsten Verbindungsaufbau des Clients erneut eingerichtet werden.

8 Automatic Intelligence verwenden

Dieser Abschnitt enthält die folgenden Themen:

- Anzeigen der Automatic Update-Website
- Ein Automatic Update-Profil erstellen
- Clients aktualisieren
- Verwenden des HP Intelligent Delivery-Dienstes
- Verwenden des HP Device Manager

Anzeigen der Automatic Update-Website

1. Auf dem Server Desktop, wählen Sie **Start > Systemsteuerung**, und klicken Sie dann **Verwaltungstools**.
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)\Hewlett-Packard\HP Smart Client Service\auto-update
```

Ein Automatic Update-Profil erstellen

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

1. Rufen Sie die MAC-Adresse des Clients über die Systeminfo ab. Zum Beispiel verwenden die folgenden Schritte die MAC-Adresse `00fcab8522ac`.
2. Verwenden Sie den Profile Editor zum Erstellen oder Ändern eines Client-Profil (siehe „Verwenden des Profile Editors“ auf Seite 40), bis Sie bereit sind, das Client-Profil zu speichern.
3. Klicken Sie im **Profile Editor** auf den Link **Beenden** im linken Bereich, um auf den Bereich **Aktuelles Profil** zuzugreifen.
4. Klicken Sie auf **Profil speichern unter**, um das Client-Profil folgendermaßen zu speichern:

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

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

Clients aktualisieren

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

Verwenden der Methode Aktualisierung per Übertragung

Um eine Aktualisierung per Übertragung durchzuführen, verbinden Sie den Client mit dem gleichen Netzwerk, in dem sich der Update Server befindet. Eine Aktualisierung per Übertragung stützt sich auf die HP Smart Zero Client Services, die in Zusammenarbeit mit IIS automatisch Aktualisierungen zum Client pushen.

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

TIPP: Damit die Aktualisierung per Übertragung sicher funktioniert, führen Sie den Profile Editor aus und nehmen Sie einige Änderungen vor. Verbinden Sie den Thin Client und überprüfen Sie, ob dieser das neue Profil heruntergeladen hat. Falls nicht, siehe „Fehlerbeseitigung von Clients“ auf Seite 34.

Verwenden der Aktualisierungsmethode mit der DHCP-Kennung

Auf Windows Server 2003- und Windows Server 2008-Systemen, ermöglicht die DHCP-Tagging einem Client die Aktualisierung. Verwenden Sie diese Methode zum aktualisieren bestimmter Clients; wenn Sie allerdings nur einen oder zwei Clients aktualisieren möchten, sollten Sie stattdessen die manuelle Aktualisierung in Betracht ziehen. Generell empfiehlt HP die Methode Aktualisierung per Übertragung.

Beispiel für die Durchführung DHCP-Kennung

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

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

1. Auf dem Server-Desktop wählen Sie **Start > Verwaltungstools > DHCP**.
2. Klicken Sie im linken Fensterbereich des **DHCP**-Bildschirms auf die Domäne, mit der die Clients verbunden sind.
3. Erweitern Sie im rechten Fensterbereich des Bildschirms **DHCP** die Anzeige von **IPv4**, klicken Sie mit der rechten Maustaste darauf, und klicken Sie dann auf **Set Predefined Options** (Vordefinierte Optionen einstellen).
4. Klicken Sie im Dialogfeld **Vordefinierte Optionen und Werte** auf **Hinzufügen**.
5. Im Feld **Optionstyp** konfigurieren Sie die Optionen wie in der folgenden Tabelle beschrieben.

Tabelle 8-1 Beispieloptionen für DHCP-Kennung

Feld	Eintrag
Name	Geben Sie `auto-update` ein.
Datentyp	Wählen Sie **Einstellungen** aus.

Tabelle 8-1 **Beispieloptionen für DHCP-Kennung (Fortsetzung)**

Feld	Eintrag
Code	Typ `137`.
Beschreibung	Typ `HP Automatic Update`.

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

   `http://auto-update.dominio.com:18287/auto-update`
8. Um das Einrichten abzuschließen, klicken Sie auf **OK**. Die DHCP-Kennung ist jetzt bereit für die Aktualisierung bestimmter Clients.

Verwenden der Aktualisierungsmethode mit DNS Alias

Während des Systemstarts versucht Automatic Update den DNS-Alias **auto-update** aufzulösen. Wenn dieser Host-Name aufgelöst werden kann, versucht es, die Updates unter **http://auto-update:18287** zu überprüfen. Diese Updatemethode ermöglicht es Clients, auf einen einzelnen Updateserver in der gesamten Domäne zuzugreifen, was die Verwaltung von Bereitstellungen mit vielen Subnetzen und DHCP-Servern vereinfacht.

So konfigurieren Sie die Aktualisierungsmethode mit DNS Alias:

- Ändern Sie den Host-Namen des Servers, der die HP Smart Zero Client Services hostet, für ein **auto-update** oder erstellen Sie einen DNS-Alias von **auto-update** für diesen Server.

Verwenden der manuellen Aktualisierungsmethode

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

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

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

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

Eine manuelle Aktualisierung durchführen

1. Klicken Sie auf der Client-Symbolleiste auf .
2. Klicken Sie auf **Wechsel zwischen Administrator-/Benutzermodus**.
3. Im Feld **Administratorkennwort** geben Sie Ihr Kennwort ein und klicken Sie dann auf **OK**.
4. Schließen Sie den Anmeldevorgang ab, indem Sie auf klicken.
5. Wählen Sie **Zusätzliche Konfiguration > Management > Automatic Update**.

6. Im Dialogfeld **Automatic Update** konfigurieren Sie die Optionen wie in der folgenden Tabelle beschrieben.

Tabelle 8-2 Automatic Update-Optionen

Feld	Eintrag
Manuelle Konfiguration aktivieren	Wählen Sie **Manuelle Konfiguration aktivieren**.
Manuelle Konfiguration > Protokoll	Wählen Sie **http**.
Manuelle Konfiguration > Server	Geben Sie den folgenden Update Server-Host-Namen und die Portnummer ein: `<Hostname>:18287`
Pfad	Typ `auto update`.

7. Klicken Sie nach Abschluss auf **OK**. Der Client führt jezt ein Pull für die automatischen Updates durch.

Verwenden des HP Intelligent Delivery-Dienstes

Wie der HP Intelligent Delivery-Dienst funktioniert

Dieser Windows-Dienst wartet an einem High-Level-Ausgang auf Broadcasts von Clients. Wenn ein Broadcast empfangen wird, antwort der HP Intelligent Delivery-Dienst mit der URL des Automatic Intelligence-Servers, den der Client zum Prüfen auf Aktualisierungen verwendet.

Starten, anhalten und beenden des HP Intelligent Delivery-Dienstes

1. Auf dem Server-Desktop wählen Sie **Start > Verwaltung > Server-Manager**.
2. Erweitern Sie im linken Fensterbereich des **Server-Manager** die Option **Konfiguration** und wählen Sie **Dienste**.
3. In mittleren Bereich unter **Dienste** doppelklicken Sie auf **HP Broadcast Server-Dienst**, und wählen Sie anschließend **Eigenschaften**.
4. Im Dialogfeld **HP Broadcast Server Properties** (HP Broadcast Server-Eigenschaften) klicken Sie unter **Dienststatus** auf eine der folgenden Optionen:
   - **Dienst starten**
   - **Dienst beenden**
   - **Dienst anhalten**

Anzeigen des Anwendungsprotokolls des HP Intelligent Delivery-Dienstes

1. Auf dem Server-Desktop wählen Sie **Start > Verwaltung > Server-Manager**.
2. Erweitern Sie im linken Bereich von **Server Manager** (Server-Manager) **Diagnostics > Event Viewer > Windows Logs > Application** (Diagnose > Ereignisanzeige > Windows Protokolle > Anwendung).
3. Das Anwendungsprotokoll wird im mittleren Bereich unter **HPSmartClientService** angezeigt.

HP Intelligent Delivery Service-Registrierungsschlüssel

Die von HP Intelligent Delivery Service verwendeten Registrierungsschlüssel, finden Sie in der folgenden Tabelle.

Tabelle 8-3 HP Intelligent Delivery Service-Registrierungsschlüssel

Registrierungsschlüssel	Pfad
Port	HKLM\SYSTEM\CurrentControlSet\Services\HP Broadcast Server
ServerURL	HKLM\SYSTEM\CurrentControlSet\Services\HP Broadcast Server

Verwenden des HP Device Manager

Der HP Device Manager Agent ist eine Software, die im Hintergrund des Client ausgeführt wird. Verwenden Sie den HP Device Manager für die Remote-Auswahl und -Bearbeitung der erforderlichen geschäftlichen Anforderungen des Client.

Weitere Informationen zum HP Device Manager finden Sie im *HP Device Manager Benutzerhandbuch*.

A Client-Tastatursprache

Verwenden Sie den **Profile Editor** zum Ändern oder Einrichten der Tastatursprachen. Ändern Sie die Registrierungseinträge wie folgt:

- /Stamm/Tastatur/Modell
- /Stamm/Tastatur/Layout
- /Stamm/Tastatur/Variante

Tabelle A-1 Tastatursprachen

Tastatur	Modell	Layout	Variante
Belgien [Belgisches Französisch]	pc105	be	wincompat
Brasilien [Brasilianisches Portugiesisch]	abnt2	br	wincompat
Bulgarien [Bulgarisch]	pc105	bg	wincompat
Kanada [Kanadisches Französisch]	pc105	ca	wincompat
Kroatien [Kroatisch]	pc105	hr	wincompat
Tschechische Republik [Tschechisch]	pc105	cz	wincompat
Dänemark [Dänisch]	pc105	dk	wincompat
Finnland [Finnisch]	pc105	fi	wincompat
Frankreich [Französisch]	pc105	fr	wincompat
Deutschland [Deutsch]	pc105	de	wincompat
Ungarn [Ungarisch]	pc105	hu	wincompat
Italien [Italiensich]	pc105	it	wincompat
Japan [Japanisch], mit " ¥" (RDP)	jp106	jp	jp106-hp-yen
Japan [Japanisch], mit " \" (RGS)	jp106	jp	jp106-hp
Korea [Koreanisch]	kr106	kr	wincompat
Lateinamerika [Lateinamerikanisch]	pc105	latam	wincompat
Niederlande [Niederländisch]	pc105	nl	wincompat
Norwegen [Norwegisch]	pc105	no	wincompat
Polen [Polnisch]	pc104	pl	wincompat
Portugal [Portugiesisch]	pc105	pt	wincompat
Rumänien [Rumänisch]	pc105	ro	wincompat
Russland [Russisch]	pc104	ru	wincompat
Slowakei [Slowakisch]	pc105	sk	wincompat
Slowenien [Slowenisch]	pc105	si	wincompat
Spanien [Spanisch]	pc105	sp	wincompat

Tabelle A-1 Tastatursprachen (Fortsetzung)

Tastatur	Modell	Layout	Variante
Schweden [Schwedisch]	pc105	se	wincompat
Schweiz [Schweizerisches Französisch]	pc105	ch	wincompat-fr_ch
Schweiz [Schweizerisches Deutsch]	pc105	ch	wincompat-de_ch
Türkei [Türkisch]	pc105	tr	wincompat
Ukraine (Ukrainisch]	pc105	ua	wincompat
Vereinigtes Königreich [English]	pc104	gb	wincompat
Vereinigte Staaten [English]	pc105	us	wincompat
Vereinigte Staaten [English], Dvorak	pc105	us	wincompat-dvorak
Vereinigte Staaten [English], International	pc105	us	wincompat-intl

B Anpassen des Client-Anmeldebildschirms

Anpassen des Bildschirmhintergrunds

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

Es gibt ein Verzeichnis für jeden Verbindungstyp – sowie einen Standardstil – zum Festlegen der Stilelemente des Hintergrundbildes der Verbindung und des Stils des Anmeldefensters. Registrierungseinträge legen die Verzeichnisse fest, in welchen diese Dateien gespeichert werden. Sie können geändert werden, um auf benutzerdefinierte Verzeichnisse zu verweisen. Zum Beispiel verweist der Registrierungsschlüssel **root/zero-login/styledir/view** auf das Verzeichnis, das Stilelemente für den Anmeldedesktop für VMware Horizon View-Verbindungen enthält. Standardmäßig wird **/etc/hptc-zero-login/styles/view** verwendet.

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

```
global {

color: 666666; # Dark gray

padding: 20; # 20 pixels }
```

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

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

Hierzu gehören:

- Gemeinsame Attribute
- Elemente
- Image
- Text

Gemeinsame Attribute

Tabelle B-1 Anmeldebildschirm > Gemeinsame Attribute > Name

Typ	Beschreibung
Parameter	Eine Zeichenfolge

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

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

Tabelle B-2 Anmeldebildschirm > Gemeinsame Attribute > padding

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

Tabelle B-3 Anmeldebildschirm > Gemeinsame Attribute > color

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

Tabelle B-4 Anmeldebildschirm > Gemeinsame Attribute > alpha

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

Tabelle B-5 Anmeldebildschirm > Gemeinsame Attribute > size

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

Tabelle B-6 Anmeldebildschirm > Gemeinsame Attribute > position

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

Tabelle B-7 Anmeldebildschirm > Gemeinsame Attribute > alignment

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

Tabelle B-8 Anmeldebildschirm > Gemeinsame Attribute > context

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

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

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

Elemente

Tabelle B-9 Anmeldebildschirm > Elemente > Benutzerdefiniert > Global

Typ	Beschreibung
Verwendung	Legt globale Hintergrund- oder Abstandswerte fest.
Erkannte gemeinsame Attribute:	**name, color, padding** • **color** – legt die Volltonfarbe für den Hintergrund des Bildschirms fest, wenn keine Farbverläufe spezifiziert sind • **padding** – legt den Standardabstand für alle nachfolgenden Elemente fest

Tabelle B-10 Anmeldebildschirm > Elemente > Benutzerdefiniert > Gradient

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

Tabelle B-11 Anmeldebildschirm > Elemente > Benutzerdefiniert > Type

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

Tabelle B-12 Anmeldebildschirm > Elemente > Benutzerdefiniert > Axis

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

Tabelle B-13 Anmeldebildschirm > Elemente > Benutzerdefiniert > Metric

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

Tabelle B-14 Anmeldebildschirm > Elemente > Benutzerdefiniert > colors

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

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

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

Tabelle B-15 Anmeldebildschirm > Elemente > Benutzerdefiniert > dithered

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

Image

Tabelle B-16 Anmeldebildschirm > Image

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

Tabelle B-17 Anmeldebildschirm > Benutzerdefinierte Attribute > Source

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

Tabelle B-18 Anmeldebildschirm > Benutzerdefinierte Attribute > Proportional

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

Text

Tabelle B-19 Anmeldebildschirm > Text

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

Tabelle B-20 Anmeldebildschirm > Text > text-locale

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

Tabelle B-21 Anmeldebildschirm > Text > text

Typ	Beschreibung
Parameter	Standard text text:
Beispiel	This will be shown on the screen.;
Standard	Nicht zutreffend
Verwendung	Wenn kein übereinstimmender lokalisierter Text festgelegt wird, wird stattdessen diese Textzeichenfolge verwendet. **HINWEIS:** Die Textdarstellungsmaschine unterstützt kein Markup im HTML-Stil.

Tabelle B-22 Anmeldebildschirm > Text > font-locale

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

Tabelle B-23 Anmeldebildschirm > Text > font

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

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

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

Tabelle B-24 Anmeldebildschirm wird > Text > font-size (Fortsetzung)

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

Tabelle B-25 Anmeldebildschirm > Text > max-width

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

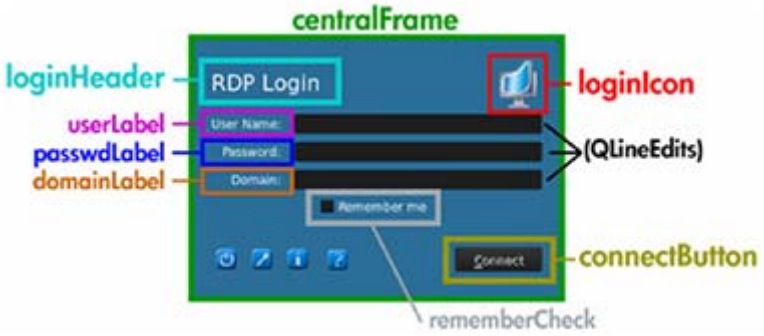
Tabelle B-26 Anmeldebildschirm > Text > max-height

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

Anpassen des Dialogfeld für die Client-Anmeldung

In diesem Abschnitt finden Sie Beispiele zur Beschreibung, wie das Dialogfeld für die Client-Anmeldung angepasst wird.

Abbildung B-1 Komponenten im Dialogfeld für die Client-Anmeldung



Das Dialogfeld Client-Anmeldung verwendet ein Verzeichnis für jeden Verbindungstyp – sowie einen Standardstil – zum Festlegen der Stilelemente des Hintergrundbildes der Verbindung und des Stils des Anmeldefensters.

Die Registrierungseinträge legen die Verzeichnisse fest, in welchen diese Dateien gespeichert werden. Sie können geändert werden, um auf benutzerdefinierte Verzeichnisse zu verweisen. Innerhalb eines Stilverzeichnisses passen Dateien mit dem Suffix `.qss` die Stilelemente des Anmeldebereichs an.

Die `*.qss` Dateien sind **QT-Stylesheets**. Weitere Informationen über Qt-Stylesheets finden Sie unter http://qt-project.org/.

Die meisten Elemente im Anmeldebereich können mit den qss-Stilelementen angepasst werden. Da jedem eine ID zugeordnet wurde, können sie mit dem **#elementID**-Selektor leicht addressiert werden.

Anpassen des zentralen Rahmen

Dieser Abschnitt enthält ein Beispiel für verschiedene Arten, den zentralen Bereich des Anmeldedialogfeldes anzupassen.

