VMware Horizon Client für Windows Installations- und Einrichtungshandbuch

VMware Horizon Client for Windows 2012

vmware®

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

https://docs.vmware.com/de/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Inhalt

VMware Horizon Client für Windows Installations- und Einrichtungshandbuch

Dieses Handbuch beschreibt die Installation, Konfiguration und Verwendung der VMware Horizon® Client™-Software auf einem Microsoft Windows-Clientsystem.

Diese Informationen sind für Administratoren bestimmt, die eine Bereitstellung von Horizon mit Microsoft Windows-Clientsystemen einrichten müssen, z. B. für Desktops und Laptops. Diese Informationen sind für erfahrene Windows-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und Vorgängen in Datencentern vertraut sind.

Wenn Sie Endbenutzer sind, finden Sie die für Sie relevanten Informationen im Dokument *VMware Horizon Client für Windows Benutzerhandbuch* oder in der Onlinehilfe für Horizon Client für Windows.

Systemanforderungen und Setup von Windows-basierten Clients

1

Systeme, auf denen Horizon Client-Komponenten ausgeführt werden, müssen bestimmte Hardware- und Softwareanforderungen erfüllen.

Auf Windows-Systemen verwendet Horizon Client zum Herstellen einer Verbindung mit einem Server die Interneteinstellungen von Microsoft Internet Explorer (einschließlich Proxy-Einstellungen). Stellen Sie sicher, dass die richtigen Internet Explorer-Einstellungen festgelegt sind und dass Sie über Internet Explorer auf die Server-URL zugreifen können.

Dieses Kapitel enthält die folgenden Themen:

Systemanforderungen für Windows-Clientsysteme

Sie können Horizon Client für Windows auf PCs und Laptops installieren, auf denen ein unterstütztes Microsoft Windows-Betriebssystem ausgeführt wird.

Sowohl die PCs oder Laptops, auf denen Sie Horizon Client installieren, als auch die verwendeten Peripheriegeräte müssen bestimmte Systemanforderungen erfüllen.

Modelle

Alle x86- oder x86-64-Windows-Geräte

Arbeitsspeicher

Mindestens 1GB RAM

Betriebssysteme

Horizon Client unterstützt die folgenden Betriebssysteme.

Betriebssystem	Version	Service Pack oder Wartungsoption	Unterstützte Editionen
Windows 10	32-Bit oder 64-Bit	Version 2009 SAC Version 2004 SAC Version 1909 SAC Enterprise 2019 LTSC Enterprise 2016 LTSC	Home, Pro, Pro für Workstations, Enterprise, Internet of Things (Internet der Dinge, IoT), Enterprise und Education
Windows Server 2012 R2	64 Bit	Letztes Update	Standard und Datacenter
Windows Server 2016	64 Bit	Letztes Update	Standard und Datacenter
Windows Server 2019	64 Bit	Letztes Update	Standard und Datacenter

Windows Server 2012 R2, Windows Server 2016 und Windows Server 2019 werden für die Ausführung von Horizon Client im geschachtelten Modus unterstützt. Informationen zu den Funktionen, die im geschachtelten Modus unterstützt werden, finden Sie in VMware-Knowledgebase-Artikel 67248.

Wichtig Mitunter werden neue Windows-Betriebssysteme unterstützt, nachdem dieses Dokument veröffentlicht wurde. Die aktuellsten Informationen zu den unterstützten Betriebssystemen finden Sie im VMware Knowledgebase (KB)-Artikel 58096.

Verbindungsserver und Horizon Agent

Die aktuelle Wartungsversion von Horizon 7 Version 7.5 und spätere Versionen.

Wenn Clientsysteme von außerhalb der firmeneigenen Firewall eine Verbindung herstellen, verwenden Sie eine Unified Access Gateway-Appliance, damit Clientsysteme keine VPN-Verbindung benötigen. Wenn Ihr Unternehmen ein internes WLAN besitzt, das über einen Router den Zugriff auf Remote-Desktops für Geräte ermöglicht, müssen Sie keine VPN-Verbindung und auch nicht Unified Access Gateway einrichten.

Anzeigeprotokolle

- PCoIP
- VMware Blast
- RDP

Netzwerkprotokolle

- IPv4
- IPv6

Bei einer benutzerdefinierten Installation von Horizon Client können Sie die automatische Auswahl des Internetprotokolls aktivieren. Weitere Informationen finden Sie unter Aktivieren der automatischen Auswahl des Internetprotokolls. Informationen zur Verwendung von Horizon in einer IPv6-Umgebung finden Sie im Dokument *Horizon-Installation*.

Hardwareanforderungen für PCoIP und VMware Blast

- x86-basierter Prozessor mit SSE2-Erweiterungen, mit einer Prozessorgeschwindigkeit von mindestens 800 MHz.
- Verfügbarer RAM über den Systemanforderungen zur Unterstützung verschiedener Monitorkonfigurationen. Im Allgemeinen gilt die folgende Formel.

  ```
  20MB + (24 * (# monitors) * (monitor width) * (monitor height))
  ```

  Im Allgemeinen können Sie die folgenden Berechnungen verwenden.

  ```
  1 monitor: 1600 x 1200: 64MB
  2 monitors: 1600 x 1200: 128MB
  3 monitors: 1600 x 1200: 256MB
  ```

Hardwareanforderungen für RDP

- x86-basierter Prozessor mit SSE2-Erweiterungen, mit einer Prozessorgeschwindigkeit von mindestens 800 MHz.
- 128 MB RAM.

Softwareanforderungen für RDP

- Für Windows 10 ist RDP 10.0 zu verwenden.
- Das Agent-Installationsprogramm konfiguriert die lokale Firewall-Regel für eingehende RDP-Verbindungen entsprechend dem aktuellen RDP-Port des Hostbetriebssystems (üblicherweise 3389). Wenn Sie die RDP-Portnummer ändern, müssen Sie auch die dazugehörigen Firewall-Regeln ändern.

Die RDC-Versionen stehen im Microsoft Download Center zum Download zur Verfügung.

Video- und Grafikvoraussetzungen

- Grafikkarte, die Direct3D 11 Video unterstützt.
- Aktuelle Video- und Grafikkartentreiber.

.NET Framework-Anforderungen

Das Installationsprogramm von Horizon Client erfordert .NET Framework Version 4.5 oder höher. Das Installationsprogramm überprüft vor der Installation, ob .NET Framework Version 4.5 oder höher installiert ist. Wenn der Clientcomputer diese Voraussetzung nicht erfüllt, lädt das Installationsprogramm automatisch die neueste Version von .NET Framework herunter.

Systemanforderungen für Horizon Client-Funktionen

Für Horizon Client-Funktionen müssen bestimmte Anforderungen an Hardware und Software erfüllt sein.

Anforderungen für die Smartcard-Authentifizierung

Clientgeräte, die eine Smartcard für die Benutzerauthentifizierung verwenden, müssen bestimmte Anforderungen erfüllen.

Hardware- und Softwareanforderungen an den Client

Für jedes Clientgerät, das zur Benutzerauthentifizierung eine Smartcard verwendet, gelten die folgenden Hardware- und Softwareanforderungen.

- Horizon Client
- Ein kompatibler Smartcard-Leser

  Horizon Client unterstützt Smartcards und Smartcard-Leser, die einen PKCS#11- oder Microsoft CryptoAPI-Anbieter verwenden. Optional können Sie das ActivClient-Softwarepaket von ActivIdentity installieren, das Tools zur Interaktion mit Smartcards bereitstellt.
- Produktspezifische Anwendungstreiber

Benutzer, die sich mithilfe von Smartcards authentifizieren, müssen über ein Smartcard- oder USB-Smartcard-Token verfügen, und jede Smartcard muss ein Benutzerzertifikat enthalten.

Verwenden Sie als Kryptografiedienstanbieter (Cryptographic Service Provider, CSP) in der Vorlage für die Ausstellung von Zertifikaten den Microsoft Base Smart Card Crypto Provider oder einen externen Smartcard-CSP, der RSA mit SHA-256-Algorithmen unterstützt.

Anforderungen für die Smartcard-Registrierung

Zum Installieren von Zertifikaten auf einer Smartcard muss Ihr Administrator einen Computer einrichten, der als Registrierungsstelle fungiert. Dieser Computer muss Smartcard-Zertifikate für Benutzer ausgeben können und Mitglied der Domäne sein, für die Sie Zertifikate ausgeben.

Wenn Sie eine Smartcard registrieren, können Sie die Schlüsselgröße des resultierenden Zertifikats auswählen. Zur Verwendung von Smartcards auf lokalen Desktops müssen Sie bei der Smartcard-Registrierung eine Schlüsselgröße von 1024 Bit oder 2048 Bit auswählen. Zertifikate mit 512-Bit-Schlüsseln werden nicht unterstützt.

Die Microsoft TechNet-Website enthält ausführliche Informationen zur Planung und Implementierung der Smartcard-Authentifizierung für Windows-Systeme.

Softwareanforderungen für Remote-Desktops und veröffentlichte Anwendungen

Ein Horizon-Administrator muss auf den virtuellen Desktops oder RDS-Hosts produktspezifische Anwendungstreiber installieren.

Aktivieren das Textfeldes „Benutzernamenhinweis“ in Horizon Client

In einigen Umgebungen können Smartcard-Benutzer ein einziges Smartcard-Zertifikat zur Authentifizierung bei mehreren Benutzerkonten verwenden. Benutzer geben ihren Benutzernamen in das Textfeld **Benutzernamenhinweis** ein, wenn Sie sich über eine Smartcard anmelden.

Damit das Feld **Benutzernamenhinweis** im Anmeldungsdialogfeld von Horizon Client angezeigt wird, müssen Sie die Funktion für den Smartcard-Benutzernamenhinweis im Verbindungsserver aktivieren. Informationen zur Aktivierung von Smartcard-Benutzernamenhinweisen erhalten Sie im Dokument *Horizon-Verwaltung*.

Wenn Ihre Umgebung für den sicheren externen Zugriff eine Unified Access Gateway-Appliance verwendet, müssen Sie die Unified Access Gateway-Appliance zur Unterstützung von Smartcard-Benutzernamenhinweisen konfigurieren. Die Funktion für Smartcard-Benutzernamenhinweise wird nur mit Unified Access Gateway 2.7.2 und höher unterstützt. Informationen zur Aktivierung von Smartcard-Benutzernamenhinweisen in Unified Access Gateway erhalten Sie im Dokument *Bereitstellen und Konfigurieren von VMware Unified Access Gateway*.

Horizon Client unterstützt weiterhin Smartcard-Zertifikate für Einzelkonten, wenn die Funktion für Smartcard-Benutzernamenhinweise aktiviert ist.

Zusätzliche Anforderungen für die Smartcard-Authentifizierung

Neben der Einhaltung der Smartcard-Anforderungen für Horizon Client-Systeme müssen andere Horizon-Komponenten zur Unterstützung von Smartcards bestimmte Anforderungen an die Konfiguration erfüllen.

Verbindungsserver- und Sicherheitsserver-Hosts

Ihr Administrator muss alle gültigen Zertifizierungsstellen-Zertifikatsketten für alle vertrauenswürdigen Benutzerzertifikate einer Serververtrauensspeicher-Datei auf dem Verbindungsserver- oder Sicherheitsserver-Host hinzufügen. Diese Zertifikatsketten beinhalten Stammzertifikate und müssen auch Zwischenzertifikate enthalten, wenn eine Zwischenzertifizierungsstelle das Smartcard-Zertifikat des Benutzers ausstellt.

Informationen zur Konfiguration des Verbindungsservers für die Unterstützung von Smartcards finden Sie im Dokument *Horizon-Verwaltung*.

Unified Access Gateway-Appliances

Informationen zur Konfiguration der Smartcard-Authentifizierung auf einer Unified Access Gateway-Appliance finden Sie im Dokument *Bereitstellen und Konfigurieren von VMware Unified Access Gateway*.

Active Directory

Informationen zu den Aufgaben, die Ihr Administrator eventuell in Active Directory zur Implementierung der Smartcard-Authentifizierung durchführen muss, finden Sie im Dokument *Horizon-Verwaltung*.

Authentifizierungsanforderungen für Clientgerätezertifikate

Mit der Authentifizierungsfunktion für Clientgerätezertifikate können Sie die Zertifikatauthentifizierung für Clientgeräte einrichten. Unified Access Gateway authentifiziert die Clientgeräte. Microsoft-Zertifikatdienste mit Active Directory verwalten die Erstellung und Verteilung von Zertifikaten an die Clientgeräte. Nach erfolgreicher Geräteauthentifizierung muss der Benutzer immer noch die Benutzerauthentifizierung durchführen.

Für diese Funktion gelten die folgenden Anforderungen.

- Unified Access Gateway 2.6 oder höher
- Horizon 7 Version 7.5 oder höher
- Ein auf dem Clientgerät installiertes Zertifikat, das von Unified Access Gateway akzeptiert wird

Informationen zum Konfigurieren von Unified Access Gateway finden Sie in der Unified Access Gateway-Dokumentation.

Verwenden Sie als Kryptografiedienstanbieter (Cryptographic Service Provider, CSP) in der Vorlage für die Ausstellung von Zertifikaten den Microsoft Enhanced RSA and AES Cryptographic Provider. Dieser CSP unterstützt SHA-256-Zertifikate und TLS v1.2. Verwenden Sie SHA-256. SHA-1 ist für Authentifizierungszwecke zu schwach.

Damit Windows ein Zertifikat für die Clientgeräteauthentifizierung verwenden kann, muss der Benutzer auf dem Clientgerät über Lesezugriff für den privaten Schlüssel des Zertifikats verfügen. Der private Schlüssel muss nicht exportierbar sein. Die Schlüsselverwendung des Zertifikats muss die digitale Signatur und Schlüsselverschlüsselung (a0) umfassen.

Sie können das Zertifikat im Zertifikatspeicher des aktuellen Benutzers oder des lokalen Computers auf dem Clientgerät installieren. Wenn Sie unter Windows 10 das Zertifikat im Zertifikatspeicher des lokalen Computers installieren und der Benutzer nicht der Benutzergruppe „System“ oder „Lokale Administratoren“ angehört, müssen Sie die folgenden Schritte ausführen, um dem Benutzer Lesezugriff für den privaten Schlüssel des Zertifikats zu gewähren. Wenn Sie das Zertifikat im Zertifikatspeicher des aktuellen Benutzers installieren, müssen Sie diese Schritte nicht durchführen.

1 Öffnen Sie den Zertifikatspeicher des lokalen Computers auf dem Clientgerät.

2 Klicken Sie mit der rechten Maustaste auf das Gerätezertifikat und wählen Sie **Alle Aufgaben > Private Schlüssel verwalten**.

3 Fügen Sie den Benutzer hinzu, weisen Sie dem Benutzer die Leseberechtigung zu und klicken Sie auf **OK**.

OPSWAT-Integrationsanforderungen

In einigen Unternehmen kann ein Administrator Unified Access Gateway in die OPSWAT-MetaAccess-Anwendung eines Drittanbieters integrieren. Diese Integration, die in der Regel auf nicht verwalteten Geräten in BYOD-Umgebungen (Bring your own device) von Unternehmen

verwendet wird, ermöglicht Organisationen die Definition von Akzeptanzrichtlinien für Horizon Client-Geräte.

Beispielsweise kann ein Administrator eine Geräteakzeptanzrichtlinie definieren, die verlangt, dass Clientgeräte kennwortgeschützt sind oder über eine minimale Betriebssystemversion verfügen. Clientgeräte, die der Geräte-Akzeptanzrichtlinie entsprechen, können über Unified Access Gateway auf Remote-Desktops und veröffentlichte Anwendungen zugreifen. Unified Access Gateway verweigert den Zugriff für Clientgeräte auf Remote-Ressourcen, die der Geräte-Akzeptanzrichtlinie nicht entsprechen.

Weitere Informationen finden Sie im Dokument *Bereitstellen und Konfigurieren von VMware Unified Access Gateway*.

Systemanforderungen für Echtzeit-Audio/Video

Echtzeit-Audio/Video funktioniert mit Standard-Webcams, USB-Audiogeräten und analogen Audiogeräten. Die Funktion funktioniert auch mit Standard-Konferenzanwendungen. Zur Unterstützung von Echtzeit-Audio/Video muss Ihre Horizon-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

Virtuelle Desktops

Um mehr als eine Webcam oder ein Mikrofon in einem virtuellen Desktop verwenden zu können, muss Horizon Agent 7.10 oder höher installiert sein.

Bei der Verwendung von Microsoft Teams mit Echtzeit-Audio/Video müssen virtuelle Desktops ein Minimum von 4 vCPUs und 4 GB RAM aufweisen.

Horizon Client-Computer oder Clientzugriffsgerät

- Echtzeit-Audio/Video wird auf allen Betriebssystemen unterstützt, auf denen Horizon Client für Windows ausgeführt wird. Weitere Informationen hierzu finden Sie unter Systemanforderungen für Windows-Clientsysteme.
- Auf dem Clientcomputer müssen Treiber für Webcam und Audiogeräte installiert sein, und die Webcam oder das Audiogerät muss betriebsbereit sein. Es ist nicht erforderlich, die Gerätetreiber auf dem Computer zu installieren, auf dem der Agent installiert ist.

Anzeigeprotokolle

- PCoIP
- VMware Blast

Systemanforderungen für Scannerumleitung

Endbenutzer können Informationen über ihre Remote-Desktops und Remoteanwendungen unter Verwendung von Scannern einscannen, die mit ihren lokalen Clientsystemen verbunden sind.

Damit Sie diese Funktion nutzen können, müssen die Remote-Desktops und Clientcomputer bestimmte Systemanforderungen erfüllen.

Remote-Desktops

Auf den Remote-Desktops muss Horizon Agent mit aktivierter Setup-Option „Scannerumleitung“ auf übergeordneten virtuellen Maschinen oder VM-Vorlagen oder RDS-Hosts installiert sein. Auf Windows-Desktop- und Windows-Server-Gastbetriebssystemen ist die Horizon Agent-Setup-Option „Scannerumleitung“ standardmäßig deaktiviert.

Informationen zu den für virtuelle Desktops und RDS-Hosts unterstützten Gastbetriebssystemen und zum Konfigurieren der Scannerumleitung auf Remote-Desktops und in veröffentlichten Anwendungen finden Sie unter „Konfigurieren der Scannerumleitung“ im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Horizon Client-Computer oder Clientzugriffsgerät

Die Scannerumleitung wird unter Windows 10 unterstützt. Auf dem Clientcomputer müssen Treiber für das Scannergerät installiert sein, und der Scanner muss betriebsbereit sein. Es ist nicht erforderlich, die Scanner-Gerätetreiber auf dem Betriebssystem des Remote-Desktops zu installieren, auf dem der Agent installiert ist.

Scangerät-Standard

TWAIN oder WIA

Anzeigeprotokolle

- PCoIP
- VMware Blast

Scannerumleitung wird in RDP-Desktop-Sitzungen nicht unterstützt.

Systemanforderungen für die Umleitung serieller Ports

Mit der Umleitung serieller Ports können Endbenutzer lokal verbundene serielle Ports (COM-Ports) wie integrierte RS232-Ports oder USB-Seriell-Adapter an ihre Remote-Desktops und veröffentlichten Anwendungen umleiten. Zur Unterstützung der Umleitung für serielle Ports muss Ihre VMware Horizon-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

Virtuelle Desktops

Horizon Agent muss mit aktivierter Setup-Option für die Umleitung serieller Ports installiert werden. Diese Setup-Option ist standardmäßig nicht ausgewählt.

Die folgenden Betriebssysteme werden auf virtuellen Desktops unterstützt.

- Windows 7, 32 oder 64 Bit
- Windows 8.x, 32 oder 64 Bit
- Windows 10, 32 oder 64 Bit

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Hinweis Horizon Agent 2006 und höher unterstützt nicht Windows 7, Windows 8.x, Windows Server 2008 R2 und Windows Server 2012 R2.