```
QFrame#centralFrame {

/* Sea green dialog

background color */ background-color: rgb(46,139,87);

/* Rounded, thicker borders */

border-width: 6px;

border-radius:

16px;

/* Make sure it is at least 400 pixels wide */

min-width:

400px; }
```

Anpassen des Text für die Kopfzeile

Dieser Abschnitt enthält ein Beispiel für verschiedene Arten, den Text im Anmeldeheader anzupassen.

```
LoginArea QLabel#loginHeader {

/* Change the login text at the top */

qproperty-text: "Login Here";

color: white;

font-size: 16pt;

font-weight: bold;

}
```

HINWEIS: In der .qss-Datei überschriebener Text wird nicht lokalisiert, wenn sich das Gebietsschema ändert.

Anpassen des Symbold für den Header

Dieser Abschnitt enthält ein Beispiel für verschiedene Möglichkeiten, das Symbol in der oberen rechten Ecke des Anmeldungsheaders anzupassen.

```
LoginArea QLabel#loginIcon {

/* Substitute my company logo for the normal

one. */ image: url

(/writable/misc/MyCompanyLogo .png); min

width: 48px;

min-height: 48px;

}
```

Es kann einen anderen Stil aufweisen, wenn es nicht aktiviert ist:

```
QPushButton#connectButton:dis

abled { /* Flat gray */

background: rgb(204,204,204);

border-radius: 3;

color: rgb(102,102,102);

font-size: 12pt;

}
```

C HP Smart Zero Core-Registrierungseinstellungen

In diesem Abschnitt werden die HP Smart Zero Core-Registrierungseinstellungen für HP Smart Zero Core 4.3 aufgelistet. Die Tabellen in diesem Abschnitt beschreiben die Registrierungsschlüsselpfade, die Anwendungsfunktionen und Optionen, wie in der Komponente Registrierungs-des Profile Editor vorgestellt.

WICHTIG: Die in diesem Anhang aufgelisteten Registrierungseinstellungen werden mit dem HP ThinPro-Betriebssystem geteilt. Einige der aufgeführte Einstellungen gelten möglicherweise nicht für HP Smart Zero Core.

Die Registrierungseinstellungen sind in die folgenden Überordner gegliedert:

- root > Audio
- root > ConnectionManager
- root > ConnectionType
- root > Display
- root > Network
- root > USB
- root > keyboard
- root > logging
- root > mouse
- root > printer-mapping-mgr
- root > printers
- root > screensaver
- root > time
- root > translation
- root > users
- root > zero-login

root > Audio

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

Tabelle C-1 root > Audio

Registrierungsschlüssel	Gültige Werte	Beschreibung
root/Audio/AdjustSoundPath	Nicht verfügbar	Gibt den vollständigen Pfad zum Standard-Sound an, der ausgegeben

Tabelle C-1 root > Audio (Fortsetzung)

Registrierungsschlüssel	Gültige Werte	Beschreibung
		wird, wenn die Wiedergabelautstärke über das Audiomixer-Bedienfeld oder die Taskleiste geändert wird. Standardmäßig ist dies ein Dreifach-Ping.
root/Audio/Device		
root/Audio/OutputMute	**1** – Stummschalten der internen Lautsprecher und Kopfhörerbuchse. **0** – Nicht Stummschalten der internen Lautsprecher und Kopfhörerbuchse.	Nicht verfügbar
root/Audio/OutputVolume	1-100	Zeigt die Lautstärkeeinstellung für den internen Lautsprecher und die Kopfhörerbuchse an, Skalierung von 1 bis 100.
root/Audio/PlaybackDevice	**1** ist der interne Audio-Controller. **2** und **3** sind für zusätzliche Geräte gedacht, z. B. ein USB-Headset.	Das für die Wiedergabe zu verwendende Gerät.
root/Audio/RecordMute	**1** – Stummschalten der Mikrofonbuchse. **0** – Nicht Stummschalten der Mikrofonbuchse.	Nicht verfügbar
root/Audio/RecordVolume	1-100	Zeigt die Lautstärkeeinstellung für die Mikrofonbuchse an, Skalierung von 1 bis 100.
root/Audio/VisibleInSystray	**0** – Symbol ist nicht sichtbar **1** – Symbol ist sichtbar	Gibt an, ob ein Lautsprechersymbol in der Taskleiste sichtbar ist.

root > ConnectionManager

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

Tabelle C-2 root > ConnectionManager

Registrierungsschlüssel	Gültige Werte	Beschreibung
root/ConnectionManager/customLogoPath		
root/ConnectionManager/defaultConnection	[type]:[label]	Dies muss auf eine gültige Verbindung mit dem Format "[type]:[label]" eingestellt sein, um beim Start eine Verbindung ordnungsgemäß starten zu können. Zum Beispiel: "xen:Default Connection"
root/ConnectionManager/splashLogoPath	Gibt den vollständigen Pfad zu dem Standardbild an, der während des Ladens der Verbinding angezeigt wird.	Dies ist der Begrüßungsbildschirm, der angezeigt wird, nachdem auf dem HP

Tabelle C-2 root > ConnectionManager (Fortsetzung)

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

root > ConnectionType

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

root > ConnectionType > freerdp

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

Tabelle C-3 root > ConnectionType > freerdp

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/authorizations/user/add	Zeigt an, ob der Benutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs durch das HP ThinPro Control Center besitzt. Nicht zutreffend für HP Smart Zero Core. Einrichten auf **1** für Erlauben, **0** für Verweigerung des Zugriffs.
root/ConnectionType/freerdp/authorizations/user/general	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp mit dem HP ThinPro Control Center besitzt. Nicht zutreffend für HP Smart Zero Core. Einrichten auf **1** für Erlauben, **0** für Verweigerung des Zugriffs.
root/ConnectionType/freerdp/connections/{UUID}/address	Die IP oder der Host-Name des Remote-Hosts, mit dem dem Sie eine Verbindung herstellen möchten.
root/ConnectionType/freerdp/connections/{UUID}/application	
root/ConnectionType/freerdp/connections/{UUID}/attachToConsole	
root/ConnectionType/freerdp/connections/{UUID}/audioLatency	Der durchschnittliche Offset in Millisekunden zwischen dem Audiostream und der Anzeige der entsprechenden Videoframes nach dem Entschlüsseln.
root/ConnectionType/freerdp/connections/{UUID}/authorizations/user/edit	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Einrichten auf **1** für Erlauben, **0** für Verweigerung des Zugriffs. **HINWEIS:** Die Verbindung kann im Administratormodus bearbeitet werden, auch wenn dieser Schlüssel auf **0** eingestellt ist.

Tabelle C-3 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/{UUID}/authorizations/user/execution	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Einrichten auf **1** für Erlauben, **0** für Verweigerung des Zugriffs. **HINWEIS:** Die Verbindung kann im Administratormodus bearbeitet werden, auch wenn diese Taste auf **0** eingestellt ist.
root/ConnectionType/freerdp/connections/{UUID}/autoReconnect	Bei der Einstellung auf **1**, wird die Verbindung neu gestartet, falls sie geschlossen oder getrennt ist. Dies ist häufig nützlich für Anwendungen im Kiosk-Stil. Bei der Einstellung auf **0**, wird die Verbindung nicht neu gestartet, falls sie geschlossen oder getrennt ist.
root/ConnectionType/freerdp/connections/{UUID}/autoReconnectDelay	Gibt die Zeit in Sekunden an, bevor die Verbindung neu gestartet wird. Der Standardwert von **0** wird die Verbindung sofort nach dem Schließen oder Trennen neu starten. Diese Einstellung ist nur wirksam,wenn "autoReconnect" auf **1** eingestellt ist.
root/ConnectionType/freerdp/connections/{UUID}/autostart	Bei der Einstellung auf **1**, wird die Verbindung automatisch beim Systemstart gestartet. Dies ist nützlich für Anwendungen im Kiosk-Stil. Standardmäßig werden Verbindungen nicht automatisch gestartet.
root/ConnectionType/freerdp/connections/{UUID}/autostartDelay	Gibt die Zeit in Sekunden an, bis die Verbindung beim Starten gestartet wird. Der Standardwert von **0** wird die Verbindung sofort beim Starten starten. Diese Einstellung ist nur wirksam,wenn "autostart" auf **1** eingestellt ist.
root/ConnectionType/freerdp/connections/{UUID}/colorDepth	Diese Einstellung ist veraltet. Sie wird verwendet, um die Farbtiefe der Verbindung auf eine Farbtiefe unterhalb der nativen Desktopauflösung zu reduzieren. Dies wird häufig verwendet, um die Netzwerkbandbreite zu reduzieren. **HINWEIS:** Die Verringerung der Farbtiefe auf eine Ebene, die nicht vom Videotreiber unterstützt wird, kann zur Bildschirmbeschädigung oder zu Startfehlern führen.
root/ConnectionType/freerdp/connections/{UUID}/compression	Falls der Wert auf **1**, gesetzt wird, ist die Komprimierung von RDP-Daten zwischen dem Client und Server aktiviert. Die Einstellung **0** deaktiviert die Komprimierung. Die Komprimierung ist standardmäßig aktiviert.
root/ConnectionType/freerdp/connections/{UUID}/dependConnectionId	
root/ConnectionType/freerdp/connections/{UUID}/directory	
root/ConnectionType/freerdp/connections/{UUID}/disableMMRwithRFX	Wenn die Einstellung nicht **0** ist, wird die Multimedia-Umleitung deaktiviert, falls eine gültige RemoteFX-Sitzung aufgebaut wurde.
root/ConnectionType/freerdp/connections/{UUID}/domain	Die Standarddomäne zur Versorgung des Remote-Host während der Anmeldung. Wenn eine Domäne nicht angegeben ist, wird die Standard-Domäne für den Remote-Host verwendet.
root/ConnectionType/freerdp/connections/{UUID} / extraEnvValues/{UUID}/key	
root/ConnectionType/freerdp/connections/{UUID} / extraEnvValues/{UUID}/value	

Tabelle C-3 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/{UUID}/fallBackConnection	Wenn die Einstellung auf die UUID einer anderen verfügbaren UUID-Verbindung erfolgte, wird diese Verbindung automatisch gestartet, falls die aktuelle Verbindung fehlschlägt oder wenn ein Fehler auftritt und sie nicht gestartet werden kann. Die UUID der gewünschten Fallback-Verbindung finden Sie normalerweise durch Ausführen von "connection-mgr list" auf dem Client oder indem Sie zu `root/ConnectionType/<type>/connections/` navigieren.
root/ConnectionType/freerdp/connections/{UUID}/frameAcknowledgeCount	Die Anzahl der Videoframes, die der Server pushen kann, ohne auf eine Bestätigung vom Client zu warten. Niedrigere Zahlen führen zu einem schneller reagierenden Desktop, jedoch einer niedrigen Bildfrequenz. Falls der Wert auf **0** eingerichtet wird, wird die Frame-Bestätgung bei den Client-Server-Interaktionen nicht verwendet.
root/ConnectionType/freerdp/connections/{UUID}/hasDesktopIcon	Falls der Wert auf **1** eingerichtet ist, wird ein Symbol für die Verbindung auf dem Desktop angezeigt. Nicht zutreffend für HP Smart Zero Core.
root/ConnectionType/freerdp/connections/{UUID}/label	Der Name der Verbindung im HP ThinPro Control Center. Bei HP Smart Zero Core wird dies normalerweise auf "Standardverbindung" eingerichtet und wird nicht in der Benutzeroberfläche angezeigt.
root/ConnectionType/freerdp/connections/{UUID}/mouseMotionEvents	Bei der Einstellung auf **0** werden die Mausbewegungsereignisse nicht an den Server gesendet. Dies kann dazu führen, das Benutzerfeedback wie Quickinfos nicht richtig funktionieren.
root/ConnectionType/freerdp/connections/{UUID}/offScreenBitmaps	Bei der Einstellung auf **0** werden Off-Screen-Bitmaps deaktiviert. Dies kann die Leistung etwas erhöhen, wird aber dazu führen, dass Blocks des Bildschirms asynchron aktualisiert werden, wodurch Übergänge nicht gleichmäßig aktualisiert werden.
root/ConnectionType/freerdp/connections/{UUID}/password	Das Standardkennwort, das der Remote-Host während der Anmeldung benötigt. Dieser Wert wird verschlüsselt gespeichert. Im Allgemeinen wird diese Einstellung für Anwendungen im Kioskstil verwendet, bei denen ein allgemeines Kennwort für die Anmeldung benutzt wird.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagDesktopComposition	Falls der Wert auf **1** eingerichtet ist, wird die Desktopkomposition erlaubt, wie durchscheinende Rahmen, falls vom Server unterstützt. Wenn Sie es ausschalten, könnte dies die Leistung für Verbindungen mit niedriger Bandbreite verbessern. Im Allgemeinen betrifft dies nur RemoteFX.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagFontSmoothing	Falls der Wert auf **1** eingerichtet ist, wird die Schriftglättungsfunktion erlaubt, wenn dies vom Server unterstützt wird und aktiviert ist. Wenn Sie es ausschalten, könnte dies die Leistung für Verbindungen mit niedriger Bandbreite verbessern.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoCursorSettings	Falls der Wert auf **1**, deaktiviert Cursor blinkt, was kann die Leistung verbessern mit geringer Bandbreite auf RDP-Verbindungen.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoCursorShadow	Falls der Wert auf **1** eingerichtet ist, werden dadurch die Mauszeigerschatten ausgeschaltet. Dies kann die Leistung bei Verbindungen mit niedriger Bandbreite verbessern.

Tabelle C-3 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoMenuAnimations	Falls der Wert auf **1** eingerichtet ist, werden die Menüanimationen ausgeschaltet. Dies kann die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessern.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoTheming	Falls der Wert auf **1** eingerichtet ist, werden die Themen der Benutzeroberfläche abgeschaltet. Dies kann die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessern.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoWallpaper	Falls der Wert auf **1** eingerichtet ist, werden die Desktop-Hintergrundbilder abgeschaltet. Dies kann die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessern.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoWindowDrag	Falls der Wert auf **1** eingerichtet ist, wird das Ziehen des vollständigen Fensters abgeschaltet. Dies kann die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessern. Statt dessen werden die Fensterumrisse verwendet.
root/ConnectionType/freerdp/connections/{UUID}/port	Die Portnummer, die zum Kontaktieren des RDP-Servers zu verwenden ist. Standardmäßig ist diese Option auf **3389** eingerichtet und muss nur selten geändert werden.
root/ConnectionType/freerdp/connections/{UUID}/portMapping	Falls der Wert auf **1** eingerichtet ist, werden die folgenden lokalen seriellen und parallelen Anschlüsse zum Remote-Host umgeleitet. ttyS0, ttyS1, ttyS2, ttyS3, ttyUSB0, lp0.
root/ConnectionType/freerdp/connections/{UUID}/printerMapping	Falls der Wert auf **1** eingerichet wird, wird das Umleitungs-Plugin für CUPS-Drucker aktiviert, wodurch alle Drucker lokal über CUPS definiert werden, um an den Remote-Host weitergeleitet zu werden.
root/ConnectionType/freerdp/connections/{UUID}/rdpEncryption	Falls der Wert auf **1** eingerichtet ist, wird die Standard-RDP-Verschlüsselung zum Verschlüsseln aller Daten zwischen dem Client und dem Server verwendet.
root/ConnectionType/freerdp/connections/{UUID}/remoteFx	Verwenden Sie RemoteFX, falls verfügbar.
root/ConnectionType/freerdp/connections/{UUID}/seamlessWindow	Falls der Wert auf **1** eingerichtet ist, werden die Fensterdekorationen deaktiviert. Dies kann in einer Multi-Monitor-Umgebung erwünscht sein, damit dieVerbindung auf die Größe des Hauptmonitors eingerichtet werden kann.
root/ConnectionType/freerdp/connections/{UUID}/sendHostname	Der angegebene Text wird als Client-Host-Name an den Remote-Host gesendet. Wenn das Feld leer bleibt, wird der System-Host-Name an den Host-Namen gesendet. **HINWEIS:** Der Schlüssel für allgemeine Einstellungen "root/ConnectionType/freerdp/coreSettings/sendHostname" muss auf "hostname" eingerichtet werden, damit dieser Schlüssel verwendet werden kann.
root/ConnectionType/freerdp/connections/{UUID}/smartcard	Falls der Wert auf **1** eingerichtet ist, wird die lokale Smart Card-Authentifizierung auf dem Remote-Host erlaubt. Dadurch wird die NLA (Network Level Authentication) deaktiviert.
root/ConnectionType/freerdp/connections/{UUID}/sound	Bei der Einstellung auf die Standardeinstellung **Wiedergabe auf diesem Computer** wird der Sound mithilfe eines virtuellen Standardkanal vom Remote-Host zum Client umgeleitet. Bei der Einstellung auf **Auf Remote-Computer lassen** verbleibt der Sound auf dem Remote-Host. Dies kann nützlich sein, wenn ein über USB umgeleitetes Audiogerät verwendet wird. Wenn es auf einen anderen Wert eingestellt ist, wird Audio deaktiviert.

Tabelle C-3 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	HP empfiehlt, dass Sound auf **Wiedergabe auf diesem Computer** eingestellt wird, da dies die Audioqualität verbessert und sicherstellt, dass das gesamte Client-Audio, das durch andere virtuelle Kanäle wie beispielsweise MMR umgeleitet wird, mit den lokalen Audioeinstellungen übereinstimmt.
root/ConnectionType/freerdp/connections/{UUID}/startMode	Wenn die Standardeinstellung **Fokus** lautet und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung mit dem Hinweis zurückgegeben, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/freerdp/connections/{UUID}/ timeoutError	Die gewünschte Anzahl von Millisekunden, die nach dem Verlust einer Verbindung mit dem Server gewartet wird, bevor Ihnen der Server ein Dialogfeld mit einer Fehlermeldung anzeigt und die Verbindung schließt. Deaktiviert, wenn **0** ausgewählt ist.
root/ConnectionType/freerdp/connections/{UUID}/ timeoutWarning	Die gewünschte Anzahl von Millisekunden, die nach dem Verlust einer Verbindung mit dem Server gewartet wird, bevor der Benutzer gewarnt wird, dass die Verbindung getrennt wurde. Deaktiviert, wenn **0** ausgewählt ist.
root/ConnectionType/freerdp/connections/{UUID}/username	Der Standardkennwort, das der Remote-Host während der Anmeldung benötigt. Im Allgemeinen wird diese Einstellung für Anwendungen im Kioskstil verwendet, bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
root/ConnectionType/freerdp/connections/{UUID}/ waitForNetwork	Falls der Wert auf **1** eingerichtet ist, wird die Verbindung nicht gestartet, bis das Netzwerk verfügbar ist. Somit wird sichergestellt, dass auf einem langsamen Netzwerk die Verbindung so lange nicht gestartet wird, bis das Netzwerk verfügbar ist, und somit keine Probleme auftreten.
root/ConnectionType/freerdp/connections/{UUID}/ xkbLayoutId	Wenn sie nicht leer ist, stellen Sie eine XKB-Layout-ID zur Verfügung, um die Systemtastatur zu umgehen. Für den Zugriff auf die Liste der verfügbaren IDs geben Sie ein Terminal ein: xfreerdp --kbd-list