Gerätetreiber für serielle Ports müssen nicht auf dem virtuellen Desktop installiert sein.

Veröffentlichte Desktops und veröffentlichte Anwendungen

Auf RDS-Hosts muss Horizon Agent 7.6 oder höher mit aktivierter Setup-Option für die Umleitung serieller Ports installiert sein. Diese Setup-Option ist standardmäßig nicht ausgewählt.

Die folgenden Betriebssysteme werden für veröffentlichte Desktops und veröffentlichte Anwendungen unterstützt.

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Hinweis Horizon Agent 2006 und höher unterstützt nicht Windows Server 2008 R2 und Windows Server 2012 R2.

Gerätetreiber für serielle Ports müssen nicht im RDS-Host installiert sein.

Die Umleitung für serielle Ports ist für vollständige Desktops verfügbar und wird von veröffentlichten Anwendungen auf RDS-Hosts nicht unterstützt.

Horizon Client-Computer oder Clientzugriffsgerät

Die Umleitung serieller Ports wird auf Windows 10-Clientsystemen unterstützt. Die erforderlichen Gerätetreiber für serielle Ports müssen installiert sein, und der serielle Port muss betriebsbereit sein.

Anzeigeprotokolle

- PCoIP
- VMware Blast

Die Umleitung serieller Ports wird in RDP-Desktop-Sitzungen nicht unterstützt.

Informationen zum Konfigurieren der Umleitung serieller Ports finden Sie unter „Konfigurieren der Umleitung serieller Ports“ im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Anforderungen für die Verwendung der URL-Inhaltsumleitung

Mit der Funktion der URL-Inhaltsumleitung können URL-Inhalte vom Client Computer zu einem Remote-Desktop oder einer veröffentlichten Anwendung (Client-zu-Agent-Umleitung) oder von einem Remote-Desktop bzw. einer veröffentlichten Anwendung zum Client Computer (Agent-zu-Client-Umleitung) umgeleitet werden.

So kann beispielsweise ein Endbenutzer durch Klicken auf einen Link in der nativen Anwendung „Microsoft Word“ auf dem Client diesen in der Remoteanwendung „Internet Explorer“ öffnen. Umgekehrt hat ein Endbenutzer die Möglichkeit, durch Klicken auf einen Link in der Remoteanwendung „Internet Explorer“ diesen in einem nativen Browser auf dem Clientcomputer zu öffnen. Es kann eine beliebige Anzahl von Protokollen für die Umleitung konfiguriert werden, u. a. HTTP, Mailto und Callto.

Hinweis Das Callto-Protokoll wird für die URL-Inhaltsumleitung mit dem Chrome-Browser nicht unterstützt.

Webbrowser

Sie können eine URL in den folgenden Browsern eingeben oder anklicken und deren Umleitung einrichten.

- Internet Explorer 9, 10 und 11
- 64-Bit- oder 32-Bit-Chrome 60.0.3112.101, offizielles Build oder höher
- Microsoft Edge 80.0.361.48 und höher (offizieller Build), 64-Bit oder 32-Bit (Horizon Agent 2006 und höher)

Die URL-Inhaltsumleitung steht nicht für Links zur Verfügung, die in universellen Windows 10-Apps inklusive Microsoft Edge Browser angeklickt werden.

Clientsystem

Sie müssen die URL-Inhaltsumleitung aktivieren, wenn Sie Horizon Client installieren. Um die URL-Inhaltsumleitung aktivieren zu können, müssen Sie Horizon Client über die Befehlszeile installieren. Weitere Informationen hierzu finden Sie unter Installieren von Horizon Client über die Befehlszeile.

Um die URL-Inhaltsumleitung mit dem Chrome- oder Edge-Browser zu verwenden, muss ein Horizon Administrator die Erweiterung VMware Horizon URL Content Redirection Helper installieren und aktivieren. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Bei der ersten Umleitung einer URL aus dem Chrome-Browser werden Sie aufgefordert, die URL in Horizon Client zu öffnen. Sie müssen auf **Open URL:VMware Hori...lient Protocol** klicken, damit die URL-Inhaltsumleitung erfolgt. Wenn Sie das Kontrollkästchen **Meine Wahl für URL:VMware Hori...lient Protocol-Links merken** aktivieren, wird diese Eingabeaufforderung nicht mehr angezeigt.

Remote-Desktop oder veröffentlichte Anwendung

Ein Horizon-Administrator muss die URL-Inhaltsumleitung aktivieren, wenn Horizon Agent installiert wird. Informationen dazu finden Sie in den Dokumenten *Einrichten von virtuellen Desktops in Horizon* und *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.

Um die URL-Inhaltsumleitung mit dem Chrome-Browser verwenden zu können, muss ein Horizon-Administrator die Erweiterung VMware Horizon URL Content Redirection Helper auf dem Windows-Agent-Computer installieren und aktivieren. Informationen hierzu finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Ein Horizon-Administrator muss durch Konfiguration von Einstellungen auch festlegen, wie Horizon Client URL-Inhalte vom Client zu einem Remote-Desktop oder einer veröffentlichten Anwendung umleitet oder wie Horizon Agent URL-Inhalte von einem Remote-Desktop oder einer veröffentlichten Anwendung zum Client umleitet. Ausführliche Informationen finden Sie im *Konfigurieren von Remote-Desktop-Funktionen in Horizon*-Dokument unter dem Thema „Konfigurieren der URL-Inhaltsumleitung“.

Systemanforderungen für die HTML5-Multimedia-Umleitung

Horizon Agent, Horizon Client und die Remote-Desktops und Clientsysteme, auf denen Sie die Agent- und die Client-Software installieren, müssen bestimmte Anforderungen zur Unterstützung der HTML5-Multimedia-Umleitungsfunktion erfüllen.

Wenn ein Endbenutzer bei aktivierter HTML5-Multimedia-Umleitung den Google Chrome- oder Microsoft Edge-Browser über einen Remote-Desktop verwendet, wird der HTML5-Multimedia-Inhalt an das Clientsystem gesendet. Das Clientsystem gibt die Medieninhalte wieder und verringert so die Last auf dem ESXi-Host. Zudem wird dem Endbenutzer ein besseres Audio- und Videoerlebnis geboten.

Remote-Desktop

- Horizon Agent muss auf dem virtuellen Desktop oder dem RDS-Host für veröffentlichte Desktops mit aktivierter Setup-Option für die HTML5-Multimedia-Umleitung installiert werden. Ab Horizon Agent 7.10 wird die benutzerdefinierte Setup-Option für die HTML5-Multimedia-Umleitung entfernt und die HTML5-Multimedia-Umleitung standardmäßig installiert. Weitere Informationen finden Sie in den Themen zur Installation von Horizon Agent in den Dokumenten *Einrichten von virtuellen Desktops in Horizon* und *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.
- Die Gruppenrichtlinieneinstellungen für die HTML5-Multimedia-Umleitung müssen auf dem Active Directory-Server konfiguriert werden. Informationen zur Konfiguration der HTML5-Multimedia-Umleitung finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.
- Der Chrome- oder Edge-Browser muss installiert sein.

- Die Erweiterung „VMware Horizon HTML5-Multimedia-Umleitung“ muss im Chrome- oder Edge-Browser installiert sein. Informationen zur Konfiguration der HTML5-Multimedia-Umleitung finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Clientsystem

- Die benutzerdefinierte Setup-Option für die Unterstützung der HTML5-Multimedia-Umleitung und der Browser-Umleitung muss ausgewählt werden, wenn Sie Horizon Client installieren. Diese Option ist standardmäßig ausgewählt.

Das Anzeigeprotokoll für die Remote-Sitzung ist

- PCoIP
- VMware Blast

TCP-Port

Die HTML5-Multimedia-Umleitung verwendet Port 9427.

Einschränkungen

Für die HTML5-Multimedia-Umleitungsfunktion gelten folgende Einschränkungen:

- Die relative Mausfunktion von Horizon Client wird nicht unterstützt.
- Es ist nicht möglich, die Funktionen **Webseite stummschalten** (Chrome-Browser) oder **Registerkarte stummschalten** (Edge-Browser) zu verwenden.

Systemanforderungen für die Browser-Umleitung

Die Remote-Desktops und Clientsysteme, auf denen Sie den Agent und die Client-Software installieren, müssen bestimmte Anforderungen zur Unterstützung der Browser-Umleitungsfunktion erfüllen.

Wenn ein Endbenutzer bei der Browser-Umleitung eine Website im Chrome-Browser auf einem Remote-Desktop öffnet, wird die Webseite auf dem Clientsystem anstelle des Agent-Systems gerendert und im Viewport des Remote Browsers angezeigt. Der Viewport ist der Teil des Browserfensters, der den Inhalt der Webseite enthält.

Remote-Desktops

- Horizon Agent 7.10 oder höher muss auf dem virtuellen Desktop oder RDS-Host für veröffentlichte Desktops installiert sein. Weitere Informationen finden Sie in den Abschnitten zum Installieren von Horizon Agent in den Dokumenten *Einrichten von virtuellen Desktops in Horizon* und *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.

- Die Gruppenrichtlinieneinstellungen für die VMware Browser-Umleitung müssen auf dem Active Directory-Server konfiguriert werden. Weitere Informationen finden Sie in den Abschnitten zum Konfigurieren der Browser-Umleitung im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.
- Der Chrome-Browsers muss installiert sein.
- Die Erweiterung „VMware Horizon-Browser-Umleitung“ muss im Chrome-Browser installiert sein. Weitere Informationen finden Sie in den Abschnitten zum Konfigurieren der Browser-Umleitung im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Das Anzeigeprotokoll für die Remote-Sitzung ist

- PCoIP
- VMware Blast

Systemanforderungen für die Multimedia-Umleitung (MMR)

Mit Multimedia-Umleitung (MMR) wird der Multimedia-Stream auf dem Clientsystem decodiert. Das Clientsystem gibt die Medieninhalte wieder, sodass die Last auf dem ESXi-Host verringert wird.

Remote-Desktops

Informationen zu den Betriebssystemanforderungen und anderen Softwareanforderungen und Konfigurationseinstellungen finden Sie in den Themen zur Windows-Multimedia-Umleitung im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Horizon Client-Computer oder Clientzugriffsgerät

Windows 10

Unterstützte Medienformate

In Windows Media Player unterstützte Medienformate, beispielsweise: M4V; MOV; MP4; WMP; MPEG-4 Part 2; WMV 7, 8 und 9; WMA; AVI; ACE; MP3; WAV.

MP3 wird bei Verwendung von MMS und RTSP nicht unterstützt.

Hinweis DRM-geschützter Inhalt wird nicht über Windows Media MMR umgeleitet.

Systemanforderungen für die Geolocation-Umleitung

Horizon Agent und Horizon Client und der virtuelle Desktop oder RDS-Host und der Client-Computer, auf dem Sie die Agent- und Client-Software installieren, müssen bestimmte Anforderungen erfüllen, um die Geolocation-Umleitungsfunktion zu unterstützen.

Bei der Geolocation-Umleitung werden Geolocation-Informationen vom Clientsystem an den Remote-Desktop oder die veröffentlichte Anwendung gesendet.

Virtueller Desktop oder RDS-Host

- Die Windows-Einstellung **Standortdienste** muss unter **Einstellungen > DatenschutzStandort aktiviert** sein.
- Die Geolocation-Umleitung unterstützt folgende Remote-Desktop-Anwendungen.

Anwendung	Plattform
Google Chrome (neueste Version)	Alle virtuellen Desktops oder RDS-Hosts
Internet Explorer 11	Alle virtuellen Desktops oder RDS-Hosts
Edge, Maps, Weather und andere Win32- und UWP-Apps	Windows 10

  Die Berechtigungseinstellung für den **Standort** muss, falls vorhanden, einzeln in jedem unterstützten Browser aktiviert werden.
- Für Horizon Agent 7.6 oder höher muss bei der Installation die benutzerdefinierte Setup-Option für die Geolocation-Umleitung aktiviert werden. Diese Option ist nicht standardmäßig ausgewählt. Weitere Informationen finden Sie in den Abschnitten zum Installieren von Horizon Agent in den Dokumenten *Einrichten von virtuellen Desktops in Horizon* und *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.
- Die Gruppenrichtlinieneinstellungen für die VMware Geolocation-Umleitung müssen auf dem Active Directory-Server konfiguriert werden. Weitere Informationen finden Sie in den Abschnitten zum Konfigurieren der Geolocation-Umleitung im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.
- Bei Internet Explorer 11 muss das Internet Explorer-Plug-in für VMware Horizon Geolocation für RDS-Hosts aktiviert werden. Sie müssen das IE-Plug-In für die VMware Horizon Geolocation-Umleitung für virtuelle Windows 10-Desktops nicht aktivieren. Internet Explorer wird auf virtuellen Windows 10-Desktops mit dem VMware Geolocation-Umleitungstreiber unterstützt. Weitere Informationen finden Sie in den Abschnitten zum Konfigurieren der Geolocation-Umleitung im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.
- Für Chrome muss das Chrome-Plug-in für die VMware Horizon Geolocation-Umleitung aktiviert werden. Weitere Informationen finden Sie in den Abschnitten zum Konfigurieren der Geolocation-Umleitung im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Clientsystem

- Um die Standortinformationen des Clientsystems freizugeben, müssen Sie die **Geolocation**-Einstellungen in Horizon Clientkonfigurieren. Weitere Informationen hierzu finden Sie unter Informationen zum Speicherort der Freigabe.

- Damit Horizon auf den Standort zugreifen kann, muss für Windows 10-Client-Systeme für die Windows-Einstellung **Positionsdienst** unter **Einstellungen > Datenschutz > Position Ein** festgelegt werden.

Das Anzeigeprotokoll für die Remote-Sitzung ist

- PCoIP
- VMware Blast

Anforderungen für die Funktion „Session Collaboration“

Mit der Funktion „Session Collaboration“ können Benutzer andere Benutzer zur Teilnahme an einer vorhandenen Remote-Desktop-Sitzung einladen. Um die Funktion „Session Collaboration“ zu unterstützen, muss Ihre Horizon-Bereitstellung bestimmte Anforderungen erfüllen.

Sitzungsteilnehmer

Um an einer gemeinsamen Sitzung teilnehmen zu können, muss auf dem Clientsystem des Benutzers Horizon Client für Windows, Mac oder Linux installiert sein oder HTML Access verwendet werden.

Windows-Remote-Desktops

Die Funktion „Session Collaboration“ muss auf Desktop-Pool- oder Farmebene aktiviert sein. Informationen zur Aktivierung der Funktion „Session Collaboration“ für Desktop-Pools finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon*. Informationen zur Aktivierung der Funktion „Session Collaboration“ für eine Farm erhalten Sie im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.

Sie können mithilfe von Horizon Agent-Gruppenrichtlinieneinstellungen die Funktion „Session Collaboration“ konfigurieren. Informationen hierzu finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Linux-Remote-Desktops

Informationen zu den Anforderungen für Linux-Remote-Desktops finden Sie im Dokument *Einrichten von Linux-Desktops in Horizon*.

Verbindungsserver

Für die Funktion „Session Collaboration“ muss die Verbindungsserver-Instanz eine Enterprise-Lizenz verwenden.

Anzeigeprotokolle

VMware Blast

Die Funktion „Session Collaboration“ unterstützt Sitzungen mit veröffentlichten Anwendungen nicht.

Voraussetzungen für die Verwendung von Skype for Business mit Horizon Client

Ein Endbenutzer kann damit Skype for Business in einem virtuellen Desktop ohne negative Auswirkungen auf die virtuelle Infrastruktur und die Netzwerklast ausführen. Bei Skype-Audio- und -Videoanrufen findet die gesamte Medienverarbeitung auf dem Client Computer und nicht im virtuellen Desktop statt.

Um diese Funktion zu verwenden, müssen Sie bei der Installation von Horizon Client für Windows die Funktion des Virtualization Pack für Skype for Business auf dem Client Computer mitinstallieren. Weitere Informationen hierzu finden Sie unter Kapitel 2 Installation von Horizon Client für Windows.

Ein Horizon-Administrator muss bei der Installation von Horizon Agent auch das VMware Virtualization Pack für Skype for Business auf dem virtuellen Desktop installieren. Informationen zum Installieren von Horizon Agent finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon*.

Die vollständigen Informationen zu den Anforderungen finden Sie unter „Konfigurieren von Skype für Business“ im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Unterstützte Desktop-Betriebssysteme

Ihr Horizon-Administrator erstellt virtuelle Maschinen mit einem Gastbetriebssystem und installiert Agent-Software im Gastbetriebssystem. Die Endbenutzer können sich an diesen virtuellen Maschinen von einem Client-Gerät aus anmelden.

Eine Liste unterstützter Windows-Gastbetriebssysteme finden Sie im Dokument *Horizon-Installation*.

Einige Linux-Gastbetriebssysteme werden ebenfalls unterstützt. Informationen zu den Systemanforderungen und zur Konfiguration von virtuellen Linux-Maschinen sowie eine Liste der unterstützten Funktionen finden Sie im Dokument *Einrichten von Linux-Desktops in Horizon*.

Vorbereiten des Verbindungsservers für Horizon Client

Bevor Endbenutzer eine Verbindung mit einem Server herstellen und auf einen Remote-Desktop oder eine veröffentlichte Anwendung zugreifen können, muss ein Horizon-Administrator bestimmte Verbindungsserver-Einstellungen konfigurieren.

Unified Access Gateway und Sicherheitsserver

Wenn Ihre VMware Horizon-Bereitstellung eine Unified Access Gateway-Appliance enthält, konfigurieren Sie den Verbindungsserver für die Arbeit mit Unified Access Gateway. Siehe das Dokument *Bereitstellen und Konfigurieren von VMware Unified Access Gateway*. Unified Access Gateway-Appliances führen Sie die gleichen Rollen wie Sicherheitsserver aus.

Wenn Ihre VMware Horizon-Bereitstellung einen Sicherheitsserver umfasst, stellen Sie sicher, dass Sie die aktuellen Wartungsversionen für einen Verbindungsserver der Version 7.5 und einen Sicherheitsserver der Version 7.5 oder höher verwenden. Weitere Informationen finden Sie im Installationsdokument für Ihre Horizon-Version.

Hinweis Sicherheitsserver werden in VMware Horizon 2006 und höher nicht unterstützt.

Sichere Tunnelverbindung

Wenn Sie eine sichere Tunnelverbindung für Clientgeräte verwenden möchten und die sichere Verbindung mit einem DNS-Hostnamen für eine Verbindungsserver-Instanz oder einen Sicherheitsserver konfiguriert ist, muss sichergestellt werden, dass das Clientgerät diesen DNS-Namen auflösen kann.

Desktop- und Anwendungspools

Verwenden Sie die folgende Checkliste bei der Konfiguration von Desktop- und Anwendungspools.

- Vergewissern Sie sich, dass ein Desktop- oder Anwendungspool erstellt wurde und das Benutzerkonto, das Sie verwenden möchten, über die Rechte zum Zugriff auf diesen Pool verfügt. Weitere Informationen dazu finden Sie in den Dokumenten *Einrichten von virtuellen Desktops in Horizon* und *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.
- Wenn Endbenutzer mit einem hochauflösenden Anzeigegerät arbeiten und die Clienteinstellung **Modus mit hoher Auflösung** verwenden, während ihre Remote-Desktops im Vollbildmodus angezeigt werden, müssen Sie sicherstellen, dass jedem Windows-Remote-Desktop ausreichend vRAM zugeteilt ist. Die vRAM-Menge hängt von der Anzeigeauflösung und der Anzahl der Monitore ab, die für Endbenutzer konfiguriert wurden.

Benutzerauthentifizierung

Verwenden Sie die folgende Checkliste beim Einrichten der Benutzerauthentifizierung.

- Um Endbenutzern den nicht authentifizierten Zugriff auf veröffentlichte Anwendungen in Horizon Client zu ermöglichen, müssen Sie diese Funktion in der Verbindungsserver-Instanz aktivieren. Weitere Informationen finden Sie in den Themen zum nicht authentifizierten Zugriff im Dokument *Horizon-Verwaltung*.
- Um Zwei-Faktor-Authentifizierung, wie z. B. RSA SecurID oder RADIUS-Authentifizierung, mit Horizon Client zu verwenden, müssen Sie die Funktion „Zwei-Faktor-Authentifizierung“ für die Verbindungsserver-Instanz aktivieren. Ab Horizon 7 Version 7.11 können Sie die Bezeichnungen auf der Anmeldeseite für die RADIUS-Authentifizierung anpassen. Ab Horizon 7 Version 7.12 können Sie die Zwei-Faktor-Authentifizierung so konfigurieren, dass Sie nach einer Zeitüberschreitung bei der Remotesitzung stattfindet. Weitere Informationen finden Sie in den Themen zur zweistufigen Authentifizierung im Dokument *Horizon-Verwaltung*.

- Um zuzulassen, dass die Verbindungsserver-Instanz die Benutzeridentitäts- und Anmeldedaten akzeptiert, die übermittelt werden, wenn Benutzer **Als aktueller Benutzer anmelden** im Menü **Optionen** in Horizon Client auswählen, müssen Sie die Einstellung **Anmeldung als aktueller Benutzer zulassen** für die Verbindungsserver-Instanz aktivieren. Diese Einstellung ist in Horizon 7, Version 7.8 und höher verfügbar. Weitere Informationen finden Sie im Dokument *Horizon-Verwaltung*.

  Sie können Horizon Client-Gruppenrichtlinieneinstellungen verwenden, um die Funktion „Als aktueller Benutzer anmelden“ zu konfigurieren. Unter anderem können Sie auch eine Liste mit Verbindungsserver-Instanzen angeben, die Authentifizierungsdaten für die Funktion „Als aktueller Benutzer anmelden“ akzeptieren. Weitere Informationen zu diesen clientseitigen Einstellungen finden Sie unter Sicherheitseinstellungen für Client-GPOs.
- Um die Server-URL in Horizon Client auszublenden, aktivieren Sie die globale Einstellung **Serverinformationen in der Kunden-Benutzeroberfläche ausblenden**. Weitere Informationen finden Sie im Dokument *Horizon-Verwaltung*.
- Um das Dropdown-Menü **Domäne** in Horizon Client auszublenden, aktivieren Sie die globale Einstellung **Domänenliste in der Kunden-Benutzeroberfläche ausblenden**. Ab Horizon 7 Version 7.8 ist diese Einstellung standardmäßig aktiviert. Weitere Informationen finden Sie im Dokument *Horizon-Verwaltung*.
- Um die Domänenliste an Horizon Client zu senden, aktivieren Sie die globale Einstellung **Domänenliste senden** in Horizon Console. Diese Einstellung ist in Horizon 7 Version 7.8 und höher verfügbar und ist standardmäßig deaktiviert. Niedrigere Versionen von Horizon 7 senden die Domänenliste. Weitere Informationen finden Sie im Dokument *Horizon-Verwaltung*.

In der folgenden Tabelle wird gezeigt, wie die globalen Einstellungen **Domänenliste senden** und **Domänenliste in der Kunden-Benutzeroberfläche ausblenden** festlegen, wie Benutzer sich beim Server anmelden können.

Einstellung „Domänenliste senden“	Einstellung „Domänenliste in der Kunden-Benutzeroberfläche ausblenden“	Wie sich Benutzer anmelden
Deaktiviert (Standard)	Aktiviert	Das Dropdown-Menü **Domäne** ist ausgeblendet. Benutzer müssen einen der folgenden Werte in das Textfeld **Benutzername** eingeben. ■ Benutzername (nicht für mehrere Domänen zulässig) ■ *Domäne\Benutzername* ■ *username@domain.com*
Deaktiviert (Standard)	Deaktiviert	Wenn eine Standarddomäne auf dem Client konfiguriert ist, wird die Standarddomäne im Dropdown-Menü **Domäne** angezeigt. Wenn der Client keine Standarddomäne kennt, wird `*DefaultDomain*` im Dropdown-Menü **Domäne** angezeigt. Benutzer müssen einen der folgenden Werte in das Textfeld **Benutzername** eingeben. ■ Benutzername (nicht für mehrere Domänen zulässig) ■ *Domäne\Benutzername* ■ *username@domain.com*
Aktiviert	Aktiviert	Das Dropdown-Menü **Domäne** ist ausgeblendet. Benutzer müssen einen der folgenden Werte in das Textfeld **Benutzername** eingeben. ■ Benutzername (nicht für mehrere Domänen zulässig) ■ *Domäne\Benutzername* ■ *username@domain.com*
Aktiviert	Deaktiviert	Benutzer können einen Benutzernamen in das Textfeld **Benutzername** eingeben und dann eine Domäne aus dem Dropdown-Menü **Domäne** auswählen. Alternativ können Benutzer auch einen der folgenden Werte in das Textfeld **Benutzername** eingeben. ■ *Domäne\Benutzername* ■ *username@domain.com*

Löschen des zuletzt für die Anmeldung bei einem Server verwendeten Benutzernamens

Wenn sich Endbenutzer bei einer Verbindungsserver-Instanz anmelden, für die die globale Einstellung **Domänenliste in der Kunden-Benutzeroberfläche ausblenden** aktiviert wurde, ist das Dropdown-Menü **Domäne** in Horizon Client ausgeblendet. Benutzer müssen dann die Domäneninformationen im Textfeld Horizon Client **Benutzername** bereitstellen. Der Benutzername muss dabei im Format *Domäne\Benutzername* oder *Benutzername@Domäne* eingegeben werden.

Auf einem Windows-Clientsystem wird durch einen Registrierungsschlüssel festgelegt, ob der letzte Benutzername gespeichert und im Textfeld **Benutzername** bei der nächsten Anmeldung des Benutzers beim Server angezeigt wird. Wenn der letzte Benutzername nicht im Feld **Benutzername** angezeigt werden soll und keine Domäneninformationen sichtbar sein sollen, müssen Sie den Wert des Registrierungsschlüssels `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\dontdisplaylastusername` auf dem Windows-Clientsystem in 1 ändern.

Informationen zum Ausblenden von Sicherheitsinformationen wie das Dropdown-Menü **Domäne** und Server-URL-Informationen in Horizon Client finden Sie in den Themen über globale Einstellungen im Dokument *Horizon-Verwaltung*.

Konfigurieren der VMware Blast-Optionen

Sie können die VMware Blast-Optionen für Sitzungen mit Remote-Desktops und veröffentlichten Anwendungen konfigurieren, die das VMware Blast-Anzeigeprotokoll verwenden.

Sie können H.264-Decodierung und High Efficiency Video Coding (HEVC) zulassen. H.264 ist ein Industriestandard für die Videokomprimierung. Dabei handelt es sich um den Prozess der Konvertierung digitaler Videos in ein Format, das weniger Kapazität beansprucht, wenn es gespeichert oder übertragen wird. Wenn H.264-Decodierung zulässig ist, können Sie auch eine verbesserte Farbtreue zulassen.

Die maximal unterstützte Auflösung und die HEVC-Unterstützung hängen von der Kapazität des Grafikprozessors (GPU, Graphical Processing Unit) auf dem Client ab. Eine GPU, die die 4K-Auflösung für JPEG/PNG unterstützt, unterstützt nicht zwangsläufig auch die 4K-Auflösung für H.264. Wird die Auflösung für H.264 nicht unterstützt, verwendet Horizon Client stattdessen JPEG/PNG.

Wenn in Ihrer Umgebung ein Proxy-Server verwendet wird, können Sie angeben, ob VMware Blast-Verbindungen zu einem Betriebssystem-Proxy-Server zugelassen werden sollen.

Für einen SSL-Proxy-Server müssen Sie zudem die Zertifikatsprüfung für sekundäre Verbindungen über den SSL-Proxy-Server konfigurieren. Weitere Informationen finden Sie unter Festlegen des Zertifikatsprüfungsmodus in Horizon Client.

Die VMware Blast-Optionen können Sie vor und nach der Herstellung einer Verbindung mit einem Server konfigurieren.

Voraussetzungen

Um High Efficiency Video Coding (HEVC) zu verwenden, muss Horizon Agent 7.7 oder höher installiert sein. Für eine höhere Farbgenauigkeit mit YUV 4:4:4 muss Horizon Agent 7.11 oder höher installiert sein. Darüber hinaus muss das Clientsystem über eine GPU verfügen, die die HEVC-Decodierung unterstützt.

Die clientseitige Gruppenrichtlinieneinstellung **Verwendung von Proxy-Einstellungen des Betriebssystems durch Blast-Verbindungen zulassen** legt fest, ob VMware Blast-Verbindungen über einen Proxyserver hergestellt werden können und ob Benutzer die VMware Blast-Proxy-Server-Einstellung auf der Horizon Client-Benutzeroberfläche ändern können. Weitere Informationen finden Sie unter Allgemeine Einstellungen für Client-GPOs.

Abhängig von der installierten Horizon Agent-Version kann ein Horizon Administrator die Agent-seitige Gruppenrichtlinieneinstellungen verwenden, um VMware Blast-Funktionen, einschließlich H.264 und der hohen Farbgenauigkeit (HEVC), zu aktivieren bzw. zu deaktivieren. Weitere Informationen finden Sie unter „VMware Blast – Richtlinieneinstellungen“ im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Verfahren

1 Starten Sie Horizon Client.

2 Klicken Sie auf die Schaltfläche **Optionen** oben rechts in der Menüleiste und wählen Sie **VMware Blast konfigurieren** aus.

   Wenn Sie bei einem Server angemeldet sind, können Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Zahnradsymbol **Einstellungen** klicken und **VMware Blast** auswählen.

3 Um die H.264-Decodierung in Horizon Client zu ermöglichen, aktivieren Sie das Kontrollkästchen **H.264-Decodierung zulassen**.

   Ist diese Option ausgewählt (Standardeinstellung), verwendet Horizon Client die H.264-Decodierung, wenn der Agent die H.264-Software- oder -Hardwarecodierung unterstützt. Wenn der Agent die H.264-Software- oder -Hardwarecodierung nicht unterstützt, verwendet Horizon Client die JPG/PNG-Decodierung (mit Horizon Agent 7.x) oder Blast Codec-Decodierung (mit Horizon Agent 2006 und höher). Wenn diese Option deaktiviert ist, verwendet Horizon Client die JPG/PNG-Decodierung (mit Horizon Agent 7.x) oder Blast Codec-Decodierung (mit Horizon Agent 2006 und höher).

4 Um erhöhte Farbtreue zuzulassen, wenn die H.264-Decodierung in Horizon Client zulässig ist, aktivieren Sie das Kontrollkästchen **Hohe Farbgenauigkeit zulassen (niedrigere Akkulaufzeit und Leistung)**.

   Wenn diese Option ausgewählt ist, verwendet Horizon Client eine hohe Farbgenauigkeit, allerdings nur, wenn der Agent diese unterstützt. Durch die Auswahl dieser Option werden möglicherweise die Akkulaufzeit und Leistung reduziert. Diese Funktion ist standardmäßig deaktiviert.

5 Um HEVC zuzulassen, aktivieren Sie das Kontrollkästchen **High Efficiency Video Coding (HEVC) zulassen**.

   Wenn diese Option ausgewählt ist, werden die Leistung und die Bildqualität verbessert, wenn der Client Computer über eine GPU verfügt, die HEVC-Decodierung unterstützt. Diese Funktion ist standardmäßig deaktiviert.

Wenn diese Option ausgewählt ist, der Clientcomputer jedoch nicht über eine GPU verfügt, die die HEVC-Decodierung unterstützt, verwendet Horizon Client stattdessen H.264-Decodierung.

6 Um VMware Blast-Verbindungen über einen Proxy-Server zuzulassen, aktivieren Sie das Kontrollkästchen **Verwendung von Proxy-Einstellungen des Betriebssystems durch Blast-Verbindungen zulassen**.

7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ergebnisse

Änderungen werden wirksam, wenn ein Benutzer beim nächsten Mal eine Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung herstellt und das VMware Blast-Anzeigeprotokoll auswählt. Ihre Änderungen haben keinen Einfluss auf vorhandene VMware Blast-Sitzungen.

Verwenden von Internet Explorer-Proxy-Einstellungen

Horizon Client verwendet die in Internet Explorer konfigurierten Proxy-Einstellungen.

Einstellungen für die Proxy-Umgehung

Horizon Client verwendet Internet Explorer-Einstellungen für die Proxy-Umgehung, um HTTPS-Verbindungen mit einem Verbindungsserver-Host, mit einem Sicherheitsserver oder mit einer Unified Access Gateway-Appliance zu umgehen.