root/ConnectionType/freerdp/coreSettings/appName	Der interne Name der Anwendung, der zum Nachverfolgen der PID verwendet wird, um den Verbindungsstatus zu überwachen. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/coreSettings/className	Der interne Klassenname der X-Windows Anwendung, der verwendet wird, wenn die PID der Verbindung für die Statusüberwachung nachverfolgt wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/coreSettings/ disableLinkDropWarning	Falls der Wert auf **1** eingerichtet ist, muss Zero-Login keinen Dialog ausführen, wenn ein Networklink getrennt wird,da das Protokoll solche Situationen bearbeitet.
root/ConnectionType/freerdp/coreSettings/editor	Der interne Name der Anwendung, der verwendet wird, wenn der Verbindungseditor für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/coreSettings/ generalSettingsEditor	Der interne Name der Anwendung, der verwendet wird, wenn der Editor für die allgemeinen Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.

Tabelle C-3 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/coreSettings/icon16Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 16x16 Pixel für diese Anwendung. Dieses Symbol ist das kleine Symbol links neben dem Namen für die Verbindung im Verbindungsdialog.
root/Connection Type/freerdp/coreSettings/icon32Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 32x32 Pixel für diese Anwendung.
root/Connection Type/freerdp/coreSettings/icon48Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 48x48 Pixel für diese Anwendung. Dies ist das große Symbol im oberen linken Bereich des Verbindungeditors für diesen Verbindungstyp.
root/ConnectionType/freerdp/coreSettings/ initialConnectionTimeout	Die Anzahl der Sekunden, die auf eine erste Antwort vom RDP-Server gewartet wird, bis aufgegeben wird.
root/Connection Type/freerdp/coreSettings/label	Der Name der Verbindung, der unter der Schaltfläche "add" auf dem HP ThinPro und im Verbindungsauswahlbildschirm auf HP Smart Zero Core angezeigt wird.
root/ConnectionType/freerdp/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn "connection-mgr stop" für diese Verbindung angefordert wird. Standardmäßig ist diese **close**. Damit wird ein Standard-Kill-Signal an den Vorgang gesendet. Bei der Einstellung auf **kill** wird der von "appName" angegebene Prozess zwangsweise geschlossen. Bei der Einstellung auf **custom** wird ein vom "wrapperScript" angegebenes, benutzerdefiniertes Ausführungsskript ausgeführt, das mit dem Argument "stop" den Prozess beendet.
root/ConnectionType/freerdp/coreSettings/watchPid	Falls der Wert auf **1** eingerichtet ist, wird die von "appName" angegebene Anwendung überwacht, um die Verbindung zu erkennen. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/coreSettings/wrapperScript	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt wird. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bearbeitet. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/general/enableMMR	Falls der Wert auf **1** eingerichtet ist, wird das MMR-Plugin aktiviert. Dies führt dazu, dass unterstützte Codes, die über den Windows Media Player wiedergegeben werden, an den Client umgeleitet werden. Dies verbessert den Vollbildmodus und die Wiedergabe von High-Definition-Videos für Codes wie WMV9, VC1 und MPEG4 in höchstem Maße.
root/ConnectionType/freerdp/general/sendHostname	Wenn dies auf die Standardeinstellung **hostname** eingerichtet ist, wird der System-Host-Name an den Remote-Host gesendet. Dies wird in der Regel von einem Administrator verwendet, um den Client-Rechner zu identifizieren, der mit einerm bestimmten RDP-Sitzung verknüpft ist. Der gesendete Host-Name kann überschrieben werden, indem der Schlüssel "sendHostname" in den für die Verbindung angegebenen Einstellungen eingerichtet wird. Falls dies auf **Mac** eingerichtet wird, wird anstelle des Host-Namens die MAC-Adresse des ersten verfügbaren Netzwerkadapters gesendet.

root > ConnectionType > view

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

Tabelle C-4 root > ConnectionType > view

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/authorizations/user/add	Zeigt an, ob der Benutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs durch das HP ThinPro Control Center besitzt. Nicht zutreffend für HP Smart Zero Core. Einrichten auf **1** für Erlauben, **0** für Verweigerung des Zugriffs.
root/ConnectionType/view/authorizations/user/general	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp mit dem HP ThinPro Control Center besitzt. Nicht zutreffend für HP Smart Zero Core. Einrichten auf **1** für Erlauben des Zugriffs, **0**. zur Verweigerung des Zugriffs.
root/ConnectionType/view/connections/{UUID}/afterStartedCommand	Der vollständige Pfad zu einem Skript oder Binärdatei, das bzw. die nach dem Start der Verbindung auszuführen ist.
root/ConnectionType/view/connections/{UUID}/afterStoppedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach Beendigung der Verbindung ausgeführt werden soll.
root/ConnectionType/view/connections/{UUID}/appInMenu	
root/ConnectionType/view/connections/{UUID}/appOnDesktop	
root/ConnectionType/view/connections/{UUID}/attachToConsole	
root/ConnectionType/view/connections/{UUID}/authorizations/user/edit	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Einrichten auf **1** für Erlauben des Zugriffs, **0**. zur Verweigerung des Zugriffs. **HINWEIS:** Die Verbindung kann im Administratormodus bearbeitet werden, auch wenn dieser Schlüssel auf **0** eingerichtet ist.
root/ConnectionType/view/connections/{UUID}/authorizations/user/execution	Zeigt an, ob der Benutzer die Berechtigung zum Ausführen der Verbindung an. Einrichten auf **1** für Erlauben des Zugriffs, **0**. zur Verweigerung des Zugriffs. **HINWEIS:** Die Verbindung kann im Administratormodus bearbeitet werden, auch wenn dieser Schlüssel auf **0** eingerichtet ist.
root/ConnectionType/view/connections/{UUID}/automaticLogin	Wenn diese Option aktiviert ist, wird der VMware Horizon View-Client versuchen, sich automatisch anzumelden,wenn alle Felder zur Verfügung stehen. Wenn dies nicht aktiviert ist, müssen Benutzer manuell im VMware Horizon View-Client auf **Verbinden** klicken, um mit dem VMware Horizon View-Server Kontakt aufzunehmen, sich anzumelden und einen Desktop auszuwählen.
root/ConnectionType/view/connections/{UUID}/autoReconnect	Falls **1** ausgewählt ist, wird das System versuchen, die Verbindung automatisch neu zu starten nachdem sie geschlossen wurde. Falls erforderlich, sollten im Feld `zero-login/defaultCredentials` Anmeldeinformationen bereitgestellt werden. "autostart" wird häufig in Verbindung mit dieser Einstellung verwendet.

Tabelle C-4 root > ConnectionType > view (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/{UUID}/autoReconnectDelay	Gibt die Zeit in Sekunden an, bevor die Verbindung neu gestartet wird. Der Standardwert von **0** wird die Verbindung sofort nach dem Schließen oder Trennen neu starten. Diese Einstellung ist nur wirksam,wenn "autoReconnect" auf **1** eingestellt ist.
root/ConnectionType/view/connections/{UUID}/autostart	Wenn dies größer als **0** ist, wird das System versuchen, die Verbindung automatisch herzustellen, wenn der Client gestartet wird. Falls erforderlich, sollten im Feld `zero-login/defaultCredentials` Anmeldeinformationen bereitgestellt werden. "autoReconnect" wird häufig in Verbindung mit dieser Einstellung verwendet.
root/ConnectionType/view/connections/{UUID}/autostartDelay	Gibt die Zeit in Sekunden an, bis die Verbindung beim Starten gestartet wird. Der Standardwert von **0** wird die Verbindung sofort beim Starten starten. Diese Einstellung ist nur wirksam,wenn "autostart" auf **1** eingestellt ist.
root/ConnectionType/view/connections/{UUID}/beforeStartingCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/view/connections/{UUID}/closeAfterDisconnect	Falls der Wert auf **1** eingerichtet ist, wird die Verbindung geschlossen, nachdem der erste Desktop getrennt wurde. Wenn dies nicht aktiviert ist, kehrt der VMware Horizon View-Client zurück zum Desktopauswahlbildschirm. Dies ist standardmäßig aktiviert, damit Benutzer nach dem Abmelden nicht versehentlich die Verbindung am Desktopauswahlbildschirm belassen.
root/ConnectionType/view/connections/{UUID}/colorDepth	
root/ConnectionType/view/connections/{UUID}/coord	
root/ConnectionType/view/connections/{UUID}/dependConnectionId	
root/ConnectionType/view/connections/{UUID}/desktop	Wenn angegeben, wird der benannte Desktop beim Anmelden automatisch gestartet. **HINWEIS:** Standardmäßig wird er, wenn nur ein Desktop verfügbar ist, automatisch gestartet, ohne angegeben worden zu sein.
root/ConnectionType/view/connections/{UUID}/directory	
root/ConnectionType/view/connections/{UUID}/domain	Die Domäne, die an VMware Horizon View-Server bereitstellt. Wenn keine Domäne angegeben ist, wird die Standarddomäne verwendet.
root/ConnectionType/view/connections/{UUID}/enableSingleMode	
root/ConnectionType/view/connections/{UUID}/ExtraArgs	Zusätzliche Argumente zum VMware Horizon View-Client können hier angegebenen werden. Führen Sie "view_client --help" or "vmware-view --help" über eine Terminalsitzung aus, um alle verfügbaren Argumente zu sehen.
root/ConnectionType/view/connections/{UUID}/extraEnvValues/{UUID}/key	
root/ConnectionType/view/connections/{UUID}/extraEnvValues/{UUID}/value	

Tabelle C-4 root > ConnectionType > view (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/{UUID}/fallBackConnection	Wenn die Einstellung auf die UUID einer anderen verfügbaren UUID-Verbindung erfolgte, wird diese Verbindung automatisch gestartet, falls die aktuelle Verbindung fehlschlägt oder wenn ein Fehler auftritt und sie nicht gestartet werden kann. Die UUID der gewünschten Fallback-Verbindung finden Sie normalerweise durch Ausführen von "connection-mgr list" auf dem Client oder indem Sie zu `root/ConnectionType/<Type>/connections/` navigieren.
root/ConnectionType/view/connections/{UUID}/fullscreen	Bei der Einstellung auf **1** wird der VMware Horizon View-Client im Vollbildmodus gestartet.
root/ConnectionType/view/connections/{UUID}/hasDesktopIcon	Falls der Wert auf **1** eingerichtet ist, wird die Verbindung auf dem HP ThinPro Desktop angezeigt. Nicht zutreffend für HP Smart Zero Core.
root/ConnectionType/view/connections/{UUID}/hideMenuBar	Falls der Wert auf **1** eingerichtet ist, wird die obere Menüleiste innerhalb des Desktops ausgeblendet. Diese Leiste wird zur Verwaltung von Remote-Geräten und zum Starten anderer Desktops verwendet. Standardmäßig wird diese auf HP ThinPro angezeigt und auf HP Smart Zero Core ausgeblendet.
root/ConnectionType/view/connections/{UUID}/isInMenu	Falls der Wert auf **1** eingerichtet ist, wird die Verbindung auf der HP ThinPro-Taskleiste angezeigt. Nicht zutreffend für HP Smart Zero Core.
root/ConnectionType/view/connections/{UUID}/label	Der Name der Verbindung. Diese Option wird verwendet von "oot/ConnectionManager/defaultConnection", um anzugeben, welche Verbindung beim Start gestartet werden soll sowie innerhalb des HP ThinPro-Verbindungsmanagers.
root/ConnectionType/view/connections/{UUID}/password	Das Standardkennwort, das der Remote-Host während der Anmeldung benötigt. Dieser Wert wird verschlüsselt gespeichert. Im Allgemeinen wird diese Einstellung für Anwendungen im Kioskstil verwendet, bei denen ein allgemeines Kennwort für die Anmeldung benutzt wird.
root/ConnectionType/view/connections/{UUID}/saveCredentials	
root/ConnectionType/view/connections/{UUID}/server	Die Adresse des Remote-Host, mit dem eine Verbindung hergestellt werden soll. In der Regel ist dies eine URL wie "https://server.domain.com'.
root/ConnectionType/view/connections/{UUID}/sessionEndAction	
root/ConnectionType/view/connections/{UUID}/singleDesktop	
root/ConnectionType/view/connections/{UUID}/smartcard	Bei Aktivierung leitet dies alle lokal angeschlossenen Smart Cards an den Remote-Host weiter. Damit können sie von Anwendungen auf dem Remote-Host verwendet werden. Damit wird nicht die Smart Card-Anmeldung für die VMware Horizon View-Serveranmeldung aktiviert, sondern nur für den Remote-Host
root/ConnectionType/view/connections/{UUID}/startMode	Wenn die Standardeinstellung auf **focus** eingerichtet ist und die Verbindung bereits gestartet ist, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung mit dem Hinweis Verbindung ist bereits gestartet zurückgegeben.

Tabelle C-4 root > ConnectionType > view (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/{UUID}/username	Der Standardkennwort, das der Remote-Host während der Anmeldung benötigt. Im Allgemeinen wird diese Einstellung für Anwendungen im Kioskstil verwendet, bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
root/ConnectionType/view/connections/{UUID}/viewSecurityLevel	Wenn die Standardeinstellung auf **Refuse** eingerichtet ist, wird der VMware Horizon View-Client dem Benutzer nicht erlauben, eine Verbindung mit dem Server herzustellen, falls das SSL-Zertifikat des Servers ungültig ist. Wenn **Warn** eingerichtet ist, wird der VMware Horizon View-Client warnen, wenn das Zertifikat nicht überprüft werden kann, und wenn es selbstsigniert oder abgelaufen ist, erhält der Benutzer weiterhin keine Erlaubnis zur Verbindungsherstellung. Wenn **Allow all connections** eingerichet ist, wird das Server Zertifikat nicht überprüft und Verbindungen zu jedem beliebigen Server sind zulässig.
root/ConnectionType/view/connections/{UUID}/waitForNetwork	Falls der Wert auf **1** eingerichtet ist, wird die Verbindung nicht gestartet, bis das Netzwerk verfügbar ist. Somit wird sichergestellt, dass auf ein langsames Netzwerk vor, ist die Verbindung wird nicht gestartet, was zu einem Netzwerk verfügbar ist.
root/ConnectionType/view/connections/{UUID}/windowsizeHeight	Nicht zutreffend für HP Smart Zero Core.
root/ConnectionType/view/connections/{UUID}/windowsizePercentage	
root/ConnectionType/view/connections/{UUID}/windowsizeWidth	Nicht zutreffend für HP Smart Zero Core.
root/ConnectionType/view/connections/{UUID}/windowType	Nicht zutreffend für HP Smart Zero Core.
root/ConnectionType/view/coreSettings/appName	Der interne Name der Anwendung, der zum Nachverfolgen der PID verwendet wird, um den Verbindungsstatus zu überwachen. Dieser Schlüssel sollte keine Änderung erfordern.
ConnectionType/view/coreSettings/className User (Benutzer anzeigen/ändern)	Der interne Klassenname der X-Windows Anwendung, der verwendet wird, wenn die PID der Verbindung für die Statusüberwachung nachverfolgt wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/view/coreSettings/editor	Der interne Name der Anwendung, der verwendet wird, wenn der Verbindungseditor für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
ConnectionType/view/coreSettings/icon16Path User (Benutzer anzeigen/ändern)	Der interne Pfad für das Anwendungssymbol für das Symbol mit 16x16 Pixel für diese Anwendung. Dies ist das kleine Symbol links neben dem Namen für die Verbindung in der connection Dialog.
ConnectionType/view/coreSettings/icon32Path User (Benutzer anzeigen/ändern)	Der interne Pfad für das Anwendungssymbol für das Symbol mit 32x32 Pixel für diese Anwendung.
ConnectionType/view/coreSettings/icon48Path User (Benutzer anzeigen/ändern)	Der interne Pfad für das Anwendungssymbol für das Symbol mit 48x48 Pixel für diese Anwendung. Dies ist das große Symbol im oberen linken Bereich des Verbindungeditors für diesen Verbindungstyp.

Tabelle C-4 root > ConnectionType > view (Fortsetzung)

Registrierungsschlüssel	Beschreibung
Erstellung einer Beschriftung mit ConnectionType/view/coreSettings/label	Der Name der Verbindung, der unter der Schaltfläche "add" auf dem HP ThinPro und im Verbindunsauswahlbildschirm auf HP Smart Zero Core angezeigt wird.
root/ConnectionType/view/coreSettings/serverRequired	Gibt an, ob ein Servername oder eine Adresse unbenutzt, optional oder für diesen Verbindungstyp erforderlich ist.
root/ConnectionType/view/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn "connection-mgr stop" für diese Verbindung angefordert wird. Standardmäßig ist diese **close**. Damit wird ein Standard-Kill-Signal an den Vorgang gesendet. Bei der Einstellung auf **kill** wird der von "appName" angegebene Prozess zwangsweise geschlossen. Bei der Einstellung auf **custom** wird ein benutzerdefiniertes Ausführungsskript (angegeben durch "wrapperscript") mit dem Argument "stop" ausgeführt, um den Prozess sanft zu beenden.
root/ConnectionType/view/coreSettings/watchPid	Falls der Wert auf **1** eingerichtet ist, wird die von "appName" angegebene Anwendung überwacht, um die Verbindung zu erkennen. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/view/coreSettings/wrapperScript	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt wird. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bearbeitet. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/view/general/rdpOptions	Die hier angegebenen Optionen werden direkt an den RDP-Client weitergeleitet, wenn RDP als Anzeigeprotokol für die VMware Horizon View-Verbindung verwendet wird. Um eine vollständige Liste der Optionen zu sehen, geben Sie im Client-Terminal "rdesktop --help" ein.
root/ConnectionType/view/gui/viewManager/name	Der Name des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/view/gui/viewManager/status	Der aktive Status der Einstellungseditor für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/view/gui/viewManager/title	Der Fenstertitel des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/view/gui/viewManager/widgets/autostart	
root/ConnectionType/view/gui/viewManager/widgets/fallBackConnection	
root/ConnectionType/view/gui/viewManager/widgets/label	

root > ConnectionType > xen

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

Tabelle C-5 root > ConnectionType > xen

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/authorizations/user/add	Zeigt an, ob der Benutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs durch das HP ThinPro Control Center besitzt. Nicht zutreffend für HP Smart Zero Core. Einrichten auf **1** für Erlauben, **0** für Verweigerung des Zugriffs.
root/ConnectionType/xen/authorizations/user/general	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp mit dem HP ThinPro Control Center besitzt. Nicht zutreffend für HP Smart Zero Core. Einrichten auf **1** für Erlauben, **0** für Verweigerung des Zugriffs.
root/ConnectionType/xen/connections/{UUID}/address	Die Adresse des Remote-Host, mit dem eine Verbindung hergestellt werden soll. In der Regel ist dies eine URL wie "https://server.domain.com".
/Connectiontype/xen/ -Verbindungen/ {UUID} / afterstartedcommand	Der vollständige Pfad zu einem Skript oder Binärdatei, das bzw. die nach dem Start der Verbindung auszuführen ist.
root/ConnectionType/xen/connections/{UUID}/ afterStoppedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach Beendigung der Verbindung ausgeführt werden soll.
root/ConnectionType/xen/connections/{UUID}/appInMenu	Falls der Wert auf **1** eingerichtet ist, werden alle Anwendungen für diese Verbindung auf dem Taskleistenmenü angezeigt.
root/ConnectionType/xen/connections/{UUID}/ appOnDesktop	Falls der Wert auf **1** eingerichtet ist, werden alle Anwendungen für diese Verbindung auf dem Desktop angezeigt.
root/ConnectionType/xen/connections/{UUID}/authorizations/ user/edit	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Einrichten auf **1** für Erlauben, **0** für Verweigerung des Zugriffs. **HINWEIS:** Die Verbindung kann im Administratormodus bearbeitet werden, auch wenn dieser Schlüssel auf **0** eingerichtet ist.
root/ConnectionType/xen/connections/{UUID}/authorizations/ user/execution	Zeigt an, ob der Benutzer die Berechtigung zum Ausführen der Verbindung an. Einrichten auf **1** für Erlauben, **0** für Verweigerung des Zugriffs. **HINWEIS:** Diese Verbindung wird immer im Administratormodus zum Starten verfügbar sein.
root/ConnectionType/xen/connections/{UUID}/ autoReconnect	Falls der Wert auf **1**, eingerichtet ist, wird das System versuchen, die Verbindung automatisch neu zu starten, nachdem sie geschlossen wurde. Falls erforderlich, sollten im Feld `zero-login/defaultCredentials` Anmeldeinformationen bereitgestellt werden. "autostart" wird häufig in Verbindung mit dieser Einstellung verwendet.
root/ConnectionType/xen/connections/{UUID}/ autoReconnectDelay	Gibt die Zeit in Sekunden an, bevor die Verbindung neu gestartet wird. Der Standardwert von **0** wird die Verbindung sofort nach dem Schließen oder Trennen neu starten. Diese Einstellung ist nur wirksam,wenn "autoReconnect" auf **1** eingestellt ist.
root/ConnectionType/xen/connections/{UUID}/autostart	Wenn dies größer als **0** ist, wird das System versuchen, die Verbindung automatisch herzustellen, wenn der Client gestartet wird. Falls erforderlich, sollten im Feld `zero-login/defaultCredentials` Anmeldeinformationen

Tabelle C-5 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	bereitgestellt werden. "autoReconnect" wird häufig in Verbindung mit dieser Einstellung verwendet.
root/ConnectionType/xen/connections/{UUID}/autostartDelay	Gibt die Zeit in Sekunden an, bis die Verbindung beim Starten gestartet wird. Der Standardwert von **0** wird die Verbindung sofort beim Starten starten. Diese Einstellung ist nur wirksam,wenn "autostart" auf **1** eingestellt ist.
root/ConnectionType/xen/connections/{UUID}/ autoStartDesktop	Um automatisch den ersten verfügbaren Desktop zu starten, wenn Sie eine Citrix-Verbindung starten, setzen Sie den Wert für den Schlüssel auf **1**.
root/ConnectionType/xen/connections/{UUID}/ autoStartResource	Um einen Desktop oder einen Anwendung automatisch zu starten, wenn Sie eine Citrix-Verbindung starten, richten Sie den Wert des folgenden Schlüssels auf den Namen des Desktops oder der Anwendung die Sie starten möchten.
root/ConnectionType/xen/connections/{UUID}/ beforeStartingCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/xen/connections/{UUID}/ clearCredentialsTimeout	
root/ConnectionType/xen/connections/{UUID}/ connectionEndAction	
root/ConnectionType/xen/connections/{UUID}/coord	
root/ConnectionType/xen/connections/{UUID}/ dependConnectionId	
root/ConnectionType/xen/connections/{UUID}/ disableSaveCredentials	
root/ConnectionType/xen/connections/{UUID}/domain	Die Domäne für die XenDesktop-Server. Wenn keine Domäne angegeben ist, wird die Standarddomäne für den Server verwendet.
root/ConnectionType/xen/connections/{UUID}/ enablePNADesktopIcons	
root/ConnectionType/xen/connections/{UUID}/enablePNA StartMenuItems	
root/ConnectionType/xen/connections/{UUID}/ extraEnvValues/{UUID}/key	
root/ConnectionType/xen/connections/{UUID}/ extraEnvValues/{UUID}/value	
root/ConnectionType/xen/connections/{UUID}/ fallBackConnection	Wenn die Einstellung auf die UUID einer anderen verfügbaren UUID-Verbindung erfolgte, wird diese Verbindung automatisch gestartet, falls die aktuelle Verbindung fehlschlägt oder wenn ein Fehler auftritt und sie nicht gestartet werden kann. Die UUID der gewünschten Fallback-Verbindung finden Sie normalerweise durch Ausführen von "connection-mgr list" auf dem Client oder indem Sie zu "root/ConnectionType/<type>/connections/" navigieren.
root/ConnectionType/xen/connections/{UUID}/folder	

Tabelle C-5 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/connections/{UUID}/fullscreen	Bei der Festlegung auf **1** wird der ICA-Client im Vollbildmodus gestartet.
root/ConnectionType/xen/connections/{UUID}/hasDesktopIcon	Falls der Wert auf **1** eingerichtet ist, wird ein Symbol für die Verbindung auf dem Desktop angezeigt. Nicht zutreffend für HP Smart Zero Core.
root/ConnectionType/xen/connections/{UUID}/isInMenu	
root/ConnectionType/xen/connections/{UUID}/label	Der Name der Verbindung. Diese Option wird verwendet von `root/ConnectionManager/defaultConnection`, um anzugeben, welche Verbindung beim Start gestartet werden soll sowie innerhalb des HP ThinPro-Verbindungsmanagers.
root/ConnectionType/xen/connections/{UUID}/logOnMethod	
root/ConnectionType/xen/connections/{UUID}/password	Falls es eingerichtet wird, wird dieses Kennwort als Standard für den Anmeldedialog bereitgestellt, wenn die Standards der Benutzer und der Domäne hier übereinstimmen. In der Regel wird dies mit "autostart"-Verbindungen verwendet.
root/ConnectionType/xen/connections/{UUID}/savePassword	
root/ConnectionType/xen/connections/{UUID}/startMode	Wenn die Standardeinstellung auf **focus** eingerichtet ist und die Verbindung bereits gestartet ist, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung mit dem Hinweis Verbindung ist bereits gestartet zurückgegeben.
root/ConnectionType/xen/connections/{UUID}/username	Der Standardkennwort, das der Remote-Host während der Anmeldung benötigt. Im Allgemeinen wird diese Einstellung für Anwendungen im Kioskstil verwendet, bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
root/ConnectionType/xen/connections/{UUID}/waitForNetwork	Falls der Wert auf **1** eingerichtet ist, wird die Verbindung nicht gestartet, bis das Netzwerk verfügbar ist. Somit wird sichergestellt, dass auf einem langsamen Netzwerk die Verbindung so lange nicht gestartet wird, bis das Netzwerk verfügbar ist, und somit keine Probleme auftreten.
root/ConnectionType/xen/coreSettings/appName	Der interne Name der Anwendung, der zum Nachverfolgen der PID verwendet wird, um den Verbindungsstatus zu überwachen. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/autoLogoutDelay	Diese Einstellung gilt für Citrix Server mit mehreren veröffentlichten Apps oder Desktops. Wenn dieser Wert mit **weniger als 0** angegeben wird, wird keine automatische Abmeldung durchgeführt. Andernfalls ist dies die Anzahl der Sekunden zwischen dem Schließen der letzten Xen-Anwendung und dem Zeitpunkt, zu dem der Xen-Desktop automatisch geschlossen wird. Verzögerungen bei der Citrix-Verarbeitung können die Verarbeitungszeit bis zur automatischen Abmeldung verlängern.
root/ConnectionType/xen/coreSettings/autoLogoutDelaySingleApp	Diese Einstellung gilt für Citrix-Server mit einem einzigen veröffentlichten App oder Desktop. Wenn dieser Wert mit **weniger als 0** angegeben wird, wird keine automatische Abmeldung durchgeführt. Andernfalls ist dies die Anzahl der Sekunden zwischen dem Schließen der letzten Xen-Anwendung und dem Zeitpunkt, zu dem der Xen-Desktop wird automatisch geschlossen wird. Verzögerungen bei der Citrix-Verarbeitung können die Verarbeitungszeit bis zur automatischen Abmeldung verlängern.

Tabelle C-5 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/coreSettings/className	Der interne Klassenname der X-Windows Anwendung, der verwendet wird, wenn die PID der Verbindung für die Statusüberwachung nachverfolgt wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/editor	Der interne Name der Anwendung, der verwendet wird, wenn der Verbindungseditor für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/generalSettingsEditor	Der interne Name der Anwendung, der verwendet wird, wenn der Editor für die allgemeinen Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/icon16Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 16x16 Pixel für diese Anwendung. Dieses Symbol ist das kleine Symbol links neben dem Namen für die Verbindung im Verbindungsdialog.
root/ConnectionType/xen/coreSettings/icon32Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 32x32 Pixel für diese Anwendung.
root/ConnectionType/xen/coreSettings/icon48Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 48x48 Pixel für diese Anwendung. Dies ist das große Symbol im oberen linken Bereich des Verbindungeditors für diesen Verbindungstyp.
root/ConnectionType/xen/coreSettings/label	Der Name der Verbindung, der unter der Schaltfläche "add" auf dem HP ThinPro und im Verbindungsauswahlbildschirm auf HP Smart Zero Core angezeigt wird.
root/ConnectionType/xen/coreSettings/serverRequired	Gibt an, ob ein Servername oder eine Adresse unbenutzt, optional oder für diesen Verbindungstyp erforderlich ist.
root/ConnectionType/xen/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn "connection-mgr stop" für diese Verbindung angefordert wird. Standardmäßig ist diese **close**. Damit wird ein Standard-Kill-Signal an den Vorgang gesendet. Bei der Einstellung auf **kill** wird der von "appName" angegebene Prozess zwangsweise geschlossen. Bei der Einstellung auf **custom** wird ein vom "wrapperScript" angegebenes, benutzerdefiniertes Ausführungsskript ausgeführt, das mit dem Argument "stop" den Prozess beendet.
root/ConnectionType/xen/coreSettings/watchPid	Falls der Wert auf **1** eingerichtet ist, wird die von "appName" angegebene Anwendung überwacht, um die Verbindung zu erkennen. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/wrapperScript	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt wird. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bearbeitet. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/general/allowReadOn**{AthruZ}**	Richten Sie ihn auf **1** ein, damit der Benutzer das zugeordnet Laufwerke vom Remote-Host lesen kann. Wenn diese Einstellung auf **0** eingerichtet wird, werden keine Dateien in dem zugeordneten Laufwerk auf dem Remote-Host angezeigt.
root/ConnectionType/xen/general/allowWriteOn**{AthruZ}**	Richten Sie ihn auf **1**, damit der Benutzer auf das zugeordnete Laufwerk vom Remote-Host schreiben kann.

Tabelle C-5 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Wenn diese Einstellung auf **0** eingerichtet wird, kann der Benutzer Dateien vom Laufwerk lesen und kopieren, jedoch keine Änderungen machen oder neue Dateien zu dem Laufwerk hinzufügen.
root/ConnectionType/xen/general/async	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung `CommPollsize=boolean`, die asynchrones Polling aktiviert. Die Standardeinstellung ist **0** für "Off".
root/ConnectionType/xen/general/autoReconnect	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung `TransportReconnectEnabled=boolean`, die die automatische Neuverbindung einer Sitzung aktiviert. Der Standardwert ist **0**. **HINWEIS:** Dies ist nicht identisch mit dem verbindungsspezifischen "autoReconnect". Diese Neuverbindung tritt intern, innerhalb des Citrix-Client auf, ohne dass die Verbindung neu gestartet werden muss.
root/ConnectionType/xen/general/bitmapCacheSize	Direkt Karten in den Citrix INI-Datei Einstellung `Persistentcacheminbitmap=Ganzzahl`, die der Mindestgröße der Bitmap zum cachen. Die Standardeinstellung ist **8192**. Auf allen Clients, ist diese Option auf eine Voreinstellung von **2048**.
root/ConnectionType/xen/general/colorDepth	Zwingt ICA mit Hilfe einer bestimmten Farbe Tiefe für alle Anschlüsse. Dies wird in der Regel entweder in spezialisierten Umgebungen durchgeführt, in denen die automatische Tiefenauswahl fehlschlägt oder in sehr langsamen Netzwerken zur Reduzieren von Überlastungen.
root/ConnectionType/xen/general/colorMapping	Richten Sie **Shared - Approximate Colors** auf aktivieren ein und **Private - Exact Colors** auf deaktivieren. Die Funktion ist standardmäßig aktiviert. Zugeordnet zu der Citrix-INI-Dateieinstellung `ApproximateColors=boolean`, die ungefähre Farben von der Standardfarbkarte verwendet statt einer privaten Farbkarte und präzisen Farben. Nur verwenden, wenn der DesiredColor-Wert 2 beträgt (256 Farben). Der Standard lautet **False**.
root/ConnectionType/xen/general/defaultBrowserProtocol	Richten Sie dies standardmäßig auf **TCP/IP-HTTP Browser** ein. Kann auf **SSL/TLS HTTPS Browser** oder **TCP/IP Browser** eingerichtet werden. Zuordnung zu der Citrix-INI-Dateieinstellung `BrowserProtocol=[UDP|HTTPonTCP]`, die das Protokoll steuert, das zum Auffinden des ICA-Hosts für die Verbindung verwendet wird. Wenn es nicht angegeben ist, wird der Standardwert von [Wfclient]-Abschnitt wfclient.ini verwendet.
root/ConnectionType/xen/general/drivePathMappedOn**{AthruZ}**	Das lokale Dateisystemverzeichnis zur Zuordnung an den Remote-Host. In der Regel ist diese Option auf **/media** eingerichtet, damit alle angeschlossenen USB-Laufwerke dem Remote-Host über einen einzigen Laufwerksbuchstaben zugeordnet werden können.
root/ConnectionType/xen/general/enableAlertSound	Richten Sie dies auf den Standard **1** ein, um die Windows-Warntöne zu aktivieren. Mit dem Wert **0** wird dies deaktiviert. Indirekte Zuordnung zu der Citrix-INI-Dateieinstellung `DisableSound=boolea`, mit der Windows-Warntöne deaktiviert werden. Der Standard lautet **False**.
root/ConnectionType/xen/general/enableAudioInput	Die Standardeinstellung **1** aktiviert den Audioeingang. Damit wird sowohl die Einstellung "AllowAudioInput" als auch die

Tabelle C-5 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Einstellung "EnableAudioInput" in "wfclient.ini" und "appsrv.ini" auf **1** eingerichtet.
root/ConnectionType/xen/general/enableDataCompression	Die Standardeinstellung **1** aktiviert die Datenkomprimierung und **0** deaktiviert sie. Direkte Zuordnung zu der Citrix-INI-Dateieinstellung `Compress=boolean`, die die Datenkomprimierung steuert.
root/ConnectionType/xen/general/enableDriveMapping	Damit können Verzeichnisse auf dem lokalen Dateisystem über ein virtuelles Laufwerk an den Remote-Host weitergeleitet werden. In der Regel würde **/media** Z zugeordnet werden, damit USB-Laufwerke an den Remote-Host weitergeleitet werden können. Wenn die USB-Umleitung aktiviert ist, sollte diese deaktiviert werden, um Speicherkonflikte zu verhindern. Damit das USB-Gerät dem Remote-Host korrekt zugeordnet werden kann, muss das USB-Gerät eines der folgenden Dateisysteme verwenden: FAT32, NTFS, ext2 oder ext3.
root/ConnectionType/xen/general/enableForceDirectConnect	Richten Sie dies auf **1** ein, um die Verbindung zu zwingen, die zu Citrix-Web-Benutzeroberfläche und diePNAgent-Dienste zu umgehen. Die Authentifizierung findet am Server statt, nachdem die erste Verbindung hergestellt wurde.
root/ConnectionType/xen/general/ enableHDXFlashRedirection	Steuerung des Verhaltens der HDX Flash-Umleitung durch Einstellung auf **Always**, **Ask** oder **Never**. Der Standardwert ist "Always" (Immer), um die HDX Flash-Umleitung bei Möglichkeit zu verwenden und den Benutzer nicht dazu aufzufordern. "Ask" (Fragen) wird den Benutzer innerhalb der Sitzung dynamisch auffordern. "Never" (Nie) wird die Funktion deaktivieren.