Wenn der sichere Tunnel auf dem Verbindungsserver-Host, dem Sicherheitsserver oder in der Unified Access Gateway-Appliance aktiviert ist, müssen Sie mit der Gruppenrichtlinieneinstellung `Adressliste zur Umgehung des Tunnel–Proxy` in der ADM- oder ADMX-Vorlagendatei für die Horizon Client-Konfiguration eine Liste von Adressen angeben, um die Tunnelverbindung zu umgehen. Der Proxy-Server wird für diese Adressen nicht verwendet. Verwenden Sie ein Semikolon (;) zum Trennen mehrerer Einträge. Diese Gruppenrichtlinieneinstellung erstellt den folgenden Registrierungsschlüssel:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\Client\TunnelProxyBypass
```

Sie können diese Gruppenrichtlinieneinstellung nicht für direkte Verbindungen verwenden. Wenn die Anwendung der Gruppenrichtlinieneinstellung nicht wie vorgesehen funktioniert, versuchen Sie den Proxy für lokale Adressen zu umgehen. Weitere Informationen finden Sie unter https://blogs.msdn.microsoft.com/askie/2015/10/12/how-to-configure-proxy-settings-for-ie10-and-ie11-as-iem-is-not-available/.

Proxy-Failover

Horizon Client unterstützt ein Proxy-Failover mit der Einstellung **Skript für automatische Konfiguration verwenden** unter **Automatische Konfiguration** in **Internetoptionen > Verbindungen > LAN-Einstellungen** in Internet Explorer. Um diese Einstellung verwenden zu können, müssen Sie ein Skript zur automatischen Konfiguration erstellen, das mehrere Proxy-Server zurückgibt.

Konfigurieren der Horizon Client-Datenfreigabe

Wenn ein Horizon-Administrator sich für die Teilnahme am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) entschieden hat, erfasst und empfängt VMware anonyme Daten von Clientsystemen über den Verbindungsserver. Sie können konfigurieren, ob diese Clientdaten für den Verbindungsserver freigegeben werden sollen.

Informationen zum Konfigurieren von Horizon für die Teilnahme am CEIP finden Sie im Dokument *Horizon-Verwaltung*.

Die Datenfreigabe ist in Horizon Client standardmäßig aktiviert. Sie müssen die Datenfreigabeeinstellung konfigurieren, bevor Sie eine Verbindung zu einem Server herstellen. Die Einstellung gilt für alle Server. Sie können die Einstellung zur Horizon Client-Datenfreigabe nach der Herstellung einer Verbindung mit einem Server nicht mehr ändern.

Sie können die Gruppenrichtlinieneinstellung **Datenfreigabe zulassen** verwenden, um die Datenfreigabe zu aktivieren oder zu deaktivieren, und verhindern, dass Benutzer die Einstellung in der Benutzeroberfläche von Horizon Client ändern. Weitere Informationen finden Sie unter Allgemeine Einstellungen für Client-GPOs.

Verfahren

1. Klicken Sie auf die Schaltfläche **Optionen** oben rechts in der Menüleiste und wählen Sie **Datenfreigabe zulassen** aus.
2. Setzen Sie den Datenfreigabemodus auf **Ein** oder **Aus** und klicken Sie auf **OK**.

Durch VMware gesammelte Horizon Client-Daten

Wenn ein Horizon Administrator am Programm zur Verbesserung der Benutzerfreundlichkeit teilnimmt und die Datenfreigabe im Clientsystem aktiviert ist, erfasst VMware Daten zum Clientsystem.

VMware sammelt Daten zu den Clientsystemen zur Priorisierung der Hardware- und Softwarekompatibilität. Wenn sich der Horizon Administrator für die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit entscheidet, erfasst VMware anonyme Daten über Ihre Bereitstellung, um besser auf Kundenanforderungen reagieren zu können. VMware sammelt keine Daten, die Rückschlüsse auf Ihre Organisation zulassen. Die Horizon Client-Informationen werden erst an die Verbindungsserver-Instanz und dann an VMware gesendet, zusammen mit Daten zum Verbindungsserver, zu Desktop-Pools und zu Remote-Desktops.

Die Informationen werden bei der Übertragung an die Verbindungsserver-Instanz verschlüsselt. Die Informationen auf dem Clientsystem werden unverschlüsselt in einem benutzerspezifischen Verzeichnis protokolliert. Die Protokolle enthalten jedoch keine personenbezogenen Informationen.

Horizon-Administratoren können bei der Installation des Verbindungsservers entscheiden, ob am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit teilgenommen wird. Sie können auch nach der Installation eine entsprechende Option in Horizon Console festlegen.

Tabelle 1-1. Von den Horizon Client-Instanzen gesammelte Daten für das Programm zur Verbesserung der Benutzerfreundlichkeit

Beschreibung	Wird dieses Feld anonymisiert?
Unternehmen, das die Horizon Client-Anwendung hergestellt hat	Nein
Produktname	Nein
Client-Produktversion	Nein
Client-Binärarchitektur	Nein
Client-Build-Name	Nein
Host-Betriebssystem	Nein
Host-Betriebssystemkernel	Nein
Host-Betriebssystemarchitektur	Nein
Hostsystem-Modell	Nein
Hostsystem-CPU	Nein
Anzahl der Cores bzw. Kerne im Prozessor des Hostsystems	Nein
MB Arbeitsspeicher auf dem Hostsystem	Nein
Anzahl der angeschlossenen USB-Geräte	Nein
Maximale Anzahl gleichzeitiger USB-Geräteverbindungen	Nein
Hersteller-ID des USB-Geräts	Nein
Produkt-ID des USB-Geräts	Nein
USB-Gerätefamilie	Nein
USB-Gerätenutzungszähler	Nein

Installation von Horizon Client für Windows

2

Das Windows-basierte Horizon Client-Installationsprogramm können Sie von der VMware-Website oder über eine Seite für den Webzugriff abrufen, die vom Verbindungsserver bereitgestellt wird. Nach der Installation von Horizon Client können Sie verschiedene Startoptionen für die Endbenutzer festlegen.

Dieses Kapitel enthält die folgenden Themen:

Aktivieren des FIPS-Modus im Windows-Clientbetriebssystem

Wenn Sie eine Installation von Horizon Client mit Federal Information Processing Standard (FIPS-)konformer Kryptografie planen, müssen Sie den FIPS-Modus im Clientbetriebssystem aktivieren, bevor Sie das Horizon Client-Installationsprogramm ausführen.

Wenn der FIPS-Modus im Clientbetriebssystem aktiviert ist, verwenden Anwendungen nur kryptografische Algorithmen, die mit FIPS-140 und mit FIPS-genehmigten Betriebsarten konform sind. Sie können den FIPS-Modus aktivieren, indem Sie eine spezifische Sicherheitseinstellung aktivieren – entweder in der lokalen Sicherheitsrichtlinie, als Teil einer Gruppenrichtlinie oder durch Bearbeiten des Windows-Registrierungsschlüssels.

Weitere Informationen zur FIPS-Konformität finden Sie im Dokument *Horizon-Installation*.

Festlegen der FIPS-Konfigurationseigenschaft

Um den FIPS-Modus im Clientbetriebssystem zu aktivieren, können Sie entweder eine Windows-Gruppenrichtlichtlinieneinstellung oder eine Windows-Registrierungseinstellung für den Clientcomputer verwenden.

- Zur Verwendung einer Gruppenrichtlichtlinie öffnen Sie den Gruppenrichtlinien-Editor, wechseln Sie zu `Computerkonfiguration\Windows–Einstellungen \Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen` und aktivieren Sie die Einstellung **Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden**.
- Um die Windows-Registrierung zu verwenden, wechseln Sie zu `HKLM\System \CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled` und legen Sie für **Aktiviert** 1 fest.

Weitere Informationen zum FIPS-Modus finden Sie unter https://support.microsoft.com/en-us/kb/811833.

Wichtig Damit die Installationsoption zur Verwendung der FIPS-konformen Kryptografie in einer benutzerdefinierten Installation angezeigt wird, muss der FIPS-Modus vor der Ausführung des Horizon Client-Installationsprogramms aktiviert werden. Die FIPS-konforme Kryptografie wird im Rahmen einer standardmäßigen Installation nicht aktiviert. Wenn Sie Horizon Client ohne die Option für eine FIPS-konforme Kryptografie installieren und sich später für die Verwendung dieser Option entscheiden, müssen Sie den Client deinstallieren, den FIPS-Modus im Clientbetriebssystem aktivieren und das Horizon Client-Installationsprogramm erneut ausführen.

Aktivieren der automatischen Auswahl des Internetprotokolls

Wenn Sie eine benutzerdefinierte Installation von Horizon Client vornehmen, können Sie die automatische Auswahl des Internetprotokolls aktivieren. Bei einer automatischen Auswahl prüft Horizon Client das aktuelle Netzwerk und stellt die Verbindung automatisch über IPv4 oder IPv6 her.

Wenn die automatische Auswahl aktiviert ist, werden die folgenden Funktionen bei Unified Access Gateway 3.3 oder höher mit dem VMware Blast-Anzeigeprotokoll unterstützt.

- Als aktueller Benutzer anmelden
- Audio-Ausgabe
- Datenerfassung für das Programm zur Verbesserung der Benutzerfreundlichkeit
- Virtueller Druck
- VMware Integrated Printing (erfordert Horizon 7, Version 7.7 oder höher)
- HTML5-Multimedia-Umleitung
- VMware Video

- USB-Umleitung
- Echtzeit-Audio/Video (RTAV)

Installation von Horizon Client für Windows

Sie können eine Windows-basierte Installationsdatei zum Installieren sämtlicher Komponenten von Horizon Client ausführen.

Dieser Vorgang beschreibt die Installation von Horizon Client über einen interaktiven Installationsassistenten. Erläuterungen zur Installation von Horizon Client über die Befehlszeile finden Sie unter Installieren von Horizon Client über die Befehlszeile. Um die Funktion der URL-Inhaltsumleitung installieren zu können, müssen Sie das Installationsprogramm über die Befehlszeile ausführen.

Hinweis Sie können Horizon Client auf der virtuellen Remote-Desktop-Maschine installieren. Unternehmen können diese Art der Installation verwenden, wenn ihre Endbenutzer auf veröffentlichte Anwendungen von Windows-Thin Client-Geräten aus zugreifen.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe Systemanforderungen für Windows-Clientsysteme.
- Stellen Sie sicher, dass Sie über die URL für eine Download-Seite verfügen, auf der sich das Horizon Client-Installationsprogramm befindet. Bei dieser URL kann es sich um die VMware Downloads-Seite unter http://www.vmware.com/go/viewclients oder um die URL für eine Verbindungsserver-Instanz handeln.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Stellen Sie sicher, dass auf den Domänencontrollern die neuesten Patches installiert sind, dass genügend freier Festplattenspeicher zur Verfügung steht und dass eine Kommunikation untereinander möglich ist.
- Wenn Sie Horizon Client mit FIPS-konformer Kryptografie installieren möchten, aktivieren Sie den FIPS-Modus im Clientbetriebssystem. Siehe Aktivieren des FIPS-Modus im Windows-Clientbetriebssystem.
- Wenn Sie das IPv6-Protokoll auswählen möchten oder sich für eine automatische Auswahl des Internetprotokolls entscheiden, finden Sie im Dokument *Horizon-Installation* Informationen zu Funktionen, die in einer IPv6-Umgebung nicht verfügbar sind.
- Wenn Sie die automatische Auswahl des Internetprotokolls aktivieren möchten, finden Sie unter Aktivieren der automatischen Auswahl des Internetprotokolls Informationen zu den unterstützten Funktionen.

- Wenn Sie die Komponente für die **USB-Umleitung** installieren möchten, führen Sie folgende Aufgaben durch:
  - Legen Sie fest, ob der Benutzer des Clientgeräts von einem Remote-Desktop auf lokal verbundene USB-Geräte zugreifen darf. Wenn der Zugriff nicht zulässig ist, installieren Sie entweder die Komponente der **USB-Umleitung** nicht oder Sie installieren die Komponente und deaktivieren diese mithilfe einer Gruppenrichtlinieneinstellung. Wenn Sie eine Gruppenrichtlinie zur Deaktivierung der USB-Umleitung verwenden, müssen Sie Horizon Client nicht erneut installieren, wenn Sie die USB-Umleitung später für einen Client aktivieren möchten. Weitere Informationen finden Sie unter Einstellungen für die Skriptdefinition für Client-GPOs.
  - Stellen Sie sicher, dass die Funktion für automatische Windows-Updates auf dem Clientcomputer nicht deaktiviert wurde.
- Legen Sie fest, ob diese Funktion verwendet werden soll, mit der Endbenutzer sich bei Horizon Client und ihrem Remote-Desktop als aktuell angemeldeter Benutzer anmelden können. Die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung beim Clientsystem eingegeben hat, werden an die Verbindungsserver-Instanz und schließlich an den Remote-Desktop übergeben. Einige Clientbetriebssysteme bieten keine Unterstützung für diese Funktion.
- Wenn Sie nicht möchten, dass Endbenutzer den vollqualifizierten Domänennamen (FQDN) der Verbindungsserverinstanz eingeben müssen, ermitteln Sie den FQDN, um ihn während der Installation angeben zu können.

Verfahren

1. Melden Sie sich beim Clientsystem als Administrator an.
2. Wechseln Sie zur VMware-Download-Seite unter http://www.vmware.com/go/viewclients.
3. Laden Sie die Installationsdatei herunter, z. B. `VMware-Horizon-Client-`*`YYMM`*`-`*`y.y.y`*`-`*`xxxxxx`*`.exe`.

   YYMM ist die Marketingversionsnummer, *y.y.y* ist die interne Versionsnummer, und *xxxxxx* ist die Build-Nummer.
4. Doppelklicken Sie auf die Installationsdatei, um die Installation zu starten.

5 Wählen Sie einen Installationstyp aus und folgen Sie den Aufforderungen.

Option	Aktion
Standardinstallation	Klicken Sie auf **Akzeptieren und Installieren**. Das Installationsprogramm konfiguriert den Client für die Verwendung des IPv4-Internetprotokolls und installiert folgende Funktionen: ■ USB-Umleitung ■ Melden Sie sich als aktueller Benutzer an, einschließlich der Anzeige der Menüoption **Als aktueller Benutzer anmelden**. ■ Virtualization Pack für Skype for Business ■ Unterstützung für HTML5 Multimedia-Umleitung und Browser-Umleitung ■ Medienoptimierung für Microsoft Teams
Benutzerdefinierte Installation	Klicken Sie auf die Option **Installation anpassen** und wählen Sie die Funktionen aus, die installiert werden sollen. Sie müssen diese Option auswählen, um die folgenden Funktionen anzugeben: ■ Einen nicht standardmäßigen Installationsort angeben. ■ Das IPv6-Internetprotokoll verwenden. ■ Die automatische Auswahl des Internetprotokolls aktivieren. Horizon Client prüft das aktuelle Netzwerk und stellt die Verbindung automatisch über IPv4 oder IPv6 her. ■ Eine standardmäßige Verbindungsserver-Instanz konfigurieren. ■ Das standardmäßige Anmeldeverhalten auf **Als aktueller Benutzer anmelden** festlegen. ■ FIPS-konforme Kryptografie aktivieren. Die Optionen der benutzerdefinierten Installation für die FIPS-konforme Kryptografie sind im Installationsprogramm nur verfügbar, wenn der FIPS-Modus auf dem Clientbetriebssystem aktiviert ist. ■ Die Komponente „32-Bit-Core Remote Experience“ auf einem 64-Bit-Computer installieren. **Hinweis** Installieren Sie die 32-Bit-Core Remote Experience-Komponente, wenn der 64-Bit-Clientcomputer nicht über 64-Bit-Plug-Ins für das Produkt verfügt. Die Funktion „Medienoptimierung für Microsoft Teams“ wird mit der 32-Bit-Core Remote Experience-Komponente nicht unterstützt.

Ergebnisse

Für einige Funktionen müssen Sie das Clientsystem neu starten.

Das Installationsprogramm installiert Windows-Dienste wie VMware Horizon Client (`horizon_client_service`) und VMware USB Arbitration Service (`VMUSBArbService`).

Nächste Schritte

Starten Sie Horizon Client und stellen Sie sicher, dass Sie sich beim richtigen Remote-Desktop bzw. bei der richtigen veröffentlichten Anwendung anmelden können. Siehe Verbindung zu einem Remote-Desktop oder einer veröffentlichten Anwendung herstellen.

Installieren von Horizon Client über die Befehlszeile

Sie können für die Installation von Horizon Client den Namen der Installationsdatei, die Installationsbefehle sowie die gewünschten Installationseigenschaften an der Befehlszeile eingeben.

Wenn Sie Horizon Client über die Befehlszeile installieren, können Sie auch eine unbeaufsichtigte Installation durchführen. Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von Horizon Client in einem großen Unternehmen.

Installationsbefehle für Horizon Client

Wenn Sie Horizon Client über die Befehlszeile installieren, können Sie bestimmte Befehle für Installation angeben.

Die folgende Tabelle beschreibt die Installationsbefehle für Horizon Client.

Tabelle 2-1. Installationsbefehle für Horizon Client

Befehl	Beschreibung
/? oder `/help`	Listet die Installationsbefehle und -eigenschaften für Horizon Client auf.
`/silent`	Installiert Horizon Client unbeaufsichtigt. Sie müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.
`/install`	Horizon Client installiert interaktiv. Sie müssen den Eingabeaufforderungen des Assistenten folgen.
`/uninstall`	Deinstalliert Horizon Client.
`/repair`	Repariert Horizon Client.
`/norestart`	Unterdrückt alle Neustarts und Neustartaufforderungen bei der Installation.
`/x /extract`	Extrahiert die Pakete des Installationsprogramms in das Verzeichnis `% TEMP %`.
`/l` oder `/log`	Gibt einen Ordner und ein Namensmuster für die Installationsprotokolldateien an. Wenn Sie beispielsweise den folgenden Befehl angeben, erstellt das Installationsprogramm Horizon Client Protokolldateien mit dem Präfix `Test` im Ordner `C:\Temp`. `/log "C:\Temp\Test"`

Installationseigenschaften für Horizon Client

Wenn Sie Horizon Client über die Befehlszeile installieren, können Sie bestimmte Eigenschaften für die Installation festlegen.

Die folgende Tabelle beschreibt die Installationseigenschaften von Horizon Client.

Tabelle 2-2. Horizon Client-Installationseigenschaften

Eigenschaft	Beschreibung	Standard
INSTALLDIR	Pfad und Ordner für die Installation von Horizon Client. Beispiel: `INSTALLDIR=""D:\abc\my folder""` Die doppelten Anführungszeichen, die den Pfad umschließen, ermöglichen es dem Installationsprogramm, das Leerzeichen als gültigen Teil des Pfades zu interpretieren.	`%ProgramFiles%VMware\VMware Horizon View Client`
VDM_IP_PROTOCOL_USAGE	IP-(Internetprotokoll-)Version, die Horizon Client-Komponenten für die Kommunikation verwenden. Folgende Werte sind gültig: ■ IPv4 ■ IPv6 ■ Dual Wenn Sie „Dual“ angeben, prüft Horizon Client das aktuelle Netzwerk und stellt die Verbindung automatisch über IPv4 oder IPv6 her.	IPv4
VDM_FIPS_ENABLED	Bestimmt, ob Horizon Client mit der FIPS-konformen Kryptografie installiert wird. Mit dem Wert 1 wird Horizon Client mit FIPS-konformer Kryptografie installiert. Mit dem Wert 0 wird Horizon Client ohne FIPs-konforme Kryptografie installiert. **Hinweis** Bevor Sie diese Eigenschaft auf 1 festlegen, müssen Sie den FIPS-Modus im Windows-Clientbetriebssystem aktivieren. Siehe Aktivieren des FIPS-Modus im Windows-Clientbetriebssystem.	0
VDM_SERVER	Der vollqualifizierte Domänenname (FQDN) der Verbindungsserver-Instanz, mit der Horizon Client-Benutzer standardmäßig eine Verbindung herstellen. Beispiel: `VDM_Server=cs1.companydomain.com` Wenn Sie diese Eigenschaft konfigurieren, müssen Horizon Client-Benutzer diesen FQDN nicht angeben.	Keine
LOGINASCURRENTUSER_DISPLAY	Legt fest, ob die Option **Als aktueller Benutzer anmelden** im Menü **Optionen** der Horizon Client-Menüleiste angezeigt wird. Gültige Werte sind 1 (aktiviert) oder 0 (deaktiviert).	1

Tabelle 2-2. Horizon Client-Installationseigenschaften (Fortsetzung)

Eigenschaft	Beschreibung	Standard
LOGINASCURRENTUSER_DEFAULT	Legt fest, ob die Option **Als aktueller Benutzer anmelden** im Menü **Optionen** der Horizon Client-Menüleiste standardmäßig ausgewählt ist. Gültige Werte sind 1 (aktiviert) und 0 (deaktiviert). Wenn „Als aktueller Benutzer anmelden“ als Standardverhalten für die Anmeldung festgelegt ist, werden die Identitäts- und Anmeldeinformationen, die Benutzer bei der Anmeldung beim Clientsystem eingeben, an die Verbindungsserver-Instanz und schließlich an den Remote-Desktop übergeben. Wenn „Als aktueller Benutzer anmelden“ nicht als Standardverhalten für die Anmeldung festgelegt ist, müssen Benutzer die Identitäts- und Anmeldeinformationen mehrfach eingeben, bevor sie auf einen Remote-Desktop oder eine Remoteanwendung zugreifen können.	0
ADDLOCAL	Legt die Funktionen fest, die installiert werden sollen. Folgende Werte sind gültig: ■ ALL – Es werden alle verfügbaren Funktionen mit Ausnahme der URL-Inhaltsumleitung installiert. ■ TSSO – Es wird die Funktion „Als aktueller Benutzer anmelden“ installiert. ■ USB – Es wird die USB-Umleitungsfunktion installiert. Geben Sie die einzelnen Funktionen in einer Liste von durch Kommas getrennten Funktionsnamen an. Verwenden Sie zwischen den Namen keine Leerzeichen. Um beispielsweise Horizon Client mit der Funktion der USB-Umleitung, aber ohne die Funktion „Als aktueller Benutzer anmelden“ zu installieren, geben Sie den folgenden Befehl ein: `VMware-Horizon-Client-y.y.y-xxxxxx.exe ADDLOCAL=USB`	Keine

Tabelle 2-2. Horizon Client-Installationseigenschaften (Fortsetzung)

Eigenschaft	Beschreibung	Standard
INSTALL_32BITRMKS	Legt auf einem 64-Bit-Clientcomputer fest, ob die 32-Bit-Core Remote Experience-Komponente installiert wird. Mit dem Wert 1 wird die 32-Bit-Core Remote Experience-Komponente installiert. Mit dem Wert 0 wird die 64-Bit-Core Remote Experience-Komponente installiert. Installieren Sie die 32-Bit-Core Remote Experience-Komponente, wenn der 64-Bit-Clientcomputer nicht über 64-Bit-Plug-Ins für das Produkt verfügt. Diese Eigenschaft kann nicht auf einem 32-Bit-Clientcomputer angewendet werden.	0
INSTALL_SFB	Legt fest, ob das VMware Virtualization Pack für Skype for Business installiert wird. Bei Verwendung des Werts 1 wird die Funktion installiert. Bei Verwendung des Werts 0 wird die Funktion nicht installiert.	1
INSTALL_HTML5MMR	Legt fest, ob die Unterstützung für HTML5-Multimedia- und Browser-Umleitungsfunktion installiert ist. Bei Verwendung des Werts 1 wird die Funktion installiert. Bei Verwendung des Werts 0 wird die Funktion nicht installiert.	1
REMOVE	Legt die Funktionen fest, die nicht installiert werden sollen. Folgende Werte sind gültig: ■ `ThinPrint` – legt fest, dass die Funktion des virtuellen Druckens nicht installiert wird. ■ `Scanner` – legt fest, dass die Funktion der Scannerumleitung nicht installiert wird. ■ `FolderRedirection` – legt fest, dass die Funktion der Ordnerumleitung nicht installiert wird. ■ `SerialPort` – legt fest, dass die Funktion der Umleitung serieller Ports nicht installiert wird. Wenn Sie mehrere Funktionen festlegen möchten, geben Sie diese mit einer Liste von durch Kommas getrennten Funktionsnamen ein. Verwenden Sie zwischen den Namen keine Leerzeichen. Der folgende Befehl installiert beispielsweise nicht die Funktionen des virtuellen Druckens und der Scannerumleitung: `VMware-Horizon-Client-`*`y.y.y-xxxxxx`*`.exe REMOVE=ThinPrint,Scanner`	Keine

Tabelle 2-2. Horizon Client-Installationseigenschaften (Fortsetzung)

Eigenschaft	Beschreibung	Standard
DESKTOP_SHORTCUT	Legt fest, ob eine Desktop-Verknüpfung für Horizon Client erstellt wird. Mit dem Wert 0 wird keine Desktop-Verknüpfung erstellt. Mit dem Wert 1 wird eine Desktop-Verknüpfung erstellt.	1
STARTMENU_SHORTCUT	Legt fest, ob eine Startmenüverknüpfung für Horizon Client erstellt wird. Mit dem Wert 0 wird keine Startmenüverknüpfung erstellt. Mit dem Wert 1 wird eine Startmenüverknüpfung erstellt.	1
URL_FILTERING_ENABLED	Legt fest, ob die Funktion für die URL-Inhaltsumleitung installiert wird. Bei Verwendung des Werts 1 wird die Funktion installiert. Bei Verwendung des Werts 0 wird die Funktion nicht installiert. Wenn Sie in einer interaktiven Installation für diese Eigenschaft 1 festlegen, wird das Kontrollkästchen **URL-Inhaltsumleitung** unter den zusätzlichen Funktionen im Dialogfeld „Benutzerdefinierte Installation“ angezeigt und standardmäßig aktiviert. Das Kontrollkästchen wird nicht angezeigt, solange Sie diese Eigenschaft nicht auf 1 setzen. **Hinweis** Die Eigenschaft ADDLOCAL=ALL umfasst nicht die Funktion der URL-Inhaltsumleitung.	0
AUTO_UPDATE_ENABLED	Legt fest, ob die Funktion für die Onlineaktualisierung aktiviert wird. Bei Verwendung des Werts 1 wird die Funktion aktiviert. Bei Verwendung des Werts 0 wird die Funktion deaktiviert. Weitere Informationen finden Sie unter Onlineaktualisierung von Horizon Client.	1
INSTALL_TEAMS_REDIRECTION	Bestimmt, ob die Funktion „Medienoptimierung für Microsoft Teams“ aktiviert ist. Bei Verwendung des Werts 1 wird die Funktion aktiviert. Bei Verwendung des Werts 0 wird die Funktion deaktiviert. Weitere Informationen zu dieser Funktion finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*. **Hinweis** Diese Funktion wird für die 32-Bit-Core Remote Experience-Komponente nicht unterstützt.	1

Installieren von Horizon Client über die Befehlszeile

Sie können Horizon Client über die Befehlszeile installieren, indem Sie den Dateinamen des Installationsprogramms eingeben sowie Installationsbefehle und -eigenschaften angeben. Sie können Horizon Client unbeaufsichtigt über die Befehlszeile installieren.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe Systemanforderungen für Windows-Clientsysteme.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Stellen Sie sicher, dass auf den Domänencontrollern die neuesten Patches installiert sind, dass genügend freier Festplattenspeicher zur Verfügung steht und dass eine Kommunikation untereinander möglich ist.
- Wenn Sie Horizon Client mit FIPS-konformer Kryptografie installieren möchten, aktivieren Sie den FIPS-Modus im Clientbetriebssystem. Siehe Aktivieren des FIPS-Modus im Windows-Clientbetriebssystem.
- Legen Sie fest, ob diese Funktion verwendet werden soll, mit der Endbenutzer sich bei Horizon Client und ihrem Remote-Desktop als aktuell angemeldeter Benutzer anmelden können. Die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung beim Clientsystem eingegeben hat, werden an die Verbindungsserver-Instanz und schließlich an den Remote-Desktop übergeben. Einige Clientbetriebssysteme bieten keine Unterstützung für diese Funktion.
- Machen Sie sich mit den Installationsbefehlen von Horizon Client vertraut. Siehe Installationsbefehle für Horizon Client.
- Machen Sie sich mit den Installationseigenschaften von Horizon Client vertraut. Siehe Installationseigenschaften für Horizon Client.
- Legen Sie fest, ob Sie Endbenutzern von ihren Remote-Desktops aus den Zugriff auf lokal angeschlossene USB-Geräte gestatten möchten. Wenn dies nicht der Fall ist, legen Sie die Installationseigenschaft `ADDLOCAL` fest, um die Liste der Funktionen anzuzeigen und die USB-Funktion auszulassen. Weitere Informationen finden Sie unter Installationseigenschaften für Horizon Client.
- Wenn Sie nicht möchten, dass Endbenutzer den vollqualifizierten Domänennamen (FQDN) der Verbindungsserverinstanz eingeben müssen, ermitteln Sie den FQDN, um ihn während der Installation angeben zu können.

Verfahren

1. Melden Sie sich beim Clientsystem als Administrator an.
2. Wechseln Sie zur VMware-Download-Seite unter http://www.vmware.com/go/viewclients.

3 Laden Sie die Horizon Client-Installationsdatei herunter, z. B. `VMware-Horizon-Client-`*`YYMM`*`-`*`y.y.y`*`-`*`xxxxxx`*`.exe`.

   YYMM ist die Marketingversionsnummer, *y.y.y* ist die interne Versionsnummer, und *xxxxxx* ist die Build-Nummer.

4 Öffnen Sie auf dem Windows-Clientcomputer eine Eingabeaufforderung.

5 Geben Sie den Namen der Installationsdatei sowie die Installationsbefehle und -eigenschaften in einer Zeile ein.

   `VMware-Horizon-Client-`*`YYMM-y.y.y-xxxxxx`*`.exe [`*`Befehle`*`] [`*`Eigenschaften`*`]`

Ergebnisse

Das Installationsprogramm installiert Horizon Client gemäß den von Ihnen angegebenen Installationsbefehlen und -eigenschaften. Mit dem Installationsbefehl `/silent` werden keine Aufforderungen des Assistenten angezeigt.

Das Installationsprogramm installiert Windows-Dienste wie VMware Horizon Client (`horizon_client_service`) und VMware USB Arbitration Service (`VMUSBArbService`).

Beispiel: Beispiele für Installationsbefehle

Der folgende Befehl installiert Horizon Client interaktiv und aktiviert die Funktion der URL-Inhaltsumleitung.