root/ConnectionType/xen/general/enableHDXMediaStream	Einrichten auf **0**., um HDX MediaStream zu deaktivieren. Wenn HDX Mediastream deaktiviert ist, werden Mediendateien weiterhin über Standardstreaming wiedergegeben, aber die Qualität ist möglicherweise nicht so gut.
root/ConnectionType/xen/general/enableMapOn**{AthruZ}**	Erlaubt das Auftreten von Laufwerkszuordnungen mithilfe des angegebenen Laufwerks auf dem Remote-Host. Muss auf ein gültiges lokales Verzeichnis eingerichtet werden, damit die Laufwerkszuordnung einwandfrei funktioniert. Andere Laufwerksbuchstaben werden auch verfügbar, wenn alle Schlüssel angezeigt werden.
root/ConnectionType/xen/general/enableOffScreenSurface	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung `EnableOSS=boolean`. Damit kann der Server Pixmaps für Offscreen-Zeichnungen erstellen und verwenden. Reduziert die Bandbreite in 15- und 24-Bit Farbe auf Kosten des X-Server-Speicher und -Prozessorzeit. Der Standardwert ist **On**.
root/ConnectionType/xen/general/enableSmartCard	Falls der Wert auf **1** eingerichtet ist, wird "DisableCtrlAltDel" auf "Off" eingestellt und die Smart Card-Anmeldung wird aktiviert. Falls der Wert auf **0**, eingerichtet ist, wird "SmartCardAllowed" auf "Off" eingestellt, damit die Smart Card-Anmeldung deaktiviert wird.
root/ConnectionType/xen/general/ enableWindowsAlertSounds	
root/ConnectionType/xen/general/encryptionLevel	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung `Encryptionlevelsession= [Keine | Basic | RC5`

Tabelle C-5 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	`(128 Bit - Anmelden Nur) | RC5 (40 Bit) | RC5 (56 Bit) | RC5 (128-Bit)]`, mit der die Verschlüsselungsstufe auf einer Basis pro Verbindung angegeben wird. Verschlüsselungsprotokolle für alle Ebenen sind im Abschnitt [Encryptionlevelsession] des module.ini definiert.
root/ConnectionType/xen/general/hotKey**{1 bis 12}**Char	Das zur Remote-Sitzung weiterzuleitende fn-Tasten-Zeichen. Zum Beispiel F1 für hotKey1Char.
root/ConnectionType/xen/general/hotKey**{1 bis 12}**Umschalt	Der Kombinationen mit der Umschalttaste zum Aktivieren der gewählten fn-Tasten-Zeichen. Standardmäßig gilt **Strg +Umschalt**. Kann auf **Umschalt**, **Strg**, **Alt**, **Alt+Umschalt**, **Alt +Strg** oder **Strg+Umschalt** eingerichtet werden.
root/ConnectionType/xen/general/httpAddresses/{UUID}/ address	
root/ConnectionType/xen/general/ keyPassthroughEscapeChar	Ordnet direkt zu den Citrix INI-Dateieinstellungen `KeyPassthroughEscapeChar=string` zu. Dies ist die Taste für den Tastaturbefehl zum Deaktivieren des transparenten Tastaturmodus. Die Standardeinstellung ist **F2**. Alle Clients gesetzt sind standardmäßig auf **F1** eingerichtet.
root/ConnectionType/xen/general/ keyPassthroughEscapeShift	Ordnet direkt den Citrix INI-Dateieinstellungen `KeyPassthroughEscapeShift=string` zu. Dies ist die Taste für den Tastaturbefehl zum Deaktivieren des transparenten Tastaturmodus. Der Standardwert ist **Strg**. Alle Clients sind standardmäßi auf **Alt** eingerichtet.
root/ConnectionType/xen/general/localTextEcho	Kann auf **Ein**, **Aus** oder die Standardeinstellung **Autom.** eingerichtet werden. Indirekte Zuordnung zu der Citrix-INI-Dateieinstellung `ZLKeyboardMode=[0|1|2]`, die die Tastatur-Latenz-Reduktion steuert. 0 = Off 1 = Always on 2 = Dynamische Auswahl basierend auf der tatsächlichen Latenz
root/ConnectionType/xen/general/mouseClickFeedback	Kann auf **Ein**, **Aus** oder die Standardeinstellung **Autom.** eingerichtet werden. Indirekte Zuordnung zu der Citrix-INI-Dateieinstellung `ZLKeyboardMode=[0|1|2]`, die die Tastatur-Latenz-Reduktion steuert. 0 = Off 1 = Always on 2 = Dynamische Auswahl basierend auf der tatsächlichen Latenz
root/ConnectionType/xen/general/mouseMiddleButtonPaste	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung `MouseSendsControlV=boolean`, wodurch ein Mitteltasten-Emulationsfunktion für Windows-Sitzungsn aktiviert wird. Der Standard lautet **False**. Alle Clients sind standardmäßig auf **0** eingerichtet.
root/ConnectionType/xen/general/noInfoBox	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung `PopupOnExit=boolean`, die bewirkt, dass der Client

Tabelle C-5 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Manager, wfcmgr, beim Benden einer Client-Sitzung eingeblendet wird.
root/ConnectionType/xen/general/printerAutoCreation	Einrichten auf **0**, um die Druckerzuordnung zu deaktivieren.
root/ConnectionType/xen/general/proxyAddress	Die zu verwendende Proxy-Adresse, wenn eine manuelle Proxy-Einstellung über "proxyType" ausgewählt wird.
root/ConnectionType/xen/general/proxyPassword	Das zu verwendende Proxykennwort, wenn eine manuelle Proxy-Einstellung über "proxyType" ausgewählt ist. Dieses Feld wird mithilfe der rc4-Verschlüsselung verschlüsselt.
root/ConnectionType/xen/general/proxyPort	Der zu verwendende Proxy-Anschluss, wenn eine manuelle Proxy-Einstellungen über "proxyType" ausgewählt ist.
root/ConnectionType/xen/general/proxyType	Wählt den Proxytyp aus, der für XenDesktops verwendet werden soll. "Browser-Einstellungen verwenden" wird nur unterstützt, wenn ein lokaler Browser installiert ist.
root/ConnectionType/xen/general/proxyUser	Der Proxy-Benutzer, der zu verwenden ist, wenn eine manuelle Proxy-Einstellung über "proxyType" ausgewählt wird.
root/ConnectionType/xen/general/seamlessWindow	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung `TWIMode=boolean`, die den nahtlosen Modus für veröffentlichte Anwendungen steuert. Alle Clients sind standardmäßig auf **1** eingerichtet.
root/ConnectionType/xen/general/sessionSharingClient	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung`EnableSessionSharingClient=boolean`, die Anfragen zur Sitzungsfreigabe an andere ICA-Sitzungen auf dem gleichen X-Display schickt. Der Standard lautet **False**. Alle Clients sind standardmäßig auf **1** eingerichtet.
root/ConnectionType/xen/general/sound	Können so eingestellt werden, dass die Standardeinstellung **mit hoher Qualität**, **Med Qualität**, **niedriger Qualität**, oder **Deaktiviert**. Qualität indirekt Karten in den Citrix INI-Datei Einstellung `Audiobandwidthlimit= [ 0 | 1 | 2].` 0 = High (Hoch) 1 = Medium (Mittel) 2 = Low (Niedrig)
root/ConnectionType/xen/general/speedScreen	
root/ConnectionType/xen/general/tcpAccel	
root/ConnectionType/xen/general/tcpAddresses/{UUID}/address	
Citrix ConnectionType/xen/general/transparentKeyPassthrough (Xen)	Kann so eingestellt werden, dass er **Übersetzt** (lokal), **Direct in Vollbild Desktops nur** (Fullscreenonly), oder **Direct** (Remote). Indirekt Karten in den Citrix INI-Datei Einstellung `Transparentkeypassthrough=Zeichenfolge`, sodass tastaturkurzbefehl Sequenzen definiert durch die lokalen Windows Manager in der Sitzung. Schlüsselwörter sind lokale, Fernbedienung und Fullscreenonly. Die Standardeinstellung ist FullScreenOnly.
Citrix ConnectionType/xen/general/useAlternateAddress (Xen)	Direkt Karten in den Citrix INI-Datei Einstellung `Usealternateaddress=Boolesche`, das eine alternative-

Tabelle C-5 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Adresse für Firewall Verbindungen. Der Standard lautet **False**. Alle Clients sind standardmäßig auf **0** eingerichtet.
Citrix ConnectionType/xen/general/useBitmapCache (Xen)	Direkt Karten in den Citrix INI-Datei Einstellung `Persistentcacheenabled=Boolesche`. Der Standard lautet **False**. Alle Clients sind standardmäßig auf **0** eingerichtet.
Citrix ConnectionType/xen/general/useEUKS (Xen)	Kontrolliert die Verwendung des Extended Unicode Keyboard Supports auf Windows-Servern: Der Standardwert ist **0**. 0=kein EUKS 1=EUKS verwendet als Ausweichlösung 2=EUKS wann immer möglich verwenden
Citrix ConnectionType/xen/general/useLocalIM (Xen)	Direkt Karten in den Citrix INI-Datei Einstellung `uselocalime=Boolesche`, das die lokale X Eingabemethode zu interpretieren. Das wird nur für europäische Sprachen unterstützt. Der Standardwert ist 0. Alle Clients sind standardmäßig auf **1** eingerichtet.
Citrix ConnectionType/xen/general/waitForNetwork (Xen)	Falls der Wert auf **1** eingerichtet ist, wird die Verbindung nicht gestartet, bis das Netzwerk verfügbar ist. Somit wird sichergestellt, dass auf ein langsames Netzwerk vor, ist die Verbindung wird nicht gestartet, was zu einem Netzwerk verfügbar ist.
Citrix ConnectionType/xen/general/windowHeight (Xen)	Wenn "windowsize" wird so eingestellt, dass **Feste Größe**, diesen Schlüssel verwendet werden, und legen Sie die Höhe des Fensters in Pixel.
Citrix ConnectionType/xen/general/windowPercent (Xen)	Wenn die Option "windowtype" wird so eingestellt, dass **Prozentsatz der Bildschirmgröße**, diesen Schlüssel verwendet werden zur Einstellung der Größe des Fensters hervor. Gültige Werte: 0 bis 100.
root/ConnectionType/xen/general/windowSize	Bei der Einstellung **Full Screen** (Vollbildmodus) wird die Verbindung auf allen verfügbaren Bildschirmen ohne Ränder maximiert. Bei der Einstellung **Percentage of Screen Size** (Prozentsatz der Bildschirmgröße) kann der Schlüssel "windowSizePercentage" dazu verwendet werden, die Größe des Fensters als Prozentsatz bezogen auf den gesamten Bildschirmbereich anzugeben. Bei der Einstellung **Fixed Size** (Feste Größe) können die Schlüssel "'windowSizeWidth" und "windowSizeHeight" dazu verwendet werden, die Größe des Fensters in Pixel anzugeben. Damit "Prozentsatz der Bildschirmgröße" wirksam wird, muss "enableForceDirectConnect" auf **1** und "seamlessWindow" auf **0** festgelegt sein. **HINWEIS:** Diese Einstellung wird nur bei XenApp funktionieren und nur, wenn der Server direkte Verbindungen ermöglicht.
root/ConnectionType/xen/general/windowWidth	Wenn die Option "windowSize" auf "Feste Größe" eingerichtet ist, wird dieser Schlüssel dazu verwendet, die Breite des Fensters in Pixel einzurichten.
root/ConnectionType/xen/gui/fbpanel/autohide	Ob die Taskleiste automatisch ausgeblendet werden soll Richten Sie dies auf "true" ein, um die Taskleiste **automatisch auszublenden**.

Tabelle C-5 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/gui/fbpanel/edge	Die voreingestellte Position in der Taskleiste wenn mehr als ein Desktop oder Anwendung veröffentlicht verfügbar ist.
root/ConnectionType/xen/gui/fbpanel/hidden	Richten Sie dies auf **1** ein, um die Taskleiste vollständig auszublenden. Kann nur ausgeblendet werden, wenn autoStartResource oder autoStartDesktop aktiviert ist.
root/ConnectionType/xen/gui/XenDesktopPanel/disabled	Richten Sie dies auf **1** ein,um den Bereich XenDesktop und seine Taskleiste zu deaktivieren. Normalerweise richten Sie dies auf **1** ein, wenn autoStartResource oder autoStartDesktop aktiviert ist.
root/ConnectionType/xen/gui/XenManager/name	Der Name des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/gui/XenManager/status	Der aktive Status des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/gui/XenManager/title	Der Fenstertitel des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/gui/XenManager/widgets/address	
root/ConnectionType/xen/gui/XenManager/widgets/appInMenu	
root/ConnectionType/xen/gui/XenManager/widgets/appOnDesktop	
root/ConnectionType/xen/gui/XenManager/widgets/autoReconnect	
root/ConnectionType/xen/gui/XenManager/widgets/autostart	
root/ConnectionType/xen/gui/XenManager/widgets/autoStartDesktop	
root/ConnectionType/xen/gui/XenManager/widgets/autoStartResource	
root/ConnectionType/xen/gui/XenManager/widgets/domain	
root/ConnectionType/xen/gui/XenManager/widgets / enablePNADesktopIcons	
root/ConnectionType/xen/gui/XenManager/widgets/enablePNAStartMenuItems	
root/ConnectionType/xen/gui/XenManager/widgets/fallBackConnection	
root/ConnectionType/xen/gui/XenManager/widgets/folder	
root/ConnectionType/xen/gui/XenManager/widgets/hasDesktopIcon	
root/ConnectionType/xen/gui/XenManager/widgets/isInMenu	
root/ConnectionType/xen/gui/XenManager/widgets/label	
root/ConnectionType/xen/gui/XenManager/widgets/password	

Tabelle C-5 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/gui/XenManager/widgets/username	
root/ConnectionType/xen/gui/XenManager/widgets/waitForNetwork	

root > Display

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

Tabelle C-6 root > Display

Registrierungsschlüssel	Beschreibung
root/Display/Configuration/displaymode	Gibt den Anzeigemodus des Geräts an. Ein Wert von **0** kennzeichnet Standardmode (1-4 Monitore), während einen Wert von **1** bedeutet, dass es sich um den 6-Monitormodus handelt. Der HP t610 mit der entsprechenden Add-on-Karte ist die einzige unterstützte Hardware.
root/Display/Configuration/primaryprofile	Diese Einstellung muss immer auf **Standard** eingestellt werden.
root/Display/Configuration/secondarymode	Wenn dies unterstützt wird, wird damit die Position des sekundären Monitors im Verhältnis zum Hauptmonitor angegeben. **0** – Same As **1** – Above **2** – Right of **3** – Left of **4** – Below **5** – None HINWEIS: Dies ist Hardware-abhängig und wird nicht auf allen Modellen unterstützt. Der HP t5535z unterstützt nicht zwei Monitore.
root/Display/Configuration/swapstate	Gibt an, welcher Anschluss den Hauptmonitor enthält. Dies ist Hardware-abhängig und möglicherweise nicht auf allen Modellen implementiert. Im Allgemeinen gilt, dass **0** der Hauptmonitor auf dem VGA-Anschluss ist und **1** der "andere" Anschluss ist.. Für den HP t5565z bedeutet **0**, dass der Hauptmonitor am DVI-I-Anschluss angeschlossen ist und **1**, dass der Hauptmonitor am DVI-D-Anschluss angeschlossen ist. Der HP t5335z unterstützt nicht zwei Monitore.
root/Display/Profiles/{UUID}/colorScaling	Die Farbtemperatur oder direkte RGB-Skalierung für ThinClients mit eingebauten Monitoren. Der Eintrag ist ein sechsstellige Hex-Wert RRGGBB, wobei ffffff auf eine vollständige (100 %) Skalierung auf allen drei farbkanäle hinweisen würde.

Tabelle C-6 root > Display (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Display/Profiles/{UUID}/depth	Die Bit-Tiefe der Anzeige pro Pixel. Eine höhere Farbtiefe bedeutet bessere Qualität, aber mehr Daten und damit geringere Leistung.
root/Display/Profiles/{UUID}/height	Die gewünschte Monitorauflösungsbreite. Einen Wert von **0** bedeutet, dass die Auflösung automatisch erkannt wird.
root/Display/Profiles/{UUID}/label	Profilnamen anzeigen Dies sollte der **Standard** sein.
root/Display/Profiles/{UUID}/orientation	Gibt die Monitorausrichtung an: **0** – Normal **1** – Nach links drehen **2** – Nach rechts drehen **3** – Invertieren
root/Display/Profiles/{UUID}/refresh	Gibt die gewünschte Bildwiederholungsrate an; nicht alle Bildwiederholungsraten werden für alle Auflösungen unterstützt. Die vom Client unterstützten Werte hängen vom Monitor ab. Ein Wert von **0** bedeutet eine automatischen Erkennung der Bildwiederholungsrate. WICHTIG: Wenn eine Wiederholungsrate ausgewählt wird, die nicht von dem mit dem Client verbundenen Monitor unterstützt wird, führt dies zu einem schwarzen Bildschirm. HP empfiehlt, diese Einstellung auf **0** zu belassen.
root/Display/Profiles/{UUID}/width	Die gewünschte Monitorauflösungsbreite. Ein Wert von **0** bedeutet eine automatischen Erkennung der Auflösung

root > Network

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

Tabelle C-7 root > Network

Registrierungsschlüssel	Beschreibung
root/Network/ActiveDirectory/Domain	Active Directory-Domäne.
root/Network/ActiveDirectory/DynamicDNS	Ermöglicht dynamische DNS
root/Network/ActiveDirectory/Enabled	Aktiviert Active Directory.
root/Network/ActiveDirectory/Method	Die Methode, die zur Bereitstellung von Anmeldeinformationen verwendet wird.
root/Network/ActiveDirectory/Password	Benutzerpasswort für Active Directory-Domäne, gilt nur in statischer Methode.
root/Network/ActiveDirectory/Username	Benutzername für Active Directory-Domäne, gilt nur in statischer Methode.
root/Network/DNSServers	Zusätzliche DNS-Server für Domain Name-Auflösung kann hier angegeben werden. Die angegebenen Server werden zusätzlich zu allen über DHCP abgerufenen Server verwendet. Bis zu fünf IPv4- oder IPv6-Adressen können angegeben werden, die durch Kommas getrennt sind.

Tabelle C-7 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/FtpProxy	FTP-Proxy-Adresse.
root/Network/Hostname	Host-Name des Client.
root/Network/HttpProxy	HTTP-Proxy-Adresse.
root/Network/HttpsProxy	HTTPS-Proxy-Adresse.
root/Network/iPeak/Status	Falls der Wert auf **1** eingerichet ist, ist HP Velocity aktiviert. Diese Technologie fügt Redundanz zu TCP-Paketen hinzu und versucht Probleme mit dem Netzwerkverlust zu korrigieren. Auch wenn es aktiviert ist, sollte dies keine Auswirkungen auf die Netzwerk-Paketübertragung haben, wenn de serverseitige Komponente nicht erkannt wird.
root/Network/IPSec/IPSecRules/{UUID}/DstAddr	Zieladresse für die IPsec-Regel.
root/Network/IPSec/IPSecRules/{UUID}/MMAuthMethod	Authentifizierungsmethode für die IPsec-Regel. Geben Sie **PSK** ein,um einen Pre-Shared-Schlüssel zu verwenden und geben Sie **Zertifikat** ein, um Zertifikat-Dateien zu verwenden.
root/Network/IPSec/IPSecRules/{UUID}/ MMAuthMethodCACert	Wenn die Authentifizierungsmethode "Certificate" lautet, wird der Dateipfad für das CA-Zertifikat in diesem Schlüssel gespeichert.
root/Network/IPSec/IPSecRules/{UUID}/ MMAuthMethodClientCert	Wenn die Authentifizierungsmethode "Certificate" lautet, wird der Dateipfad für das Zertifikat in diesem Schlüssel gespeichert.
root/Network/IPSec/IPSecRules/{UUID} / MMAuthMethodPresharedKey	Wenn die Authentifizierungsmethode "PSK" lautet, wird der Wert für den Pre-Shared-Key in diesem Schlüssel gespeichert.
root/Network/IPSec/IPSecRules/{UUID}/ MMAuthMethodPrivateKey	Wenn die Authentifizierungsmethode "Zertifikat" lautet, wird der Pfad der Client-Zertifikatsdatei, der zu der entsprechenden privaten Schlüsseldatei in diesem Schlüssel gespeichert.
root/Network/IPSec/IPSecRules/{UUID}/MMDHGroup	Phase 1 Diffie-Hellman-Gruppe
root/Network/IPSec/IPSecRules/{UUID}/MMEncryptionAlg	Phase 1 Verschlüsselungsalgorithmus.
root/Network/IPSec/IPSecRules/{UUID}/MMIntegrityAlg	Phase 1 Integritätsalgorithmus.
root/Network/IPSec/IPSecRules/{UUID}/MMLifetimeMinutes	Phase 1 Lebensdauer
root/Network/IPSec/IPSecRules/{UUID}/QMAHEnable	Ermöglicht Phase 2 AH.
root/Network/IPSec/IPSecRules/{UUID}/QMAHIntegrityAlg	Phase 2 AH Integritätsaalgorithmus.
root/Network/IPSec/IPSecRules/{UUID}/QMESPEnable	Ermöglicht Phase 2 ESP.
root/Network/IPSec/IPSecRules/{UUID}/ QMESPEncryptionAlg	Phase 2 ESP Verschlüsselungsalgorithmus.
root/Network/IPSec/IPSecRules/{UUID}/QMESPIntegrityAlg	Phase 2 ESP Integritätsalgorithmus.
root/Network/IPSec/IPSecRules/{UUID}/QMLifetimeSeconds	Phase 2 Lebensdauer
root/Network/IPSec/IPSecRules/{UUID}/RuleDescription	Beschreibung für die IPsec Regel ein, wie z. B. den Zweck zum Erstellen der Regel.
root/Network/IPSec/IPSecRules/{UUID}/RuleEnable	Kennzeichen für Regel aktivieren oder deaktivieren. Wenn dies auf **1** eingerichtet ist, wird die Regel aktiviert. Richten Sie auf **0** ein, um die Regel zu deaktivieren.

Tabelle C-7 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/IPSec/IPSecRules/{UUID}/RuleName	Name der IPsec-Regel.
root/Network/IPSec/IPSecRules/{UUID}/SrcAddr	Quell-Adresse für die IPsec Regel.
root/Network/IPSec/IPSecRules/{UUID}/TunnelDstAddr	Tunnel-Zieladresse für die IPsec-Regel.
root/Network/IPSec/IPSecRules/{UUID}/TunnelEnable	Ermöglicht Tunnel-Einstellung für die IPsec-Regel. Wenn diese Option aktiviert ist, lautet die Regel "Anwenden auf Tunnelmodus".
root/Network/IPSec/IPSecRules/{UUID}/TunnelSrcAddr	Tunnel-Quell-Adresse für die IPsec Regel.
root/Network/SearchDomains	Zusätzliche Suchdomänen für die FQDN-Auflösung können hier angegeben werden. Die angegebenen Domänen werden an alle unvollständigen Serverdefinitionen angehängt, um zu versuchen, einen FQDN zu erzeugen, der über DNS aufgelöst werden kann. Ein Beispiel: eine Suchdomäne von "mydomain.com" erlaubt der Serverdefinition "myserver" die korrekte Auflösung für "myserver.mydomain.com", auch wenn der DSN-Server "myserver" nicht in seinen Namensauflösungstabellen hat. Es können bis zu fünf zusätzliche Suchdomänen angegeben werden.
root/Network/VPN/AutoStart	Startet VPN beim Systemstart automatisch.
root/Network/VPN/Domain	VPN-Domäne.
root/Network/VPN/Gateway	VPN-Gateway.
root/Network/VPN/Group	VPN-Gruppe.
root/Network/VPN/GroupPassword	VPN-Gruppenkennwort
root/Network/VPN/Password	VPN-Benutzerkennwort
root/Network/VPN/Type	VPN-Type.
root/Network/VPN/Username	VPN-Benutzername.
root/Network/Wired/DefaultGateway	Das Standard-Gateway, das das Gerät für die Kommunikation mit dem Internet verwendet. In der Regel ist dies die Adresse des Routers. **HINWEIS:** Diese Einstellung wird nur dann wirksam, wenn "Methode" auf "Statisch" eingerichtet ist.
root/Network/Wired/EthernetSpeed	Die Verbindungsgeschwindigkeit der primären Ethernet-Netzwerkschnittstelle. Automatisch erlaubt die Auswahl der schnellsten verfügbaren Verbindungsgeschwindigkeit (in der Regel 1 Gbit/s oder 100 Mbit/s, je nach Switch). Die Verbindungsgeschwindigkeit kann auch auf eine einzige Geschwindigkeit gezwungen werden (100 Mbit/s oder 10 Mbit/s) und zu Duplexmodus (Voll- oder Halbduplex), um Switches oder Hubs zu unterstützen, die keine passende automatische Verhandlung durchführen.
root/Network/Wired/Interface	Die Standard-Ethernet-Schnittstelle oder NIC.
Root/Netzwerk/kabelgebundener/ipaddress	Die IPv4-Adresse des Geräts. Diese Einstellung wird nur dann wirksam, wenn "Methode" auf "Statisch" eingerichtet ist.

Tabelle C-7 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/Wired/IPv6Enable	Richten Sie diesen Schlüssel auf **1** ein, wenn Sie in einer IPv6-Umgebung arbeiten.
root/Network/Wired/Method	Bei der Einstellung **Automatic** wird das Gerät DHCP verwenden und versuchen, die Netzwerkeinstellungen abzurufen. Bei der Einstellung **Static** können "IPAdress", "SubnetMask" und "DefaultGateway" mithilfe der verfügbaren Schlüssel manuell eingerichtet werden. HP rät von der Verwendung von "Static" in einem generischen Client-Profil ab, da dies dazu führt, dass alle Clients die gleiche IP-Adresse erhalten.
root/Network/Wired/Security/CACert	Pfad zu der CA-Zertifizierungsdatei.
root/Network/Wired/Security/Identity	Identität oder anonyme Identität.
root/Network/Wired/Security/InnerAuth	PEAP innere Authentifizierungsprotokolle.
root/Network/Wired/Security/InnerAuthTTLS	TTLS innere Authentifizierungsprotokolle.
root/Network/Wired/Security/Password	Kennwort.
root/Network/Wired/Security/PEAPVersion	PEAP-Version.
root/Network/Wired/Security/PrivateKey	Pfad zu der privaten Schlüsseldatei, nur zur Verwendung bei der TLS-Authentifizierung.
root/Network/Wired/Security/Type	Kabelgebundene 802.1x-Authentifizierungstypen.
root/Network/Wired/Security/UserCert	Pfad zu der Benutzerzertifizierungsdatei, nur zur Verwendung bei der TLS-Authentifizierung.
root/Network/Wired/Security/Username	Benutzername.
root/Network/Wired/SubnetMask	Die Subnetzmaske des Geräts. Zum Beispiel 255.255.255.0 für ein Standard-Subnetz der Klasse C. Diese Einstellung wird nur dann wirksam, wenn "Method" auf "Static" eingerichtet ist.
root/Network/Wireless/DefaultGateway	Das Standard-Gateway, das das Gerät für die Kommunikation mit dem Internet verwendet. In der Regel ist dies die Adresse des Routers. Diese Einstellung wird nur dann wirksam, wenn "Method" auf "Static" eingerichtet ist.
root/Network/Wireless/Interface	Die drahtlose Standardschnittstelle oder der Wireless-Netzwerkadapter.
root/Network/Wireless/IPAddress	Die IPv4-Adresse des Geräts. Diese Einstellung wird nur dann wirksam, wenn "Methode" auf "Statisch" eingerichtet ist.
root/Network/Wireless/IPv6Enable	Richten Sie diesen Schlüssel auf **1** ein, wenn Sie in einer IPv6-Umgebung arbeiten.
root/Network/Wireless/Method	Bei der Einstellung **Automatic** wird das Gerät DHCP verwenden und versuchen, die Netzwerkeinstellungen abzurufen. Bei der Einstellung auf "Static" können "IPAdress", "SubnetMask" und "DefaultGateway" mithilfe der verfügbaren Schlüssel manuell eingerichtet werden. HP rät von der Verwendung von "Static" in einem generischen Client-Profil ab, da dies dazu führt, dass alle Clients die gleiche IP-Adresse erhalten.
root/Network/Wireless/Security/CACert	Pfad zu der CA-Zertifizierungsdatei.

Tabelle C-7 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/Wireless/Security/Identity	Identität oder anonyme Identität.
root/Network/Wireless/Security/InnerAuth	PEAP innere Authentifizierungsprotokolle.
root/Network/Wireless/Security/InnerAuthTTLS	TTLS innere Authentifizierungsprotokolle.
Root/Netzwerk/Wireless/Security/Password	Kennwort.
root/Network/Wireless/Security/PEAPVersion	PEAP-Version.
root/Network/Wireless/Security/PrivateKey	Pfad zu der privaten Schlüsseldatei, nur zur Verwendung bei der TLS-Authentifizierung.
root/Network/Wireless/Security/Type	Drahtlos-Authentifizierungstypen.
root/Network/Wireless/Security/UserCert	Pfad zu der Benutzerzertifizierungsdatei, nur zur Verwendung bei der TLS-Authentifizierung.
root/Network/Wireless/Security/Username	Benutzername.
root/Network/Wireless/Security/WEPAuth	WEP-Authentifizierungstyp.
root/Network/Wireless/Security/WEPIndex	WEP-Kennwortindex, nur für WEP.
root/Network/Wireless/SSID	Die ausgewählte WLAN-Access Point-SSID.
root/Network/Wireless/SSIDHidden	Der ausgeblendete Status der ausgewählten WLAN-Access Point-SSID.
root/Network/Wireless/SubnetMask	Die Subnetzmaske des Geräts. Zum Beispiel 255.255.255.0 (für ein Standard-Subnetz der Klasse C). Diese Einstellung wird nur dann wirksam, wenn "Method" auf "Static" eingerichtet ist.

root > USB

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

Tabelle C-8 root > USB

Registrierungsschlüssel	Beschreibung
root/USB/root/mass-storage/allowed	Falls der Wert auf **1** eingerichtet ist, werden Massenspeichergeräte automatisch bereitgestellt, wenn das Protokoll "local" lautet.
root/USB/root/mass-storage/read-only	Falls der Wert auf **1** eingerichtet ist, werden Massenspeichergeräte schreibgeschützt, wenn sie automatisch lokal bereitgestellt werden.
root/USB/root/protocol	Nachverfolgung der aktuellen Eigentümer des Remote-USB. Wird nur intern verwendet.

root > keyboard

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

Tabelle C-9 root > keyboard

Registrierungsschlüssel	Beschreibung
root/keyboard/enable2	Falls der Wert auf **1** eingerichtet ist, kann die sekundäre Tastatur "layout2" umgestellt werden durch die Tastenkombination, die durch "switch" definiert wurde.
root/keyboard/layout	Das Tastaturlayout definiert, welche Symbole die Tasten generieren. Dies hängt häufig von der jeweiligen Sprache ab. Englisch (en), Spanisch (es), Französisch (fr), Deutsch (de), und Japanisch (jp) sind die häufigsten Layouts.
root/keyboard/layout2	Das sekundäre Tastaturlayout.
root/keyboard/model	Das Tastaturmodell definiert, welche Tasten sich wo auf der Tastatur befinden. Am häufigsten ist der Standard "pc104" oder "pc105" für International. Andere Modelle werden ebenfalls unterstützt.
root/keyboard/model2	Das sekundäre Tastaturmodell.
root/keyboard/numlock	Wenn dies auf die Standardeinstellung **1** gesetzt wird, wird die NUM-Funktion beim Systemstart eingeschaltet. Andernfalls wird die NUM-Led ausgeschaltet.
root/keyboard/rdp_kb	Ein interner Schlüssel, der dazu verwendet wird, das Modell/Layout einer RDP-Tastaturkarte zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/switch	Wird dazu verwendet, die Tastenkombination zum Umschalten zwischen dem ersten und zweiten Layout, zu verwenden, wenn "enable2" gesetzt ist. Gültige Werte sind **grp:ctrl_shift_toggle**, **grp:ctrl_alt_toggle** und **grp:alt_shift_toggle**.
root/keyboard/variant	Die Tastaturvariante definiert leichte Abweichungen im Layout. In der Regel wird die Abweichung **wincompat** verwendet, da sie am nähesten mit den Windows Tastaturlayouts übereinstimmt.
root/keyboard/variant2	Die sekundäre Tastaturvariante.
root/keyboard/XkbLayout	Ein interner Schlüssel, der dazu verwendet wird, das Modell/Layout einem XKB-Tastaturlayout zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/XkbModel	Ein interner Schlüssel, der dazu verwendet wird, das Modell/Layout einem XKB-Tastaturmodell zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.

root > logging

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

Tabelle C-10 root > logging

Registrierungsschlüssel	Beschreibung
root/logging/general/debug	Falls der Wert auf **1** festgelegt ist, ist Debugging auf allen unterstützten Debug-Subsystemen aktiviert. Dies wird gewöhnlich in Verbindung mit "generateDiagnostic.sh" oder mit dem Diagnosetool "Systeminformationen" verwendet, um

Tabelle C-10 root > logging

Registrierungsschlüssel	Beschreibung
	ein Diagnosepaket mit Systemdebugging-Protokollen zu erzeugen.

root > mouse

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

Tabelle C-11 root > mouse

Registrierungsschlüssel	Beschreibung
root/mouse/MouseHandedness	Ob die Maus rechts- oder linkshändig ist. **0 für** Rechtshänder, **1** für Linkshänder.
/Maus/Mousespeed	Die Beschleunigung des Mauszeigers. In der Regel ist eine Zahl von 0-25 der nutzbare Bereich. **0** wird die Beschleunigung vollständig deaktivieren. Dadurch bewegt sich der Mauszeiger ständig langsam, aber messbar.
root/mouse/MouseThreshold	Die Anzahl der Pixel vor Beginn der Beschleunigung ist aktiviert. **0** richet die Beschleunigung auf eine natürliche Kurve ein, die allmählich die Beschleunigung skaliert und damit präzise und zugleich schnelle Bewegungen erlaubt.

root > printer-mapping-mgr

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibung im Ordner **root > printer-mapping-mgr**.

Tabelle C-12 root > printer-mapping-mgr

Registrierungsschlüssel	Beschreibung
root/printer-mapping-mgr/{UUID}/BaudRate	Für serielle Drucker definiert dies die Baudrate des Druckers. Standardmäßig ist dies auf **9600** eingerichtet.
root/printer-mapping-mgr/{UUID}/Port	Ein interner Schlüssel, der zur Identifizierung des Anschlusses verwendet wird. Normalerweise ist er auf das gleiche eingerichtet wie `root/printers/ {UUID} / Port`.

root > printers

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

Tabelle C-13 root > printers

Registrierungsschlüssel	Beschreibung
root/printers/{UUID}/Active	Falls der Wert auf **1** eingerichet ist, wird der Drucker als aktiv markiert und kann zu Remote-Sitzungen umgeleitet werden.

Tabelle C-13 root > printers (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/printers/{UUID}/Port	Der Anschluss für den Drucker. Bei einem lokalen Drucker ist dies häufig /dev/ttyS0, /dev/lp0 oder /dev/ttyUSB0. Wenn ein Netzwerkdrucker definiert ist, wird dieser auf **Netzwerk** eingerichtet und ein Schlüssel "ServerIP" wird mit der IP-Adresse des Druckers definiert.
root/printers/{UUID}/PrinterMDL	Auf das Druckermodell eingerichtet. Dies ist ein Textfeld, das zur Ermittlung des Druckers in lokalen und Remote-Sitzungen verwendet wird.
root/printers/{UUID}/WindowsDriver	Auf das genaue Windows Treiber-Modell eingerichtet. Dies wird von der RDP- und Citrix-Druckerzuordnung verwendet, um zu ermitteln, welcher Druckertreiber auf dem Remote-Host zu installieren ist.

root > screensaver

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

Tabelle C-14 root > screensaver

Registrierungsschlüssel	Beschreibung
root/screensaver/enableDPMS	Richten Sie dies auf **0** ein, um die Monitor-Energieverwaltung zu deaktivieren. Das führt dazu, dass der Monitor eingeschaltet bleibt, es sei denn, er wird manuell ausgeschaltet.
root/screensaver/off	Zeitüberschreitung-Verzögerung zum Ausschalten des Monitors (in Minuten).
root/screensaver/standby	Zeitüberschreitung-Zeitverzögerung, um den Monitor in den Energiesparmodus zu bringen (in Minuten).
root/screensaver/suspend	Zeitüberschreitung-Zeitverzögerung, um den Monitor in den Bereitschaftsstatus zu bringen (in Minuten).

root > time

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

Tabelle C-15 root > time

Registrierungsschlüssel	Beschreibung
root/time/NTPServers	Eine durch Kommata getrennte Liste mit zu verwendenden NTP-Servern. Private NTP-Server oder große virtuelle NTP-Cluster wie "pool.ntp.org" sind die beste Auswahl, um die Serverlast zu minimieren. Löschen Sie dieses Feld, um wieder zur Verwendung von DHCP-Servern (Tag 42) zurückzukehren anstelle einer festen Liste.
root/time/timezone	Wird verwendet, um die Zeitzone manuell einzugeben. Zeitzonen sollten im folgenden Format angegeben werden: "[region]/[subregion]", wie von "Linux Zeitzone" definiert: Im

Tabelle C-15 root > time (Fortsetzung)

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

root > translation

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

Tabelle C-16 root > translation

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

root > users

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

Tabelle C-17 root > users

Registrierungsschlüssel	Beschreibung
root/users/root/password	Das Kennwort für den Administratormodus. Falls dieses Feld leer ist, ist der Administratormodus gesperrt. Der Administratormodus bietet Zugriff auf alle Elemente des Bedienfelds.
root/users/user/apps/hptc-auto-update/authorized	Falls der Wert auf **0** eingerichtet ist, sind Benutzer nicht in der Lage,auf die Automatic Update-Servereinstellungen zuzugreifen. Die Standardkonfiguration ist deaktiviert, weil Clients ihre Automatic Update Server-URL per Broadcast oder DHCP-Kenning erhalten.
root/users/user/apps/hptc-cert-mgr/authorized	Falls der Wert auf **0** eingerichtet ist, sind Benutzer nicht in der Lage auf die Einstellungen des Zertifikat-Managers zuzugreifen. Dies kann hilfreich in einer Nur-DHCP-Umgebung sein. Hier werden alle Einstellungen des Zertifikat-Managers über den DHCP-Server an die Clients weitergeben.
root/users/user/apps/hptc-color-temp/t410aio/authorized	Falls der Wert auf **0** eingerichtet ist, sind Benutzer nicht in der Lage, die Farbtemperatur des Bildschirms zu ändern.