```
VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe URL_FILTERING_ENABLED=1
```

Der folgende Befehl installiert Horizon Client unbeaufsichtigt und unterdrückt alle Neustarts und Neustartaufforderungen bei der Installation.

```
VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe /silent /norestart
```

Nächste Schritte

Wenn Sie bei der Installation von Horizon Client die Funktion der URL-Inhaltsumleitung aktiviert haben, prüfen Sie, ob die Funktion installiert ist. Siehe Überprüfen der Installation der URL-Inhaltsumleitung.

Starten Sie Horizon Client und stellen Sie sicher, dass Sie sich beim richtigen Remote-Desktop bzw. bei der richtigen veröffentlichten Anwendung anmelden können. Siehe Verbindung zu einem Remote-Desktop oder einer veröffentlichten Anwendung herstellen.

Überprüfen der Installation der URL-Inhaltsumleitung

Wenn bei der Installation von Horizon Client die Funktion der URL-Inhaltsumleitung aktiviert wurde, müssen Sie prüfen, ob deren Installation erfolgreich war.

Voraussetzungen

Legen Sie bei der Installation von Horizon Client die Installationseigenschaft `URL_FILTERING_ENABLED=1` fest. Siehe Installieren von Horizon Client über die Befehlszeile.

Verfahren

1. Melden Sie sich beim Clientcomputer an.
2. Stellen Sie sicher, dass die Dateien `vmware-url-protocol-launch-helper.exe` und `vmware-url-filtering-plugin.dll` im Verzeichnis `%PROGRAMFILES%\VMware\VMware Horizon View Client\` installiert sind.
3. Stellen Sie sicher, dass das VMware Horizon View URL Filtering-Plugin als Add-on installiert und in Internet Explorer aktiviert wurde.

Onlineaktualisierung von Horizon Client

Sie können Horizon Client online aktualisieren.

Standardmäßig wird ein roter Punkt im Menü **Optionen** (vor der Verbindungsherstellung mit einem Server) und auf der Schaltfläche **Hilfe** (nach der Verbindungsherstellung mit einem Server) angezeigt, um anzugeben, dass eine neue Horizon Client-Version verfügbar ist.

Während des Aktualisierungsvorgangs können Sie standardmäßig das Kontrollkästchen **Nach Updates suchen und Badge-Benachrichtigung anzeigen** aktivieren oder deaktivieren, um festzulegen, ob Horizon Client automatisch nach Updates sucht und die Benachrichtigung über die neue Version anzeigt.

Sie können das Verhalten der Onlineupdateoption steuern, indem Sie die folgenden Gruppenrichtlinieneinstellungen konfigurieren.

- **Onlineaktualisierung von Horizon Client aktivieren**, wodurch die Onlineupdateoption aktiviert oder deaktiviert wird.
- **URL für die Horizon Client-Onlineaktualisierung**, wodurch eine alternative URL angegeben wird, von der Horizon Client Updates abrufen kann.
- **Automatisch nach Updates suchen**, was das Kontrollkästchen **Nach Updates suchen und Badge-Benachrichtigung anzeigen** steuert.
- **Popup-Fenster für Nachrichten aktualisieren**, wodurch das Kontrollkästchen **Popup-Meldung anzeigen, wenn ein Update vorliegt** gesteuert wird. Das Kontrollkästchen **Popup-Meldung anzeigen, wenn ein Update vorliegt** wird nur wirksam, wenn das Kontrollkästchen **Nach Updates suchen und Badge-Benachrichtigung** aktiviert ist.
- **Überspringen der Horizon Client-Aktualisierung durch Benutzer zulassen**, wodurch die Schaltfläche **Überspringen** gesteuert wird.

Vollständige Informationen zu diesen Gruppenrichtlinieneinstellungen finden Sie im Abschnitt Allgemeine Einstellungen für Client-GPOs.

Sie können die Funktion für die Onlineaktualisierung auch durch Festlegung der Eigenschaft `AUTO_UPDATE_ENABLED` auf 0 deaktivieren, wenn Sie Horizon Client über die Befehlszeile installieren. Weitere Informationen finden Sie unter Installationseigenschaften für Horizon Client.

Voraussetzungen

- Speichern Sie vor der Aktualisierung von Horizon Client Ihre Arbeit. Das Update startet eventuell das System neu.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.

Verfahren

1. Melden Sie sich beim Clientsystem als Administrator an.
2. Starten Sie Horizon Client und klicken Sie auf **Software-Updates**.

Option	Aktion
Vor dem Herstellen einer Verbindung mit einem Server	Klicken Sie auf **Optionen > Software-Updates**.
Nach dem Herstellen einer Verbindung mit einem Server	Klicken Sie auf **Hilfe > Software-Updates**.

3. Klicken Sie auf **Auf Updates prüfen**, um festzustellen, ob Aktualisierungen vorhanden sind.

   Horizon Client zeigt an, ob eine Aktualisierung verfügbar ist.
4. Um den Updatevorgang zu starten, wenn eine neue Version verfügbar ist, klicken Sie auf **Herunterladen und installieren**.

   Alternativ können Sie auf **Überspringen** (sofern verfügbar) klicken oder auf **Später erinnern**, um das Update zu einem anderen Zeitpunkt zu installieren. Wenn Sie auf **Überspringen** klicken, wird keine weitere Updatebenachrichtigung angezeigt, bis die nächste Horizon Client-Version verfügbar ist. Sie können nach wie vor auf **Software-Updates** klicken, um manuell auf ein Update zu prüfen.
5. Um das Update zu installieren, nachdem Horizon Client das Update heruntergeladen hat, klicken Sie auf **OK**.

   Der interaktive Installationsassistent von Horizon Client wird geöffnet.

Konfigurieren von Horizon Client für Endbenutzer

3

Die Konfiguration von Horizon Client für Endbenutzer kann verschiedene Aufgaben umfassen, z. B. die Konfiguration von URIs zum Start von Horizon Client, die Konfiguration des Zertifikatsprüfungsmodus, die Festlegung erweiterter TLS-Optionen, die Anpassung von Horizon Client-Menüs sowie die Konfiguration benutzerdefinierter Einstellungen mithilfe von Gruppenrichtlinien.

Dieses Kapitel enthält die folgenden Themen:

Allgemeine Konfigurationseinstellungen

Horizon Client bietet mehrere Konfigurationsmechanismen zur Vereinfachung der Anmeldung und Remote-Desktop-Auswahl und zur Verbesserung der Benutzererfahrung sowie zur Durchsetzung von Sicherheitsrichtlinien.

In der folgenden Tabelle werden nur einige Konfigurationseinstellungen beschrieben, die Sie auf verschiedene Weise festlegen können.

Tabelle 3-1. Allgemeine Konfigurationseinstellungen

Einstellung	Konfigurationsmechanismen
Serveradresse	URI, Gruppenrichtlinie, Befehlszeile, Windows-Registrierung
Active Directory-Benutzername	URI, Gruppenrichtlinie, Befehlszeile, Windows-Registrierung
Domänenname	URI, Gruppenrichtlinie, Befehlszeile, Windows-Registrierung
Remote-Desktop-Anzeigename	URI, Gruppenrichtlinie, Befehlszeile
Fenstergröße	URI, Gruppenrichtlinie, Befehlszeile
Anzeigeprotokoll	URI, Befehlszeile
Konfigurieren der Zertifikatsprüfung	Gruppenrichtlinie, Windows-Registrierung
Konfigurieren von TLS-Protokollen und kryptografischen Algorithmen	Gruppenrichtlinie, Windows-Registrierung

Verwenden von URIs zur Konfiguration von Horizon Client

Sie können Uniform Resource Identifiers (URIs) verwenden, um Webseiten- oder E-Mail-Links zu erstellen, auf die Endbenutzer klicken können, um Horizon Client zu starten, eine Verbindung zu einem Server herzustellen oder einen Remote-Desktop bzw. eine veröffentlichte Anwendung zu öffnen.

Diese Links werden durch die Generierung von URIs erstellt, die einige oder alle der folgenden Informationen bereitstellen, sodass die Endbenutzer diese nicht angeben müssen.

- Serveradresse
- Portnummer für den Server
- Active Directory-Benutzername
- RADIUS- oder RSA SecurID-Benutzername, wenn dieser nicht mit dem Active Directory-Benutzernamen identisch ist
- Domänenname
- Anzeigename des Remote-Desktops oder der veröffentlichten Anwendung
- Fenstergröße
- Aktionen, darunter „Zurücksetzen“, „Abmelden“ und „Sitzung starten“
- Anzeigeprotokoll
- Optionen zur Umleitung von USB-Geräten

Verwenden Sie zur Generierung eines URI das URI-Schema `vmware-view` mit Horizon Client-spezifischen Pfad- und Abfragekomponenten.

Um URIs zum Start von Horizon Client zu verwenden, muss Horizon Client bereits auf den Client Computern installiert sein.

Syntax für die Erstellung von vmware-view-URIs

Die URI-Syntax umfasst das URI-Schema `vmware-view`, einen Pfadauszug zur Angabe des Remote-Desktops oder der veröffentlichten Anwendung sowie optional eine Abfrage zur Angabe von Aktionen oder Konfigurationsoptionen für den Remote-Desktop oder die veröffentlichte Anwendung.

URI-Spezifikation

Verwenden Sie zum Generieren von URIs für den Start von Horizon Client die folgende Syntax.

```
vmware-view://[authority-part][/path-part][?query-part]
```

Das einzig erforderliche Element ist das URI-Schema `vmware-view`. Da der Schemaname für einige Versionen bestimmter Clientbetriebssysteme die Groß-/Kleinschreibung beachtet, geben Sie `vmware-view` ein.

Wichtig In allen Abschnitten müssen Nicht-ASCII-Zeichen zunächst gemäß UTF-8 [STD63] codiert werden, anschließend muss für jedes Oktett der entsprechenden UTF-8-Sequenz eine Prozentcodierung durchgeführt werden, um diese als URI-Zeichen darzustellen.

Informationen zur Codierung von ASCII-Zeichen finden Sie in der URL-Codierungsreferenz unter http://www.utf8-chartable.de/.

authority-part

Die Serveradresse und optional ein Benutzername, eine nicht standardmäßige Portnummer oder beides. Unterstriche (_) werden in Servernamen nicht unterstützt. Die Servernamen müssen der DNS-Syntax entsprechen.

Verwenden Sie zur Angabe eines Benutzernamens die folgende Syntax.

```
user1@server-address
```

Sie können keine UPN-Adresse angeben, auch keine Domäne. Zur Angabe des Domänennamens können Sie den Abfrageteil `domainName` im URI verwenden.

Verwenden Sie zur Angabe einer Portnummer die folgende Syntax.

```
server-address:port-number
```

path-part

Der Anzeigename des Remote-Desktops oder der veröffentlichten Anwendung. Der Anzeigename wird in Horizon Console angegeben, wenn der Desktop- oder der Anwendungspool erstellt wird. Wenn der Anzeigename ein Leerzeichen enthält, verwenden Sie den Codierungsmechanismus **`%20`**, um das Leerzeichen darzustellen.

Alternativ können Sie eine Desktop-ID oder eine Anwendungs-ID angeben, bei der es sich um eine Pfadangabe einschließlich der Desktop-ID oder der Anwendungspool-ID handelt. Um eine Desktop- oder Anwendungs-ID aufzufinden, öffnen Sie den ADSI-Editor auf dem

Verbindungsserver-Host, navigieren Sie zu `DC=vdi,dc=vmware,dc=int` und wählen Sie den Knoten `OU=Applications` aus. Alle Desktop- und Anwendungspools werden aufgelistet. Das Attribut `distinguishedName` legt den ID-Wert fest. Sie müssen den ID-Wert kodieren, bevor Sie ihn in einem URI angeben, z. B. `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`.

Wenn Sie eine Desktop- oder Anwendungs-ID angeben, dürfen Sie nur Kleinbuchstaben verwenden, auch wenn die Desktop- oder Anwendungs-ID Großbuchstaben in ADSI Edit enthält.

Hinweis Mehrere Remote-Desktops oder veröffentlichte Anwendungen können denselben Anzeigenamen besitzen. Desktop- und Anwendungs-ID sind jedoch eindeutig. Wenn Sie einen bestimmten Remotedesktop oder eine bestimmte veröffentlichte Anwendung angeben müssen, verwenden Sie anstelle des Anzeigenamens die Desktop-ID oder die Anwendungs-ID.

query-part

Die zu verwendenden Konfigurationsoptionen oder auszuführende Aktionen für den Remote-Desktop oder die veröffentlichte Anwendung. Für die Abfragen muss die Groß- und Kleinschreibung nicht beachtet werden. Verwenden Sie für den Einsatz mehrerer Abfragen das kaufmännische Und-Zeichen (&) zwischen den Abfragen. Wenn die Abfragen in Konflikt stehen, verwendet Horizon Client die letzte Abfrage in der Liste. Verwenden Sie die folgende Syntax.

```
query1=value1[&query2=value2...]
```

Unterstützte Abfragen

Die folgenden Abfragen werden für diesen Horizon Client-Typ unterstützt. Wenn Sie URIs für mehrere Arten von Clients erstellen, wie z. B. Desktop-Clients und mobile Clients, finden Sie die Liste der unterstützten Abfragen im Installations- und Einrichtungshandbuch für jede Art von Clientsystem.

action

Tabelle 3-2. Werte, die mit der Abfrage „action“ verwendet werden können

Wert	Beschreibung
`browse`	Zeigt eine Liste der verfügbaren Remote-Desktops und veröffentlichten Anwendungen an, die auf dem angegebenen Server gehostet werden. Bei Verwendung dieser Aktion müssen Sie keinen Remote-Desktop bzw. keine veröffentlichte Anwendung angeben.
`start-session`	Öffnet den angegebenen Remote-Desktop oder die angegebene veröffentlichte Anwendung. Wenn keine „action“-Abfrage bereitgestellt wird und der Name des Remote-Desktops oder der veröffentlichten Anwendung angegeben wird, ist `start-session` die Standardaktion.

Tabelle 3-2. Werte, die mit der Abfrage „action“ verwendet werden können (Fortsetzung)

Wert	Beschreibung
`reset`	Fährt den angegebenen Remote-Desktop bzw. die angegebene veröffentlichte Anwendung herunter und startet ihn bzw. sie neu. Nicht gespeicherte Daten gehen verloren. Das Zurücksetzen eines Remote-Desktops entspricht dem Betätigen der Reset-Taste auf einem physischen PC.
`restart`	Fährt den angegebenen Remote-Desktop herunter und startet ihn neu. Der Neustart eines Remote-Desktops entspricht dem Neustartbefehl für das Windows-Betriebssystem. In der Regel wird der Benutzer dabei vom Betriebssystem aufgefordert, alle nicht gespeicherten Daten zu speichern, bevor der Neustart erfolgt.
`logoff`	Meldet den Benutzer vom Gastbetriebssystem auf dem Remote-Desktop ab. Wenn Sie eine veröffentlichte Anwendung angeben, wird die Aktion ignoriert, oder der Endbenutzer sieht die Warnmeldung „Ungültige URI-Aktion“.

args

Gibt Befehlszeilenargumente zum Hinzufügen an, wenn die veröffentlichte Anwendung gestartet wird. Verwenden Sie die Syntax `args=`*Wert*, wobei *Wert* eine Zeichenfolge sein muss. Verwenden Sie für die folgenden Zeichen die Prozentkodierung:

- Für einen Doppelpunkt (:) verwenden Sie **`%3A`**.
- Für einen umgekehrten Schrägstrich (\) verwenden Sie **`%5C`**.
- Für ein Leerzeichen ( ) verwenden Sie **`%20`**.
- Für ein doppeltes Anführungszeichen (") verwenden Sie **`%22`**

Um beispielsweise den Dateinamen "`My new file.txt`" für die Notepad++-Anwendung anzugeben, verwenden Sie **`%22My%20new%20file.txt%22`**.

appProtocol

Gültige Werte für veröffentlichte Anwendungen sind **`PCOIP`** und **`BLAST`**. Zur Angabe von PCoIP verwenden Sie beispielsweise die Syntax **`appProtocol=PCOIP`**.

connectUSBOnInsert

Verbindet ein USB-Gerät beim Anschließen des Geräts mit dem im Vordergrund angezeigten Remote-Desktop bzw. der veröffentlichten Anwendung. Diese Abfrage wird bedingungslos festgelegt, wenn Sie die Abfrage `unattended` für einen Remote-Desktop angeben. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf **`start-session`** setzen oder ohne die Abfrage `action` arbeiten. Gültige Werte sind **`true`** und **`false`**. Ein Beispiel für die Syntax ist etwa **`connectUSBOnInsert=true`**.

connectUSBOnStartup

Leitet alle aktuell mit dem Clientsystem verbundenen USB-Geräte an den Remote-Desktop bzw. die veröffentlichte Anwendung um. Diese Abfrage wird bedingungslos festgelegt, wenn Sie die Abfrage `unattended` für einen Remote-Desktop angeben. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf **`start-session`** setzen oder ohne die Abfrage

`action` arbeiten. Gültige Werte sind **`true`** und **`false`**. Ein Beispiel für die Syntax ist etwa **`connectUSBOnStartup=true`**.

desktopLayout

Legt die Größe des Remote-Desktop-Fensters fest. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf **`start-session`** setzen oder die Abfrage `action` nicht verwenden.

Tabelle 3-3. Gültige Werte für desktopLayout-Abfrage

Wert	Beschreibung
`fullscreen`	Vollbild auf einem Monitor. Dieser Wert ist der Standardwert.
`multimonitor`	Vollbild auf allen Monitoren.
`windowLarge`	Großes Fenster.
`windowSmall`	Kleines Fenster.
WxH	Benutzerdefinierte Auflösung, bei der Sie die Breite mal Höhe in Pixel angeben. Ein Beispiel für die Syntax ist etwa **`desktopLayout=1280x800`**.

desktopProtocol

Gültige Werte für Remote-Desktops sind **`RDP`**, **`PCOIP`** und **`BLAST`**. Zur Angabe von PCoIP verwenden Sie beispielsweise die Syntax **`desktopProtocol=PCOIP`**.

domainName

Gibt den NETBIOS-Domänennamen an, der mit dem Benutzer verknüpft ist, der eine Verbindung zum Remote-Desktop bzw. zur veröffentlichten Anwendung herstellt. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.

filePath

Gibt den Pfad zur Datei im lokalen System an, die Sie mit einer veröffentlichten Anwendung öffnen möchten. Sie müssen den vollständigen Pfad einschließlich des Laufwerksbuchstabens eingeben. Verwenden Sie für die folgenden Zeichen die Prozentkodierung:

- Für einen Doppelpunkt (:) verwenden Sie **`%3A`**.
- Für einen umgekehrten Schrägstrich (\) verwenden Sie **`%5C`**.
- Für ein Leerzeichen ( ) verwenden Sie **`%20`**.

Um beispielsweise den Dateipfad `C:\test file.txt` darzustellen, verwenden Sie **`C%3A%5Ctest%20file.txt`**.

launchMinimized

Startet Horizon Client im minimierten Modus. Horizon Client bleibt minimiert, bis der angegebene Remote-Desktop oder die angegebene veröffentlichte Anwendung gestartet wird. Die Syntax lautet **`launchMinimized=true`**. Sie können diese Abfrage nicht mit der **unbeaufsichtigten** Abfrage verwenden.

tokenUserName

Gibt den RSA- oder RADIUS-Benutzernamen an. Verwenden Sie diese Abfrage nur, wenn der RSA- oder RADIUS-Benutzername nicht mit dem Active Directory-Benutzernamen identisch ist. Wenn Sie diese Abfrage nicht angeben und die RSA- oder RADIUS-Authentifizierung erforderlich ist, verwendet Horizon Client den Windows-Benutzernamen. Die Syntax lautet `tokenUserName=`*`name`*.

unattended

Erstellt eine Serververbindung zu einem Remote-Desktop im Kioskmodus. Wenn Sie diese Abfrage verwenden, geben Sie keine Benutzerinformationen an, wenn Sie den Kontonamen aus der MAC-Adresse des Clientgeräts generiert haben. Wenn Sie benutzerdefinierte Kontonamen in ADAM generiert haben, z. B. Namen, die mit „custom-“ beginnen, müssen Sie die Kontoinformationen angeben.

useExisting

Wenn für diese Option **`True`** festgelegt ist, kann nur eine Horizon Client-Instanz ausgeführt werden. Wenn Benutzer eine Verbindung zu einem zweiten Server herstellen möchten, müssen sie sich vom ersten Server abmelden, damit die Sitzungen mit Remote-Desktops und veröffentlichten Anwendungen getrennt werden. Ist für diese Option **`False`** festgelegt, können mehrere Horizon Client-Instanzen ausgeführt werden und die Benutzer haben die Möglichkeit, mit mehreren Servern gleichzeitig eine Verbindung herzustellen. Die Standardeinstellung ist **`True`**. Ein Beispiel für die Syntax ist etwa **`useExisting=false`**.

unauthenticatedAccessEnabled

Wenn für diese Option **`True`** festgelegt ist, ist die Funktion für den nicht authentifizierten Zugriff standardmäßig aktiviert. Die Option **Anonym mit nicht authentifiziertem Zugriff anmelden** ist dann in der Benutzeroberfläche verfügbar und aktiviert. Wenn für diese Option **`False`** festgelegt ist, ist die Funktion für den nicht authentifizierten Zugriff deaktiviert. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** ist dann ausgeblendet und deaktiviert. Wenn für diese Option **""** festgelegt ist, ist die Funktion für den nicht authentifizierten Zugriff deaktiviert. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** ist dann nicht mehr in der Benutzeroberfläche verfügbar und deaktiviert. Ein Beispiel für die Syntax ist etwa **`unauthenticatedAccessEnabled=true`**.

unauthenticatedAccessAccount

Wenn die Funktion für nicht authentifizierten Zugriff aktiviert ist, legt dies das zu verwendende Konto fest. Wenn der nicht authentifizierte Zugriff deaktiviert ist, wird diese Abfrage ignoriert. Die entsprechende Syntax lautet beispielsweise bei Verwendung des Benutzerkontos **`anonymous1`** dann **`unauthenticatedAccessAccount=anonymous1`**.

Beispiele für vmware-view-URIs

Sie können das URI-Schema `vmware-view` verwenden, um Hypertext-Links oder Schaltflächen zu erstellen und diese Links in E-Mails oder Webseiten aufzunehmen. Beispielsweise kann ein

Endbenutzer auf einen URI-Link klicken, um einen Remote-Desktop mit den angegebenen Startoptionen zu starten.

URI-Syntaxbeispiele

Nach jedem URI-Beispiel finden Sie eine Beschreibung, was der Endbenutzer nach Anklicken des URI-Links sieht.

1 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session`

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Das Anmeldedialogfeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Remote-Desktop her, dessen Anzeigename `Primary Desktop` lautet. Der Benutzer wird dann beim Gastbetriebssystem angemeldet.

Hinweis In diesem Beispiel werden das Standardanzeigeprotokoll und die Standardfenstergröße verwendet. Das Standardanzeigeprotokoll ist PCoIP, und die Standardfenstergröße ist Vollbild.

2 `vmware-view://view.mycompany.com/cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Das Anmeldedialogfeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung mit dem Remote-Desktop her, der die Desktop-ID `CN=win7-32,OU=Applications,DC=vdi,DC=vmware,DC=int` (kodierter Wert `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`) besitzt.

3 `vmware-view://view.mycompany.com:7555/Primary%20Desktop`

Dieser URI hat die gleiche Wirkung wie im vorherigen Beispiel, außer dass er den nicht standardmäßigen Port 7555 für die Verbindungsserverinstanz verwendet. (Der standardmäßige Port lautet 443.) Da ein Remote-Desktop-Bezeichner bereitgestellt wird, wird der Remote-Desktop geöffnet, obwohl die Aktion `start-session` nicht im URI enthalten ist.

4 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCOIP`

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Im Anmeldedialogfeld wird das Textfeld **Benutzername** mit dem Namen `fred` gefüllt. Der Benutzer muss den Domänennamen und das Kennwort eingeben. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Remote-Desktop her, dessen Anzeigename `Finance Desktop` lautet. Der Benutzer wird dann beim Gastbetriebssystem angemeldet. Die Verbindung nutzt das PCoIP-Anzeigeprotokoll.

5 `vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST`

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. In das Anmeldedialogfeld muss der Benutzer den Benutzernamen, den Domänennamen und das Kennwort eingeben. Nach einer erfolgreichen Anmeldung verbindet sich der Client mit der veröffentlichten Anwendung mit dem Anzeigenamen `Calculator`. Die Verbindung nutzt das VMware Blast-Anzeigeprotokoll.

6 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Im Anmeldedialogfeld wird das Textfeld **Benutzername** mit dem Namen `fred` und das Textfeld **Domäne** mit `mycompany` gefüllt. Der Benutzer muss das Kennwort eingeben. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Remote-Desktop her, dessen Anzeigename `Finance Desktop` lautet. Der Benutzer wird dann beim Gastbetriebssystem angemeldet.

7 `vmware-view://view.mycompany.com/`

Horizon Client startet und der Benutzer wird zur Anmeldeaufforderung für die Verbindung mit dem Server `view.mycompany.com` geleitet.

8 `vmware-view://view.mycompany.com/Primary%20Desktop?action=reset`

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Das Anmeldedialogfeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung zeigt Horizon Client ein Dialogfeld an, in dem der Benutzer aufgefordert wird, das Zurücksetzen für `Primary Desktop` zu bestätigen.

Hinweis Diese Aktion ist nur möglich, wenn ein Horizon-Administrator die Funktion zum Zurücksetzen für den Remote-Desktop aktiviert hat.

9 `vmware-view://view.mycompany.com/Primary%20Desktop?action=restart`

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Das Anmeldedialogfeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung zeigt Horizon Client ein Dialogfeld an, in dem der Benutzer aufgefordert wird, den Neustart für `Primary Desktop` zu bestätigen.

Hinweis Diese Aktion ist nur möglich, wenn ein Horizon-Administrator die Neustartfunktion für den Remote-Desktop aktiviert hat.

10 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session&connectUSBOnStartup=true`

Dieser URI hat die gleiche Wirkung wie das erste Beispiel, und alle an das Clientsystem angeschlossenen USB-Geräte werden an den Remote-Desktop umgeleitet.

11 `vmware-view://`

Wenn Horizon Client nicht ausgeführt wird, wird er gestartet. Wenn Horizon Client bereits ausgeführt wird, wird es im Vordergrund angezeigt.

12
```
vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22
```

Startet My Notepad++ auf dem Server 10.10.10.10 und übergibt das Argument `My new file.txt` an den Befehl zum Start der veröffentlichten Anwendung. Für Leerzeichen und doppelte Anführungszeichen gilt die Prozentkodierung. Der Dateiname ist in doppelte Anführungszeichen gesetzt, da er Leerzeichen enthält.

Sie können diesen Befehl auch in der Windows-Befehlszeile mit der folgenden Syntax eingeben:

```
vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""
```

In diesem Beispiel werden doppelte Anführungszeichen durch die Zeichen \" kodiert.

13
```
vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt
```

Startet Notepad++ 12 auf dem Server 10.10.10.10 und übergibt das Argument `a.text b.txt` an den Befehl zum Start der veröffentlichten Anwendung. Da dieses Argument nicht in Anführungszeichen gesetzt ist, trennt ein Leerzeichen die Dateinamen und die beiden Dateien werden gesondert in Notepad++ geöffnet.

Hinweis Veröffentlichte Anwendungen können sich in der Umsetzung von Befehlszeilenargumenten unterscheiden. Wenn Sie beispielsweise das Argument `a.txt b.txt` an WordPad übergeben, öffnet WordPad nur eine Datei, `a.txt`.

14
```
vmware-view://view.mycompany.com/Notepad?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous1
```

Horizon Client startet und stellt mithilfe des Benutzerkontos **`anonymous1`** eine Verbindung mit dem `view.mycompany.com`-Server her. Die Anwendung „Editor“ wird ohne Aufforderung des Benutzers zur Eingabe seiner Anmeldedaten gestartet.

Beispiel für HTML-Code

Sie können URIs verwenden, um Hypertext-Links und Schaltflächen zu erstellen, die in E-Mails oder auf Webseiten eingebunden werden können. Die folgenden Beispiele veranschaulichen, wie Sie den URI aus dem ersten Beispiel verwenden, um einen Hypertext-Link mit dem Text **Test Link** und eine Schaltfläche mit dem Text **TestButton** zu codieren.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>
```

```
</body>
</html>
```

Festlegen des Zertifikatsprüfungsmodus in Horizon Client

Serverzertifikatsprüfungen werden für Verbindungen zwischen Horizon Client und einem Server durchgeführt. Ein Zertifikat ist eine digitale Identifikationsmethode, die wie ein Pass oder Führerschein funktioniert.

Die Serverzertifikatsprüfung umfasst die folgenden Prüfungen:

- Wurde das Zertifikat widerrufen?
- Ist das Zertifikat für einen anderen Zweck bestimmt als für die Überprüfung der Identität des Absenders und die Verschlüsselung der Serverkommunikation? Mit anderen Worten: Handelt es sich um den korrekten Zertifikattyp?
- Ist das Zertifikat abgelaufen oder erst zukünftig gültig? Mit anderen Worten: Ist das Zertifikat laut Computeruhr gültig?
- Stimmt der allgemeine Name auf dem Zertifikat mit dem Hostnamen des Servers überein, der es sendet? Zu einer fehlenden Übereinstimmung kann es kommen, wenn ein Lastenausgleich Horizon Client an einen Server mit einem Zertifikat umleitet, das nicht mit dem in Horizon Client eingegebenen Hostnamen übereinstimmt. Ein weiterer möglicher Grund für eine fehlende Übereinstimmung ist die Eingabe einer IP-Adresse statt eines Hostnamens im Client.
- Ist das Zertifikat von einer unbekannten oder nicht als vertrauenswürdig eingestuften Zertifizierungsstelle (CA) signiert worden? Selbstsignierte Zertifikate sind ein Typ der nicht als vertrauenswürdig eingestuften CA. Um diese Prüfung zu bestehen, muss sich das Stammzertifikat für die Zertifikatvertrauenskette im lokalen Zertifikatspeicher des Geräts befinden.

Informationen zur Verteilung eines selbstsignierten Stammzertifikats an alle Windows-Clientsysteme in einer Domäne finden Sie unter „Stammzertifikat zu den vertrauenswürdigen Zertifizierungsstellen hinzufügen“ im Dokument *Horizon-Installation*.

Zum Festlegen des Zertifikatsprüfungsmodus starten Sie Horizon Client und wählen Sie im Menü **Optionen** auf der Horizon Client-Menüleiste **SSL konfigurieren**. Sie können eine der folgenden Optionen auswählen:

- **Nie mit nicht vertrauenswürdigen Servern verbinden**. Diese Einstellung bedeutet, dass Sie keine Verbindung mit dem Server herstellen können, wenn eine der Zertifikatprüfungen fehlschlägt. Die nicht bestandenen Prüfungen werden in einer Fehlermeldung aufgelistet.
- **Warnung vor Verbindung mit nicht vertrauenswürdigen Servern ausgeben**. Diese Einstellung bedeutet, dass Sie auf **Weiter** klicken können, um die Warnung zu ignorieren, wenn eine Zertifikatsprüfung fehlschlägt, weil der Server ein selbstsigniertes Zertifikat verwendet. Bei selbstsignierten Zertifikaten muss der Zertifikatsname nicht mit dem Servernamen übereinstimmen, den Sie in Horizon Client eingegeben haben. Möglicherweise erhalten Sie auch eine Warnung, wenn das Zertifikat abgelaufen ist.

- **Server-Identitätszertifikate nicht überprüfen**. Mit dieser Einstellung werden Zertifikate nicht überprüft.

Installiert ein Administrator später ein Sicherheitszertifikat von einer vertrauenswürdigen Zertifizierungsstelle, sodass alle Zertifikatsprüfungen bei der Verbindungsherstellung bestanden werden, wird diese vertrauenswürdige Verbindung für diesen speziellen Server vorgemerkt. Legt dieser Server in Zukunft wieder ein selbstsigniertes Zertifikat vor, schlägt die Verbindung fehl. Nachdem ein bestimmter Server ein vollständig überprüfbares Zertifikat vorgelegt hat, muss er dies auch in Zukunft immer so handhaben.

Wichtig Wenn Sie zuvor eine Gruppenrichtlinie verwendet haben, um die Clientsysteme Ihres Unternehmens für die Verwendung einer bestimmten Verschlüsselung zu konfigurieren, wie z. B. die Konfiguration von Gruppenrichtlinieneinstellungen für die Reihenfolge von SSL-Verschlüsselungs-Suites, müssen Sie jetzt eine Horizon Client-Gruppenrichtlinien-Sicherheitseinstellung verwenden. Siehe Sicherheitseinstellungen für Client-GPOs. Alternativ können Sie auch die Registrierungseinstellung `SSLCipherList` auf dem Clientsystem verwenden. Siehe Konfigurieren des Horizon Client mithilfe der Windows-Registrierung.

Sie können den Standardmodus für die Zertifikatsprüfung konfigurieren und verhindern, dass Endbenutzer ihn in Horizon Client ändern. Weitere Informationen finden Sie unter Konfigurieren des Zertifikatsprüfungsmodus für Endbenutzer.

Verwenden eines SSL-Proxy-Servers

Wenn Sie einen SSL-Proxy-Server verwenden, um den von der Clientumgebung an das Internet gesendeten Datenverkehr zu überprüfen, aktivieren Sie die Einstellung **Verbindung über einen SSL-Proxy zulassen**. Diese Einstellung ermöglicht die Zertifikatsprüfung für sekundäre Verbindungen über einen SSL-Proxy-Server und gilt sowohl für Blast Secure Gateway als auch für sichere Tunnelverbindungen. Wenn Sie einen SSL-Proxy-Server verwenden und die Zertifikatsprüfung aktivieren, aber die Einstellung **Verbindung über einen SSL-Proxy zulassen** nicht aktivieren, schlagen Verbindungen aufgrund nicht übereinstimmender Fingerabdrücke fehl. Die Einstellung **Verbindung über einen SSL-Proxy zulassen** ist nicht verfügbar, wenn Sie die Option **Server-Identitätszertifikate nicht verifizieren** aktivieren. Wenn die Option **Server-Identitätszertifikate nicht verifizieren** aktiviert ist, wird das Zertifikat oder der Fingerabdruck von Horizon Client nicht überprüft und ein SSL-Proxy ist immer zulässig.

Mit der Gruppenrichtlinieneinstellung **Konfiguriert das Verhalten der SSL-Proxy-Zertifikatsprüfung des Horizon Client** können Sie konfigurieren, ob die Zertifikatsprüfung für sekundäre Verbindungen über einen SSL-Proxy-Server zugelassen werden soll. Weitere Informationen finden Sie unter Sicherheitseinstellungen für Client-GPOs.

Informationen zum Zulassen von VMware Blast-Verbindungen über einen Proxy-Server finden Sie unter Konfigurieren der VMware Blast-Optionen.

Konfigurieren des Zertifikatsprüfungsmodus für Endbenutzer

Sie können den Zertifikatsprüfungsmodus für Endbenutzer konfigurieren. Sie können beispielsweise festlegen, dass immer die vollständige Überprüfung durchgeführt wird. Die Zertifikatsprüfung wird für TLS-Verbindungen zwischen einem Server und Horizon Client durchgeführt.

Sie können eine der folgenden Zertifikatsprüfungsstrategien für Endbenutzer konfigurieren.

- Endbenutzer dürfen den Zertifikatsprüfungsmodus in Horizon Client auswählen.
- (Keine Überprüfung) Es werden keine Zertifikatsprüfungen durchgeführt.
- (Warnen) Endbenutzer werden gewarnt, wenn der Server ein selbstsigniertes Zertifikat präsentiert. Benutzer können dann selbst entscheiden, ob sie diesen Verbindungstyp zulassen.
- (Volle Sicherheit) Es wird eine vollständige Überprüfung durchgeführt. Die Verbindungen, für die diese Prüfung nicht erfolgreich verläuft, werden abgelehnt.