Root/Benutzer/Benutzer/Apps/hptc-date-Mgr/autorisiert	Falls der Wert auf **0** eingerichtet ist, sind Benutzer nicht in der Lage, auf die lokalen Datums- und Uhrzeiteinstellungen des Client zuzugreifen. Dies kann hilfreich sein in einer Umgebung, in der das Datum und die Uhrzeit des Client von NTP eingerichtet werden.
root/users/user/apps/hptc-display-prefs/authorized	Falls der Wert auf **0** eingerichtet ist, sind Benutzer nicht in der Lage.die Auflösung, Bit-Tiefe oder Wiederholungsrate eines Bildschirms zu ändern.
root/users/user/apps/hptc-display-prefs/t410aio/authorized	Falls der Wert auf **0** eingerichtet ist, sind Benutzer nicht in der Lage, die Auflösung, Bit-Tiefe oder Wiederholungsfrequenz eines Bildschirms zu ändern.
root/users/user/apps/hptc-i18n-mgr/authorized	Falls der Wert auf **1** eingerichtet ist, ist das Bedienfeld für die Elemente der Gebietsschemen für Benutzer aktiviert. Dies ist normalerweise deaktiviert, weil eine direkte Steuerung über `root/zero-login/controls` vorhanden ist.
root/users/user/apps/hptc-keyboard-layout/authorized	Falls der Wert auf **1** eingerichtet ist, ist das Element des Bedienfelds für das vollständige Tastatur-Layout für Benutzer aktiviert. Dies ist normalerweise deaktiviert, weil eine direkte Steuerung über `root/zero-login/controls` vorhanden ist.
root/users/user/apps/hptc-mixer/authorized	Falls der Wert auf **0** eingerichtet ist, ist das Bedienfeld für den Mixer in voller Größe für Benutzer deaktiviert. Es ist normalerweise überflüssig, weil die Ministeuerung die gleichen Funktionen abdeckt. Um die Lautstärkeregelung vollständig zu deaktivieren, muss `root/zero-login/controls/audio/authorized` auch auf **0** eingerichtet sein.
root/users/user/apps/hptc-mouse/authorized	Falls der Wert auf **0** eingerichtet ist, sind Benutzer nicht in der Lage, die lokalen Client-Mauseinstellungen zu ändern.

Tabelle C-17 root > users (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Benutzer können jedoch die Mauseinstellungen jederzeit über die Remote-Host-Einstellungen ändern.
root/users/user/apps/hptc-network-mgr/authorized	Falls der Wert auf **0** eingerichtet ist, sind Benutzer nicht in der Lage, auf Netzwerkeinstellungen zuzugreifen. Dies kann in einer Nur-DHCP-Umgebung hilfreich sein, in der alle Netzwerkeinstellungen vom DHCP-Server an die Clients übergeben werden.
root/users/user/apps/hptc-printer-mapping-mgr/authorized	Falls der Wert auf **0** eingerichtet ist, sind Benutzer nicht in der Lage, die Windows Treiber-Werte für lokal angeschlossene Drucker einzurichten. Dies könnte dazu führen, dass manche Drucker nicht korrekt zu Remote-Sitzungen zuordnen können. Diese Einstellung hat keine Auswirkungen auf die USB-Umleitung.
root/users/user/apps/hptc-printer-mgr/authorized	Falls der Wert auf **0** eingerichtet ist, sind Benutzer nicht in der Lage, die Windows Treiber-Werte für über CUPS angeschlossene Drucker einzurichten. Dies könnte dazu führen, dass manche Drucker nicht korrekt zu Remote-Sitzungen zuordnen können. Diese Einstellung hat keine Auswirkungen auf die USB-Umleitung.
root/users/user/apps/hptc-profile-mgr/authorized	Wenn **0** eingerichtet ist, sind Benutzer nicht in der Lage, den Client auf die Werkseinstellungen zurückzusetzen. Die einzige Möglichkeit, ein Gerät auf die Werkseinstellungen zurückzusetzen, wenn diese Steuerung deaktiviert ist, ist das Aktualisieren des Client mit einer neuen Konfiguration, bei der diese Steuerung aktiviert ist, oder das Zurücksetzen des Werks-Image über einen USB-Schlüssel.
root/users/user/apps/hptc-root-xterm/authorized	Falls der Wert auf **1** eingerichtet ist, wird das Element Stammverzeichnis-X-Terminal im Bedienfeld für den Benutzer aktiviert. **ACHTUNG:** Den Zugriff auf das Stammverzeichnis-Terminal zu aktivieren ist ein Sicherheitsrisiko und wird für eine Produktionsumgebung nicht empfohlen. Das Stammverzeichnis-Terminal sollte nur zur Verwendung in einer geschützten, nicht produktiven Umgebung aktiviert werden.
root/users/user/apps/hptc-shortcut-mgr/authorized	Falls der Wert auf **1** eingerichtet ist, wird das Element Verknüpfungsmanager für Benutzer aktiviert.
root/users/user/apps/hptc-switch-admin/authorized	Falls der Wert auf **1** eingerichtet ist, wird Wechsel zwischen Administrator-/Benutzermodus für Benutzer aktiviert.
root/users/user/apps/hptc-vncshadow/authorized	Falls der Wert auf **1** eingerichtet ist, wird das Element VNC Shadowing im Bedienfeld für Benutzer aktiviert.
root/users/user/apps/scim-setup/authorized	Falls der Wert auf **1** eingerichtet ist, wird das Element SCIM (Eingabemethode) im Bedienfeld für den Benutzer aktiviert. **HINWEIS:** SCIM wird für die Eingabe lokaler asiatischer Sprachen verwendet und ist auf Ihrem Server möglicherweise ohne die Installation eines asiatischen Sprachkits nicht vorhanden.
root/users/user/AutoBrightEnabled	Richten Sie dies auf **1** ein, um die automatische Helligkeitskonfiguration auf dem HP t410 All-in-one zu aktivieren, wenn der Modus "Power over Ethernet" ist. Diese Funktion versucht, die Helligkeit zu senken, wenn der

Tabelle C-17 root > users (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Stromverbrauch einen kritischen Grenzwert überschreitet, um zu verhindern, dass der Ethernet-Switch den Strom zum Gerät abschaltet.
root/users/user/MaxPowerDetectEnabled	Richten Sie dies auf **1** ein, um den Algorithmus zur Erkennung der maximalen Leistung auf dem HP t410 All-in-one zu aktivieren, wenn der Modus "Power over Ethernet" ist.. Diese Funktion versucht, die tatsächliche maximale Leistung zu ermitteln, die vom Ethernet-Switch bezogen werden kann. Kürzere Ethernet-Kabel bieten höhere maximale Leistung.
root/users/user/OnDemandCPUThrottleEnabled	Richten Sie dies auf **1** ein, um das On-Demand-Throttling auf dem HP t410 Alli-in-one zu aktivieren, wenn der Modus "Power over Ethernet" ist. Diese Funktion senkt die CPU-Frequenz, wenn der Energieverbrauch einen kritischen Grenzwert überschreitet, um zu verhindern, das der Ethernet-Switch den Strom zum Gerät unterbricht.
root/users/user/WOLEnabled	Richten Sie dies auf **0** ein, um Wake On LAN zu deaktivieren.

root > zero-login

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

Tabelle C-18 root > zero-login

Registrierungsschlüssel	Beschreibung
root/zerologin/buttons/configure/authorized	Aktiviert bzw. deaktiviert das Konfigurationsmenü. Falls der Wert auf **0** eingerichtet ist, sind Benutzer nicht in der Lage, irgendwelche Geräteeinstellungen zu konfigurieren.
root/zero-login/buttons/info/authorized	Aktiviert oder deaktiviert den Bereich Systeminformationen. Falls der Wert auf **0** eingerichtet ist, sind Benutzer nicht in der Lage, irgendwelche Informationen über das System zu sehen.
root/zerologin/buttons/shutdown/authorized	Aktiviert oder deaktiviert die Taste Herunterfahren auf dem Anmeldebildschirm. Falls der Wert auf **0** eingerichtet ist, können die Benutzer das Gerät nur ausschalten, indem Sie die Betriebstaste drücken.
root/zero-login/controls/audio/authorized	Falls der Wert auf **0** eingerichtet ist, können die Benutzer die Lautstärke der Soundausgabe nicht ändern. Dies kann hilfreich sein in einer Umgebung, bei der jeglicher Sound stummgeschaltet oder auf eine bestimmte Lautstärke eingestellt sein soll. Um Benutzer vollständig daran zu hindern, die Soundausgabestufen zu ändern, stellen Sie sicher, dass `root/users/user/apps/hptc-mixer/authorizations` ebenfalls auf **0** eingerichtet ist.
root/zerologin/controls/connection/authorized	Falls der Wert auf **0** eingerichtet ist, können Benutzer den Verbindungstyp nicht neu definieren. Dies ist standardmäßig deaktiviert, da es normalerweise nicht wünschenswert ist, Benutzern zu erlauben, in einer Produktionsumgebung den Verbindungstyp zu ändern.

Tabelle C-18 root > zero-login (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/zero-login/controls/i18n/authorized	Falls der Wert auf **0** eingerichtet ist, können Benutzer das Gebietsschema nicht ändern. Dies ist nützlich in einer Umgebung mit nur einer Sprache.
root/zero-login/controls/keyboard/authorized	Falls der Wert auf **0** eingerichtet ist, können Benutzer das Tastaturlayout nicht ändern. Dies ist nützlich in einer Umgebung mit nur einer Sprache.
root/zero-login/defaultCredentials/domain	Falls dies eingerichtet ist, wird dieser Domänenname als Standard für diesen Anmeldedialog bereitgestellt, falls über "RememberMe" keine Alternative gespeichert wurde. Dies ist nützlich in Umgebungen, in denen hauptsächlich ein einziger Domänenname verwendet wird.
root/zero-login/defaultCredentials/domainList	Durch Semikolon getrennte Liste von Domänen; siehe beispielsweise `domain1:domain2:(…)`. Diese Domänen werden in einem Menü auf dem Anmeldebildschirm zur Verfügung gestellt. Eine bestimmte Domäne kann vorab ausgewählt werden, indem sie unter `root/zero-login/defaultCredentials/domain registry key` eingerichtet wird.
root/zerologin/defaultCredentials/password	Falls es eingerichtet wird, wird dieses Kennwort als Standard für den Anmeldedialog bereitgestellt, wenn die Standards der Benutzer und der Domäne hier übereinstimmen. In der Regel wird dies mit Verbindungen mit automatischem Start verwendet.
root/zerologin/defaultCredentials/readOnly	Falls der Wert auf **1** eingerichtet ist, sind Anmeldebenutzername, Kennwort und Domäne schreibgeschützte Felder. Dies ist nur nützlich für Verbindungen mit automatischem Start und automatischer Neuverbindung.
root/zerologin/defaultCredentials /rememberMe	Falls der Wert auf **1** eingerichtet ist, werden der Benutzername und die Domäne, die für eine Verbindung verwendet wurden, als Standard gespeichert, der bei der nächsten Anmeldung im Anmeldedialog angezeigt wird. Für die meisten Verbindungstypen kann der Benutzer diesen Wert mithilfe des Kontrollkästchens "RememberMe" umschalten.
root/zerologin/defaultCredentials /smartcard	Wird als Standardeinstellung im Anmeldedialog bereitgestellt, wenn die Standards des Benutzers und der Domäne hier übereinstimmen. Wird in der Regel bei Verbindungen mit automatischem Start verwendet.
root/zerologin/defaultCredentials /username	Falls dies eingerichtet ist, wird dieser Benutzername als Standard im Anmeldefenster bereitgestellt, falls über "RememberMe" keine Alternative gespeichert wurde. Wird in der Regel bei Verbindungen mit automatischem Start verwendet.
root/zero-login/styledir/default	Das Verzeichnis, in dem die Dateien für den Standardstil (.qss) und Hintergrund (.rtf) gespeichert sind.
root/zero-login/styledir/rdesktop	Das Verzeichnis, in dem die Dateien für den Standardstil (.qss) und Hintergrund (.rtf) zur Verwendung mit rdesktop-Verbindungen gespeichert sind.

Tabelle C-18 root > zero-login (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/zero-login/styledir/view	Das Verzeichnis, in dem die Dateien für den Standardstil (.qss) und Hintergrund (.rtf) zur Verwendung mit VMware Horizon View Verbindungen gespeichert sind.
root/zero-login/styledir/xen	Das Verzeichnis, in dem die Dateien für den Standardstil (.qss) und Hintergrund (.rtf) zur Verwendung mit Citrix XenDeskto-Verbindungen gespeichert sind.

D VMware Horizon View-USB-Konfiguration

Dieser Anhang umfasst die folgenden Themen:

- USB-Optionen in vorhergehenden-Releases
- VMware Horizon View-USB-Gerätefamilien

USB-Optionen in vorhergehenden-Releases

So deaktivieren Sie USBR auf Audiogeräten:

1. Ändern Sie in der Client-Registrierung den Eintrag `/etc/vmware/config`.
2. Fügen Sie die folgende Zeile hinzu:

   ```
   viewusb.ExcludeFamily = "audio-in;audio-out;"
   ```

So schließen Sie ein bestimmtes Gerät aus oder ein:

1. Rufen Sie die VID und PID des Geräts ab.
2. Ändern Sie in der Client-Registrierung den Eintrag `/etc/vmware/config`.
3. Fügen Sie die entsprechende Zeile hinzu:
   - `Viewusb.ExcludeVidPid = "vid-0f0_pid-0001;vid-**21_pid-*8*a;"`
   - `Viewusb.IncludeVidPid = "vid-003a_pid-1234"`

HINWEIS: Die Informationen in diesem Abschnitt gelten nicht für eine Teradici-beschleunigte t410-Einheit. Zur Steuerung von USBR auf dieser Einheit, führen Sie ein Upgrade auf HP Smart Zero Core 4.3 oder höher durch, das eine eingebaute USB-Manager-GUI enthält.

HINWEIS: Weitere Informationen zu einer VMware Horizon View-USB-Konfiguration finden Sie unter *Verwendung des VMware Horizon View Client für Linux* unter http://www.vmware.com.

VMware Horizon View-USB-Gerätefamilien

Tabelle D-1 VMware Horizon View-USB-Gerätefamilien

Familie	Familienname
Vendor (Anbieter)	vendor
Unknown (Unbekannt)	unknown
Other (Sonstiges)	other
Audio In (Audioeingang)	audio-in
Audio Out (Audioausgang)	audio-out
Communications (Kommunikation)	comm
Human Interface Device (Schnittstelle für die Benutzerinteraktion)	hid
Bootable HID (Bootfähige HID)	hid-bootable

Tabelle D-1 VMware Horizon View-USB-Gerätefamilien (Fortsetzung)

Familie	Familienname
Force Feedback Device (Gerät zum Erzwingen von Feedback)	physical
Imaging	imaging
Printer (Drucker)	printer
Mass Storage (Massenspeicher)	storage
Smardcard Reader (Smart Card-Lesegerät)	smart-card
Security (Sicherheit)	security
Video	video
Wireless Adapter (Wireless-Adapter)	wireless
Bluetooth	bluetooth
Wireless USB (Wireless-USB)	wusb
PDA (Handheld)	Pda

Index

A
Administratormodus
  Bedienfeld, verwenden 12
  wechseln zum Benutzermodus 12
Aktualisieren von Clients
  Aktualisierung mit DHCP-Kennung 47
  Aktualisierung per Übertragung 47
Audioumleitung
  RDP 20
  VMware Horizon View 26
Automatic Intelligence
  verwenden 46

B
Benutzermodus
  Bedienfeld, verwenden 10
  Wechsel zu Administratormodus 11

C
Citrix
  HDX MediaStream 23
  Supportmatrix 23
  Übersicht 21
Client-Anmeldebildschirm
  benutzerdefiniert 53
Client-Bedienfeld
  verwenden im Administratormodus 12
  verwenden in Benutzermodus 10
  zugreifen 10
Client-Informationsbildschirme
  ausblenden 9
  verwenden 6
Client-Profil
  bearbeiten 40
  Dateien hinzufügen 42
  laden 40
  Registrierungseinstellungen 41
  speichern 44
  Symbolischen Link hinzufügen 43
  Zertifikate 42
Clients
  aktualisieren. *Siehe* Aktualisieren von Clients
  Fehlerbeseitigung 34
  konfigurieren 10
  navigieren 5
  Tastatursprache 51
Clients aktualisieren
  DNS Alias Update 48
  manuelle Aktualisierung 48
Client-Symbolleiste
  verwenden 5

D
Desktop
  Kürzel 4
  Verwenden 4
Druckerkonfiguration 44
Druckerumleitung
  RDP 19
  VMware Horizon View 26
Druckerzuordnung 32

E
Einführung 3
Einstellungen, Administrator
  Audio 13
  automatisches Update 15
  Datum und Zeit 14
  Druckerzuordnung 14
  Einstellungen anzeigen 13
  Maus 13
  Netzwerk 14
  Sicherheit 15
  Sound 14
  Sprache 14
  Task-Manager 16
  Tastaturlayout 13
  Tastenkombinationen 16
  Textbearbeitung 16
  USB 14
  X-Terminal 16
  Zertifikate 15
  Zurücksetzen auf Werkseinstellungen 15
Einstellungen, Benutzer
  Audio 11
  Datum und Zeit 11
  Druckerzuordnung 12
  Einstellungen anzeigen 11
  Maus 11
  Netzwerk 11
  Sprache 11
  Tastaturlayout 11
Einstellungen, VNC-Shadowing
  Zurücksetzen auf Werkseinstellungen 15

F
Fehlerbeseitigung
  Druckerkonfiguration 35
  Firmware-Beschädigung 35
  Netzwerkverbindung 34
  verwenden der Systemdiagnose 36

G
Geräteumleitung
  RDP 18
  VMware Horizon View 25

H
HDX MediaStream 23
HP Device Manager 50
HP Intelligent Delivery-Dienst 49
HP Smart Zero Client Services
  installieren 39
  Profile Editor. *Siehe* Profile Editor
  Übersicht 38
  unterstützte Betriebssysteme 38

K
Kioskmodus
  RDP 16
  VMware Horizon View 24
Konfiguration eines parallelen Druckers 44
Konfiguration eines seriellen Druckers 44

M

Massenspeicherumleitung
- RDP 19
- VMware Horizon View 26

MMR
- RDP 17
- VMware Horizon View 25

Multimedia Redirection. *Siehe* MMR

P

Profile Editor
- verwenden 40

R

RDP
- Audioumleitung 20
- Druckerumleitung 19
- Experience-Optionen 21
- Geräteumleitung 18
- Kioskmodus 16
- Massenspeicherumleitung 19
- MMR 17
- Multi-Monitor-Sitzungen 18
- RFX 17
- Smart Card-Umleitung 20
- Übersicht 16
- USB-Umleitung 18

Registrierungseinstellungen 64

Remotefx. *Siehe* RFX

RFX 17

S

Smart Card-Umleitung
- RDP 20
- VMware Horizon View 27

Symbol Systemstatus 5

Systemdiagnose 36

U

USB-Umleitung
- RDP 18
- USB-Manager 32
- VMware Horizon View 25

V

Verbindungen
- auswählen 3, 10
- konfigurieren 3
- Standard bearbeotem 12
- Standard-Typen 3

Virtual Network Computing. *Siehe* VNC

VMware Horizon View
- Audioumleitung 26
- Command Line Arguments (Befehlszeilenargumente) 29
- Druckerumleitung 26
- Geräteumleitung 25
- Kioskmodus 24
- Massenspeicherumleitung 26
- MMR 25
- Multi-Monitor-Sitzungen 25
- Protokolle ändern 30
- Sicherheitsstufen 31
- Smart Card-Umleitung 27
- Tastaturbefehle 25
- Teradici-beschleunigt 29
- Übersicht 24
- USB-Konfiguration 102
- USB-Umleitung 25
- Verbindungsoptionen 28
- Webcamumleitung 28
- Zertifikate 31

VNC-Shadowing 15

W

Webcamumleitung
- VMware Horizon View 28

Z

Zertifikate
- installieren 30
- VMware Horizon View 31