Wenn Sie einen SSL-Proxy-Server verwenden, um den von der Clientumgebung gesendeten Datenverkehr an das Internet zu überprüfen, können Sie die Zertifikatsprüfung für sekundäre Verbindungen über den SSL-Proxy-Server konfigurieren. Diese Funktion gilt sowohl für Blast Secure Gateway als auch für sichere Tunnelverbindungen. Sie können auch die Verwendung von Proxy-Servern für VMware Blast-Verbindungen zulassen.

Weitere Informationen zu den Arten von Zertifikatsprüfungen, die durchgeführt werden können, finden Sie unter Festlegen des Zertifikatsprüfungsmodus in Horizon Client.

Sie können Horizon Client-Gruppenrichtlinieneinstellungen verwenden, um den Zertifikatsprüfungsmodus festzulegen, die Verwendung von SSL-Proxys zu erlauben, die Verwendung bestimmter kryptografischer Algorithmen und Protokolle zu beschränken, bevor eine verschlüsselte TLS-Verbindung hergestellt wird, und die Proxy-Verwendung für VMware Blast-Verbindungen zu aktivieren. Weitere Informationen dazu finden Sie unter Sicherheitseinstellungen für Client-GPOs und Allgemeine Einstellungen für Client-GPOs.

Wenn Sie den Zertifikatsprüfungsmodus nicht als Gruppenrichtlinie konfigurieren möchten, können Sie die Zertifikatsprüfung durch Hinzufügen des Wertnamens `CertCheckMode` zu einem der folgenden Registrierungsschlüssel auf dem Client Computer aktivieren:

- Für 32-Bit-Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- Für 64-Bit-Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Verwenden Sie die folgenden Werte im Registrierungsschlüssel:

- `0` implementiert `Do not verify server identity certificates`.
- `1` implementiert `Warn before connecting to untrusted servers`.

- 2 implementiert `Never connect to untrusted servers`.

Wenn Sie sowohl die Gruppenrichtlinieneinstellung als auch die Einstellung `CertCheckMode` im Registrierungsschlüssel konfigurieren, hat die Gruppenrichtlinieneinstellung Vorrang vor der Registrierungsschlüsseleinstellung.

Konfigurieren erweiterter TLS-Optionen

Sie können die Sicherheitsprotokolle und kryptografischen Algorithmen auswählen, die zum Verschlüsseln der Kommunikation zwischen Horizon Client und Servern oder zwischen Horizon Client und dem Agent in einem Remote-Desktop verwendet werden.

Diese Sicherheitsoptionen werden auch zur Verschlüsselung des USB-Kanals verwendet.

In der Standardeinstellung verwenden Verschlüsselungs-Suites 128- oder 256-Bit-AES, entfernen anonyme DH-Algorithmen und sortieren anschließend die aktuelle Verschlüsselungsliste nach der Schlüssellänge des Verschlüsselungsalgorithmus.

TLS v1.1 und TLS v1.2 sind standardmäßig aktiviert. SSL v2.0, SSL v3.0 und TLS v1.0 werden nicht unterstützt.

Wenn Sie ein Sicherheitsprotokoll für Horizon Client konfigurieren, das auf dem Server, mit dem sich der Client verbindet, nicht aktiviert ist, tritt ein TLS-Fehler auf, und die Verbindung schlägt fehl.

Wichtig Mindestens eines der Protokolle, das Sie in Horizon Client aktivieren, muss auch auf dem Remote Desktop aktiviert sein. Ansonsten können USB-Geräte nicht zum Remote Desktop umgeleitet werden.

Sie können auf dem Clientsystem entweder eine Gruppenrichtlinien- oder eine Windows-Registrierungseinstellung verwenden, um die Standardverschlüsselungen und -protokolle zu ändern. Informationen zur Verwendung einer Gruppenrichtlinieneinstellung finden Sie unter der Einstellung **Konfigurieren von SSL-Protokollen und kryptografischen Algorithmen** in Sicherheitseinstellungen für Client-GPOs. Weitere Informationen zur Verwendung der Einstellung „SSLCipherList“ in der Windows-Registrierung finden Sie unter Konfigurieren des Horizon Client mithilfe der Windows-Registrierung.

Anpassen der Horizon Client-Menüs

Sie können Horizon Client-Gruppenrichtlinien verwenden, um einige Elemente in bestimmten Menüs der Horizon Client-Benutzeroberfläche zu verbergen.

Allgemeine Informationen zur Verwendung der Horizon Client-Gruppenrichtlinien finden Sie unter Verwenden von Gruppenrichtlinieneinstellungen zum Konfigurieren von Horizon Client.

Ausführliche Informationen zur Verwendung der Gruppenrichtlinien, die die Horizon Client-Menüs steuern, finden Sie in den Beschreibungen der Gruppenrichtlinieneinstellungen **Elemente in Anwendungskontextmenü ausblenden**, **Elemente in Desktop-Kontextmenü ausblenden**, **Elemente in Desktop-Symbolleiste ausblenden**, **Elemente im Taskleistenmenü ausblenden** und **Elemente im Symbolleistenmenü des Clients ausblenden** unter Allgemeine Einstellungen für Client-GPOs.

Anpassen der Horizon Client-Fehlermeldungen

Sie können die Gruppenrichtlinieneinstellung Horizon Client**Benutzerdefinierte Fußzeile für Fehlerbildschirm** verwenden, um benutzerdefinierten Hilfetext an das Ende aller Fehlermeldungen anzufügen, die in der Horizon Client-Benutzeroberfläche angezeigt werden. Beispielsweise kann Ihr Hilfetext Benutzer darauf hinweisen, wie Sie den Helpdesk Ihres Unternehmens kontaktieren können.

Sie müssen eine reine Textdatei (`.txt`) mit dem Hilfetext auf dem lokalen Clientsystem erstellen. Die Textdatei kann bis zu 2.048 Zeichen, einschließlich Steuerzeichen enthalten. Sowohl ANSI- als auch Unicode-Kodierung werden unterstützt. Sie geben den vollständigen Pfad zu dieser Textdatei an, wenn Sie die Gruppenrichtlinieneinstellung **Benutzerdefinierte Fußzeile für Fehlerbildschirm** konfigurieren.

Allgemeine Informationen zur Verwendung der Horizon Client-Gruppenrichtlinien finden Sie unter Verwenden von Gruppenrichtlinieneinstellungen zum Konfigurieren von Horizon Client.

Ausführliche Informationen zur Verwendung der Gruppenrichtlinieneinstellung **Benutzerdefinierte Fußzeile für Fehlerbildschirm** finden Sie unter Allgemeine Einstellungen für Client-GPOs.

Konfigurieren der Cursor-Ereignisbehandlung

Sie können die Cursor-Ereignisbehandlung optimieren, indem Sie Einstellungen in der Datei `C:\ProgramData\VMware\VMware Horizon View\Config.ini` auf dem-Windows-Clientsystem konfigurieren.

Hinweis Für die Verwendung der Cursor-Ereignisbehandlung muss Horizon Agent 2006 oder höher auf dem Remotedesktop installiert sein.

Einstellung	Beschreibung
`RemoteDisplay.allowCursorWarping`	Aktiviert bzw. deaktiviert die Funktion „Cursor-Verzerrung“. Wenn diese Funktion aktiviert ist und sich die Maus im absoluten Modus befindet, erkennt der Remote-Agent plötzliche Cursorbewegungen und gibt diese im Client wieder, indem er den lokalen Cursor bewegt. Wenn diese Funktion deaktiviert ist, ignoriert der Client plötzliche Cursorbewegungen im Remote-Agent. Gültige Werte sind „TRUE“ und „FALSE“. Der Standardwert lautet „TRUE“.
`RemoteDisplay.allowCursorEventsOnLowLatencyChannel`	Legt fest, ob der Kanal mit niedriger Latenz für Cursoraktualisierungen verwendet wird. Gültige Werte sind „TRUE“ und „FALSE“. Der Standardwert lautet „TRUE“.

Sie können die maximale Latenz konfigurieren, die beim Zusammenfügen von Mausbewegungen zulässig ist, indem Sie die Gruppenrichtlinieneinstellung **Konfigurieren der maximalen Latenzen für die Mauszusammenfügung** festlegen. Weitere Informationen finden Sie unter Allgemeine Einstellungen für Client-GPOs.

Sie können die Cursor-Ereignisbehandlung auch auf dem Agent-Computer konfigurieren. Sie können z. B. die Gruppenrichtlinieneinstellung **Cursor-Verzerrung** am Agent verwenden, um die Cursor-Verzerrung zu konfigurieren. Außerdem können Sie die Windows-Registrierungseinstellungen auf dem Agent-Computer ändern, um die Zusammenfügung von Mausbewegungen und den Kanal mit niedriger Latenz zu aktivieren bzw. zu deaktivieren. Die Einstellungen müssen sowohl auf dem Client als auch auf dem Agent übereinstimmen, um die Funktion zu aktivieren. Informationen zu den Agent-Einstellungen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Verwenden von Gruppenrichtlinieneinstellungen zum Konfigurieren von Horizon Client

Horizon Client enthält eine Gruppenrichtlinien-ADMX-Vorlagendatei, mit der Sie die Funktionen und das Verhalten von Horizon Client konfigurieren können. Sie können Verbindungen mit Remote-Desktops und veröffentlichten Anwendungen optimieren und sichern, indem Sie die Richtlinieneinstellungen in der ADMX-Vorlagendatei einem neuen oder vorhandenen Gruppenrichtlinienobjekt (Group Policy Object, GPO) in Active Directory hinzufügen.

Die Vorlagendatei enthält sowohl Gruppenrichtlinien für die Computerkonfiguration als auch Gruppenrichtlinien für die Benutzerkonfiguration.

- Richtlinien für die Computerkonfiguration gelten für Horizon Client, unabhängig davon, wer den Client auf dem Host ausführt.
- Mit Richtlinien für die Benutzerkonfiguration werden Horizon Client-Richtlinien festgelegt, die für alle Benutzer gelten, die Horizon Client ausführen, sowie für RDP-Verbindungseinstellungen. Richtlinien für die Benutzerkonfiguration setzen gleichwertige Richtlinien für die Computerkonfiguration außer Kraft.

Horizon Client wendet Richtlinien an, wenn Remote-Desktops und veröffentlichte Anwendungen gestartet werden und wenn Benutzer sich anmelden.

Die ADMX-Vorlagendatei für die Horizon Client-Konfiguration (`vdm_client.admx`) sowie alle ADMX-Vorlagendateien, die Gruppenrichtlinieneinstellungen bereitstellen, befinden sich in `VMware-Horizon-Extras-Bundle-`*`YYMM`*`-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, wobei *YYMM* die Marketingversionsnummer, *x.x.x* die interne Versionsnummer und *yyyyyyy* die Build-Nummer ist. Sie können diese ZIP-Datei auf der VMware-Download-Site unter https://my.vmware.com/web/vmware/downloads herunterladen. Sie müssen die Datei auf Ihren Active Directory-Server kopieren und die Verwaltungsvorlagen mithilfe des Gruppenrichtlinienverwaltungs-Editors hinzufügen. Die Anweisungen dazu finden Sie im *Konfigurieren von Remote-Desktop-Funktionen in Horizon*-Dokument.

Einstellungen für die Skriptdefinition für Client-GPOs

Sie können Gruppenrichtlinien für viele der Einstellungen festlegen, die Sie auch konfigurieren können, wenn Sie Horizon Client über die Befehlszeile ausführen, einschließlich Fenstergröße des Remote-Desktops, Anmeldebenutzername und Anmeldedomänenname.

In der folgenden Tabelle werden die in der ADMX-Vorlagendatei für die VMware Horizon Client-Konfiguration enthaltenen Einstellungen für die Skriptdefinition beschrieben. Diese Vorlagendatei stellt für jede Skriptdefinition eine Version für die Computerkonfiguration und eine Version für die Benutzerkonfiguration bereit. Die Einstellung für die Benutzerkonfiguration setzt hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft. Die Einstellungen sind im Ordner **VMware Horizon Client-Konfiguration > Skriptdefinitionen** im Gruppenrichtlinienverwaltungs-Editor enthalten.

Tabelle 3-4. Konfigurationsvorlage für VMware Horizon Client: Skriptdefinitionen

Einstellung	Beschreibung
`Automatically connect if only one launch item is entitled`	Wenn ein Benutzer zur Verwendung nur eines Remote-Desktops berechtigt ist, verbinden Sie den Benutzer mit diesem Remote-Desktop. Dadurch muss der Benutzer nicht einen Remote-Desktop aus einer Liste mit nur einem Remote-Desktop auswählen.
`Connect all USB devices to the desktop or remote application on launch`	Legt fest, ob alle verfügbaren USB-Geräte auf dem Clientsystem mit dem Remote-Desktop oder der veröffentlichten Anwendung verbunden werden, wenn der Remote-Desktop oder die veröffentlichte Anwendung gestartet wird.
`Connect USB devices to the desktop or remote application when they are plugged in`	Legt fest, ob USB-Geräte mit dem Remote-Desktop oder der veröffentlichten Anwendung verbunden werden, wenn die Geräte an das Clientsystem angeschlossen werden.

Tabelle 3-4. Konfigurationsvorlage für VMware Horizon Client: Skriptdefinitionen (Fortsetzung)

Einstellung	Beschreibung
`DesktopLayout`	Gibt das Layout des Horizon Client-Fensters an, das Benutzern angezeigt wird, wenn sie sich bei einem Remote-Desktop anmelden. Es stehen folgende Optionen zur Auswahl: ■ `Full Screen` ■ `Multimonitor` ■ `Window – Large` ■ `Window – Small` Diese Einstellung ist nur verfügbar, wenn die Einstellung `DesktopName to select setting` ebenfalls gesetzt ist.
`DesktopName to select`	Legt den von Horizon Client während der Anmeldung verwendeten Standard-Remote-Desktop fest.
`Disable 3rd–party Terminal Services plugins`	Legt fest, ob Terminaldienste-Plug-Ins von Drittanbietern, die als normale RDP-Plug-Ins installiert sind, von Horizon Client überprüft werden. Wenn Sie diese Einstellung nicht konfigurieren, überprüft Horizon Client standardmäßig Plug-Ins von Drittanbietern. Diese Einstellung hat keine Auswirkung auf Horizon-spezifische Plug-Ins, wie beispielsweise die USB-Umleitung.
`Locked Guest Size`	Wenn die Anzeige auf einem Bildschirm verwendet wird, gibt dies die Bildschirmauflösung des Remote-Desktops an. Diese Einstellung funktioniert nicht, wenn Sie die Remote-Desktop-Anzeige auf **Alle Monitore** setzen. Nachdem Sie diese Einstellung aktiviert haben, ist die Funktion für die automatische Anpassung von Remote-Desktops deaktiviert, und die Option **Anzeigeskalierung zulassen** wird in der Horizon Client-Benutzeroberfläche ausgeblendet.
`Logon DomainName`	Legt die von Horizon Client während der Anmeldung verwendete NetBIOS-Domäne fest.
`Logon Password`	Legt das von Horizon Client während der Anmeldung verwendete Kennwort fest. Das Kennwort wird von Active Directory im Textformat gespeichert. Zur Erhöhung der Sicherheit sollten Sie diese Einstellung nicht angeben. Benutzer können das Kennwort interaktiv eingeben.
`Logon UserName`	Legt das von Horizon Client während der Anmeldung verwendete Kennwort fest. Das Kennwort wird von Active Directory im Textformat gespeichert.
`Server URL`	Legt die von Horizon Client während der Anmeldung verwendete URL fest, z. B. `https://view1.beispiel.com`.
`Suppress error messages (when fully scripted only)`	Legt fest, ob Horizon Client Fehlermeldungen während der Anmeldung unterdrückt. Diese Einstellung ist nur anwendbar, wenn der Anmeldevorgang vollständig per Skript ausgeführt wird, z. B. wenn alle erforderlichen Anmeldeinformationen über eine Gruppenrichtlinie vorausgefüllt werden. Wenn die Anmeldung aufgrund von falschen Anmeldeinformationen fehlschlägt, werden Benutzer hierüber nicht benachrichtigt, und der Horizon Client-Prozess wird beendet.

Tabelle 3-4. Konfigurationsvorlage für VMware Horizon Client: Skriptdefinitionen (Fortsetzung)

Einstellung	Beschreibung
`Disconnected application session resumption behavior`	Legt fest, wie ausgeführte veröffentlichte Anwendungen sich verhalten, wenn Benutzer erneut eine Verbindung mit einem Server herstellen. Es stehen folgende Optionen zur Auswahl: ■ Vor Neuverbindung zum Öffnen von Anwendungen fragen ■ Neuverbindung zum Öffnen von Anwendungen automatisch herstellen ■ Nicht fragen und nicht automatisch erneut verbinden Wenn diese Einstellung aktiviert ist, haben Endbenutzer keine Möglichkeit, das Wiederverbindungsverhalten von veröffentlichten Anwendungen in Horizon Client zu konfigurieren. Wenn diese Einstellung deaktiviert ist, können Endbenutzer das Wiederverbindungsverhalten von veröffentlichten Anwendungen in Horizon Client konfigurieren. Diese Einstellung ist standardmäßig deaktiviert.
`Enable Unauthenticated Access to the server`	Legt fest, ob Benutzer Anmeldedaten für den Zugriff auf ihre veröffentlichten Anwendungen eingeben müssen, wenn sie Horizon Client verwenden. Wenn diese Einstellung aktiviert ist, wird die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** in Horizon Client angezeigt, deaktiviert und ausgewählt. Wenn der nicht authentifizierte Zugriff nicht verfügbar ist, kann der Client auf eine andere Authentifizierungsmethode zurückgreifen. Wenn diese Einstellung deaktiviert ist, müssen Benutzer immer ihre Anmeldedaten für die Anmeldung bei ihren veröffentlichten Anwendungen und für den Zugriff darauf eingeben. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** in Horizon Client ist ausgeblendet und nicht ausgewählt. Benutzer können den nicht authentifizierten Zugriff in Horizon Client standardmäßig aktivieren. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** wird angezeigt, aktiviert und nicht ausgewählt.
`Account to use for Unauthenticated Access`	Legt das Benutzerkonto für den nicht authentifizierten Zugriff fest, das Horizon Client für die anonyme Anmeldung beim Server verwendet, wenn die Gruppenrichtlinieneinstellung `Enable Unauthenticated Access to the server` aktiviert ist oder wenn ein Benutzer den nicht authentifizierten Zugriff durch Auswahl von **Anonym mit nicht authentifiziertem Zugriff anmelden** in Horizon Client aktiviert. Wenn der nicht authentifizierte Zugriff nicht für eine bestimmte Verbindung mit einem Server verwendet wird, wird diese Einstellung ignoriert. Benutzer können standardmäßig ein Konto auswählen.
`Use existing client instance when connect to same server`	Legt fest, ob eine Verbindung zur vorhandenen Horizon Client-Instanz hinzugefügt wird, mit der der Benutzer bereits mit demselben Server verbunden ist. Diese Einstellung ist standardmäßig deaktiviert, sofern sie nicht konfiguriert wird.

Sicherheitseinstellungen für Client-GPOs

Sicherheitseinstellungen enthalten Gruppenrichtlinien für Zertifikate, Anmeldedaten und die Single Sign-on-Funktion.

In der folgenden Tabelle werden die in der ADMX-Vorlagendatei für die Horizon Client-Konfiguration enthaltenen Sicherheitseinstellungen beschrieben. Diese Tabelle zeigt, ob die Konfiguration sowohl die Einstellung „Computer Configuration (Computerkonfiguration)“ und wie die Einstellung „User Configuration (Benutzerkonfiguration)“ enthält oder nur die Einstellung „Computer Configuration (Computerkonfiguration)“. Bei den Sicherheitseinstellungen, die beide Einstellungstypen einschließen, setzt die Einstellung für die Benutzerkonfiguration hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft. Diese Einstellungen befinden sich im Ordner **VMware Horizon Client-Konfiguration > Sicherheitseinstellungen** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 3-5. Horizon Client-Konfigurationsvorlage: Sicherheitseinstellungen

Einstellung	Computer	Benutzer	Beschreibung
`Allow command line credentials`	X		Legt fest, ob Benutzeranmeldedaten mit Horizon Client-Befehlszeilenoptionen bereitgestellt werden können. Wenn diese Einstellung deaktiviert ist, stehen die Optionen `smartCardPIN` und `password` nicht zur Verfügung, wenn Benutzer Horizon Client über die Befehlszeile ausführen. Diese Einstellung ist standardmäßig aktiviert. Der entsprechende Wert in der Windows-Registrierung lautet `AllowCmdLineCredentials`.
`Configures the SSL Proxy certificate checking behavior of the Horizon Client`	X		Legt fest, ob die Zertifikatsprüfung für sekundäre Verbindungen über einen SSL-Proxy-Server für Blast Secure Gateway und sichere Tunnelverbindungen zugelassen werden soll. Wenn diese Einstellung nicht konfiguriert ist (Standardeinstellung), können Benutzer die SSL-Proxy-Einstellung manuell in Horizon Client ändern. Siehe Festlegen des Zertifikatsprüfungsmodus in Horizon Client. Standardmäßig sperrt Horizon Client SSL-Proxy-Verbindungen für Blast Secure Gateway und sichere Tunnelverbindungen.

Tabelle 3-5. Horizon Client-Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Servers Trusted For Delegation`	X		Legt die Verbindungsserver-Instanzen fest, die die übergebenen Identitäts- und Anmeldeinformationen des Benutzers akzeptieren, wenn ein Benutzer die Option **Als aktueller Benutzer anmelden** im Menü **Optionen** der Horizon Client-Menüleiste auswählt. Wenn Sie keine Verbindungsserver-Instanzen angeben, akzeptieren alle Verbindungsserver-Instanzen diese Informationen, es sei denn, die Authentifizierungseinstellung **Anmeldung als aktueller Benutzer zulassen** ist für die Verbindungsserver-Instanz in Horizon Console deaktiviert. Verwenden Sie zum Hinzufügen einer Verbindungsserverinstanz eines der folgenden Formate: ■ `domain\system$` ■ `system$@domain.com` ■ Service Principal Name (SPN) des Verbindungsserver-Dienstes Der entsprechende Wert in der Windows-Registrierung lautet `BrokersTrustedForDelegation`.

Tabelle 3-5. Horizon Client-Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Certificate verification mode`	X		Konfiguriert die Ebene der Zertifikatsprüfung, die Horizon Client durchführt. Es stehen folgende Modi zur Auswahl: ■ `No Security`. Zertifikate werden nicht überprüft. ■ `Warn But Allow`. Wenn eine Zertifikatsprüfung fehlschlägt, weil der Server ein selbstsigniertes Zertifikat verwendet, sehen Benutzer eine Warnung, die sie ignorieren können. Bei selbstsignierten Zertifikaten muss der Zertifikatsname nicht mit dem Servernamen übereinstimmen, den Benutzer in Horizon Client eingeben. Wenn andere Zertifikatsfehlerbedingungen auftreten, zeigt Horizon Client eine Fehlermeldung an und verhindert, dass Benutzer eine Verbindung mit dem Server herstellen. `Warn But Allow` ist der Standardwert. ■ `Full Security`. Wenn ein beliebiger Zertifikatsfehler auftritt, können Benutzer keine Verbindung mit dem Server herstellen. Horizon Client zeigt dem Benutzer die Zertifikatfehler an. Wenn diese Einstellung konfiguriert ist, können Benutzer den ausgewählten Modus für die Zertifikatsprüfung in Horizon Client sehen, die Einstellung aber nicht konfigurieren. Das Dialogfeld „Zertifikatsprüfungsmodus“ informiert Benutzer darüber, dass ein Administrator die Einstellung gesperrt hat. Wenn diese Einstellung deaktiviert wurde, können Horizon Client-Benutzer einen Zertifikatsprüfungsmodus auswählen. Diese Einstellung ist standardmäßig deaktiviert. Damit ein Server die von Horizon Client bereitgestellten Zertifikate prüfen kann, muss der Client HTTPS-Verbindungen zum Verbindungsserver- oder Sicherheitsserver-Host herstellen. Die Zertifikatsprüfung wird nicht unterstützt, wenn Sie TLS auf ein Zwischengerät verlagern, das HTTP-Verbindungen zum Verbindungsserver- oder Sicherheitsserver-Host herstellt. Wenn Sie diese Einstellung nicht als Gruppenrichtlinie konfigurieren möchten, können Sie die Zertifikatsprüfung auch durch Hinzufügen des Wertnamens `CertCheckMode` zu einem der folgenden Registrierungsschlüssel auf dem Clientcomputer aktivieren: ■ Für 32-Bit-Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security` ■ Für 64-Bit-Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security` Verwenden Sie die folgenden Werte im Registrierungsschlüssel: ■ **`0`** implementiert `No Security`. ■ **`1`** implementiert `Warn But Allow`. ■ **`2`** implementiert `Full Security`.

Tabelle 3-5. Horizon Client-Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
			Wenn Sie sowohl die Gruppenrichtlinieneinstellung als auch die Einstellung `CertCheckMode` im Windows-Registrierungsschlüssel konfigurieren, hat die Gruppenrichtlinieneinstellung Vorrang vor dem Registrierungsschlüsselwert. **Hinweis** In einer zukünftigen Horizon Client-Version wird die Verwendung der Windows-Registrierung zum Konfigurieren dieser Einstellung möglicherweise nicht mehr unterstützt. Stattdessen muss dann die Gruppenrichtlinieneinstellung verwendet werden.
`Default value of the 'Log in as current user' checkbox`	X	X	Legt den Standardwert der Option **Als aktueller Benutzer anmelden** im Menü **Optionen** der Horizon Client-Menüleiste fest. Diese Einstellung setzt den Standardwert außer Kraft, der während der Horizon Client-Installation angegeben wurde. Wenn ein Benutzer Horizon Client über die Befehlszeile ausführt und die Option `logInAsCurrentUser` angibt, wird diese Einstellung durch den eingegebenen Wert überschrieben. Wenn die Option **Als aktueller Benutzer anmelden** im Menü **Optionen** aktiviert ist, werden die Identitäts- und Anmeldeinformationen des Benutzers, die dieser zur Anmeldung beim Clientsystem angegeben hat, an die Verbindungsserver-Instanz und schließlich an den Remote-Desktop oder die veröffentlichte Anwendung übergeben. Wenn die Option **Als aktueller Benutzer anmelden** deaktiviert ist, müssen Benutzer die Identitäts- und Anmeldeinformationen mehrfach eingeben, bevor sie auf einen Remote-Desktop oder eine veröffentlichte Anwendung zugreifen können. Diese Einstellung ist standardmäßig deaktiviert. Der entsprechende Wert in der Windows-Registrierung lautet `LogInAsCurrentUser`.
`Display option to Log in as current user`	X	X	Legt fest, ob die Option **Als aktueller Benutzer anmelden** im Menü **Optionen** der Horizon Client-Menüleiste angezeigt wird. Wenn die Option **Als aktueller Benutzer anmelden** angezeigt wird, können Benutzer diese aktivieren oder deaktivieren und den Standardwert überschreiben. Wenn die Option **Als aktueller Benutzer anmelden** ausgeblendet ist, können Benutzer deren Standardwert im Menü Horizon Client **Optionen** nicht überschreiben. Sie können den Standardwert für **Als aktueller Benutzer anmelden** über die Richtlinieneinstellung `Default value of the 'Log in as current user' checkbox` festlegen. Diese Einstellung ist standardmäßig aktiviert. Der entsprechende Wert in der Windows-Registrierung lautet `LogInAsCurrentUser_Display`.

Tabelle 3-5. Horizon Client-Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Enable jump list integration`	X		Legt fest, ob eine Sprungliste im Horizon Client icon on the taskbar of Windows 7 and later systems. Über die Sprungliste können Benutzer die Verbindung mit zuletzt verwendeten Servern, Remote-Desktops und veröffentlichten Anwendungen herstellen. Wenn Horizon Client gemeinsam verwendet wird, sollen die Namen der zuletzt verwendeten Desktops und veröffentlichten Anwendungen Benutzern möglicherweise nicht angezeigt werden. Die Sprungliste können Sie deaktivieren, indem Sie diese Einstellung deaktivieren. Diese Einstellung ist standardmäßig aktiviert. Der entsprechende Wert in der Windows-Registrierung lautet `EnableJumplist`.
`Enable SSL encrypted framework channel`	X	X	Legt fest, ob TLS für Remote-Desktops mit View 5.0 und früher aktiviert ist. Vor View 5.0 wurden die über den Port TCP 32111 an den Remote-Desktop gesendeten Daten nicht verschlüsselt. ■ **Aktivieren**: Aktiviert TLS, aber ermöglicht das Zurückgreifen auf die vorherige unverschlüsselte Verbindung, falls der Remote-Desktop TLS nicht unterstützt. Beispielsweise wird TLS von Remote-Desktops mit View 5.0 und älter nicht unterstützt. **Enable** ist die Standardeinstellung. ■ **Deaktivieren**: Deaktiviert TLS. Diese Einstellung kann hilfreich sein für das Debugging oder wenn der Kanal nicht getunnelt wird und deshalb möglicherweise durch ein Produkt zur WAN-Beschleunigung optimiert werden könnte. ■ **Erzwingen**: Ermöglicht TLS und verweigert die Verbindung mit Remote-Desktops, die keine Unterstützung für TLS bieten. Der entsprechende Wert in der Windows-Registrierung lautet `EnableTicketSSLAuth`.

Tabelle 3-5. Horizon Client-Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Configures SSL protocols and cryptographic algorithms`	X	X	Konfiguriert die Verschlüsselungsliste, um die Verwendung bestimmter kryptografischer Algorithmen und Protokolle zu beschränken, bevor Sie eine verschlüsselte TLS-Verbindung herstellen. Die Verschlüsselungsliste besteht aus einer oder mehreren Verschlüsselungszeichenfolgen, die durch Doppelpunkte voneinander getrennt werden. Bei der Schlüsselzeichenfolge wird die Groß-/Kleinschreibung beachtet. Der Standardwert ist **TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**. Diese Schlüsselzeichenfolge bedeutet, dass TLS v1.1 und TLS v1.2 aktiviert sind und SSL v.2.0, SSL v3.0 und TLS v1.0 deaktiviert sind. SSL v2.0, SSL v3.0 und TLS v1.0 sind nicht mehr die genehmigten Protokolle und werden dauerhaft deaktiviert. Verschlüsselungs-Suites verwenden ECDHE, ECDH und RSA mit 128-Bit- oder 256-Bit-AES. GCM-Modus ist vorzuziehen. Weitere Informationen finden Sie unter http://www.openssl.org/docs/apps/ciphers.html. Der entsprechende Wert in der Windows-Registrierung lautet `SSLCipherList`.
`Enable Single Sign-On for smart card authentication`	X		Legt fest, ob für die Smartcard-Authentifizierung das Single Sign-On (SSO) aktiviert ist. Ist ein Single Sign-On aktiviert, speichert Horizon Client die verschlüsselte Smartcard-PIN im temporären Arbeitsspeicher, bevor sie an den Verbindungsserver gesendet wird. Ist Single Sign-On deaktiviert, zeigt Horizon Client kein benutzerdefiniertes PIN-Dialogfeld an. Der entsprechende Wert in der Windows-Registrierung lautet `EnableSmartCardSSO`.

Tabelle 3-5. Horizon Client-Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Ignore certificate revocation problems`	X	X	Legt fest, ob Fehler in Zusammenhang mit einem gesperrten Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn das Zertifikat, das der Server sendet, gesperrt wurde oder wenn der Client den Sperrstatus des Zertifikats nicht überprüfen kann. Diese Einstellung ist standardmäßig deaktiviert. **Hinweis** Wenn diese Einstellung aktiviert ist, verwendet der Client bei der Serverzertifikatsprüfung möglicherweise nur eine zwischengespeicherte URL. Die Typen von zwischengespeicherten URL-Informationen können CRL Distribution Point (CDP) und Autorisierungsinformationszugriff (OCSP und Zertifizierungsstellenzugriffsmethoden) sein.
`Unlock remote sessions when the client machine is unlocked`	X	X	Legt fest, ob die Funktion „Rekursives Entsperren“ aktiviert ist. Die Funktion der rekursiven Entsperrung entsperrt alle Remotesitzungen, wenn der Clientcomputer entsperrt wird. Diese Funktion kann nur dann angewendet werden, wenn ein Benutzer sich beim Server mit der Funktion „Als aktueller Benutzer anmelden“ anmeldet. Diese Einstellung ist standardmäßig aktiviert.

Die folgenden Einstellungen befinden sich im Ordner **VMware Horizon Client-Konfiguration > Sicherheitseinstellungen > NTLM-Einstellungen** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 3-6. Horizon Client-Konfigurationsvorlage: Sicherheitseinstellungen, NTLM-Authentifizierungseinstellungen

Einstellung	Computer	Benutzer	Beschreibung
`Allow NTLM Authentication`	X		Wenn diese Einstellung aktiviert ist, ist die NTLM-Authentifizierung für die Funktion **Als aktueller Benutzer anmelden** zulässig. Wenn diese Einstellung deaktiviert ist, wird die NTLM-Authentifizierung nicht für Server verwendet. Wenn diese Einstellung aktiviert ist, können Sie im Dropdown-Menü **Fallback von Kerberos zu NTLM erlauben** die Option **Ja** oder **Nein** auswählen. ■ Wenn Sie **Ja** auswählen, kann die NTLM-Authentifizierung jederzeit verwendet werden, sobald der Client kein Kerberos-Ticket für den Server abrufen kann. ■ Wenn Sie **Nein** auswählen, ist die NTLM-Authentifizierung nur für Server zulässig, die in der Gruppenrichtlinieneinstellung **NTLM immer für Server verwenden** aufgeführt sind. Wenn diese Einstellung nicht konfiguriert ist, ist die NTLM-Authentifizierung für Server zulässig, die in der Gruppenrichtlinieneinstellung **NTLM immer für Server verwenden** aufgeführt sind. Um die NTLM-Authentifizierung verwenden zu können, muss das SSL-Zertifikat des Servers gültig sein und die Verwendung von NTLM darf nicht durch Windows-Richtlinien eingeschränkt sein. Informationen zum Konfigurieren des Fallbacks von Kerberos zu NTLM in einer Verbindungsserverinstanz finden Sie im Dokument *Verwaltung der VMware Horizon Console* unter „Verwenden der Funktion ‚Anmelden als aktueller Benutzer', die mit Windows-basierten Horizon Client-Instanzen verfügbar ist".
`Always use NTLM for servers`	X		Wenn diese Einstellung aktiviert ist, wird bei der Funktion **Als aktueller Benutzer anmelden** immer die NTLM-Authentifizierung für die aufgeführten Server verwendet. Um die Serverliste zu erstellen, klicken Sie auf **Anzeigen** und geben in der Spalte **Wert** den Servernamen ein. Das Benennungsformat für Server ist der vollqualifizierte Domänenname (FQDN).

RDP-Einstellungen für Client-GPOs

Sie können Gruppenrichtlinieneinstellungen für Optionen wie die Umleitung von Audio, Druckern, Ports und anderen Geräten festlegen, wenn Sie das Microsoft RDP-Anzeigeprotokoll verwenden.

In der folgenden Tabelle werden die in der ADMX-Vorlagendatei für die Horizon Client-Konfiguration enthaltenen RDP-Einstellungen (Remote Desktop Protocol) beschrieben. Alle RDP-Einstellungen sind Einstellungen für die Benutzerkonfiguration. Die Einstellungen befinden sich im Ordner **VMware Horizon Client Configuration > RDP-Einstellungen** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 3-7. ADM-Vorlage für Horizon Client-Konfiguration: RDP-Einstellungen

Einstellung	Beschreibung
`Audio redirection`	Legt fest, ob auf dem Remote-Desktop wiedergegebene Audioinformationen umgeleitet werden. Es stehen folgende Einstellungen zur Auswahl: ■ **Audio deaktivieren**: Audio ist deaktiviert. ■ **In VM wiedergeben (erforderlich für VoIP USB-Unterstützung)**: Audiodaten werden im Remote-Desktop wiedergegeben. Diese Einstellung erfordert ein gemeinsam genutztes USB-Audiogerät zur Wiedergabe von Sound auf dem Client. ■ **An Client umleiten**: Audiodaten werden an den Client umgeleitet. Diese Einstellung ist der Standardmodus. Diese Eigenschaft gilt nur für RDP-Audio. Über MMR umgeleitete Audiodaten werden im Client wiedergegeben.
`Enable audio capture redirection`	Legt fest, ob das standardmäßige Audioeingabegerät vom Client an die Remote-Sitzung umgeleitet wird. Wenn diese Einstellung aktiviert ist, wird das Audioaufzeichnungsgerät des Clients im Remote-Desktop angezeigt und kann zur Aufzeichnung von Audioeingabedaten verwendet werden. Diese Einstellung ist standardmäßig deaktiviert.
`Bitmap cache file size in` *unit* `for` *number* `bpp bitmaps`	Gibt die Größe des Bitmapcaches (in KB oder MB) für die Zwischenspeicherung von Bitmaps mit einer bestimmten Farbeinstellung (Bits pro Pixel, bpp) an. Für die verschiedenen Kombinationen aus Einheit und Bits pro Pixel stehen unterschiedliche Versionen zur Verfügung: ■ MB/8bpp ■ MB/16bpp ■ MB/24bpp ■ MB/32bpp
`In-memory bitmap cache size in KB for 8bpp bitmaps`	Legt die Größe des RAM-Bitmap-Cache für die 8-Bit-pro-Pixel-Farbeinstellung in Kilobyte fest. Wenn für ScaleBitmapCachesByBPP „true“ festgelegt ist (Standard), wird für die Bestimmung der tatsächlichen RAM-Cache-Größe die Cache-Größe mit der Anzahl der Byte pro Pixel multipliziert. Wenn diese Einstellung aktiviert ist, geben Sie die Größe in Kilobyte ein.
`Bitmap caching/cache persistence active`	Legt fest, ob für Bitmaps eine dauerhafte Zwischenspeicherung durchgeführt wird (aktiv ist). Eine dauerhafte Zwischenspeicherung für Bitmaps kann die Leistung verbessern, erfordert jedoch zusätzlichen Speicherplatz.
`Color depth`	Legt die Farbtiefe für den Remote-Desktop fest. Es stehen folgende Einstellungen zur Auswahl: ■ 8 Bit ■ 15 Bit ■ 16 Bit ■ 24 Bit ■ 32 Bit
`Cursor shadow`	Legt fest, ob auf dem Remote-Desktop unter dem Mauszeiger ein Schatten angezeigt wird.
`Desktop background`	Legt fest, ob der Desktop-Hintergrund angezeigt wird, wenn Clients eine Verbindung zu einem Remote-Desktop herstellen.

Tabelle 3-7. ADM-Vorlage für Horizon Client-Konfiguration: RDP-Einstellungen (Fortsetzung)

Einstellung	Beschreibung
`Desktop composition`	Legt fest, ob die Desktopgestaltung auf dem Remote-Desktop aktiviert ist. Wenn die Desktop-Gestaltung aktiviert ist, werden einzelne Fenster nicht länger direkt auf dem Bildschirm oder dem primären Anzeigegerät dargestellt, wie dies in früheren Versionen von Microsoft Windows der Fall war. Stattdessen werden die Bilddaten zunächst in den nicht sichtbaren Offscreen-Bereich des Videospeichers umgeleitet und anschließend zur Darstellung auf dem Anzeigegerät in ein Desktop-Bild gerendert.
`Enable compression`	Legt fest, ob RDP-Daten komprimiert werden. Diese Einstellung ist standardmäßig aktiviert.
`Enable RDP Auto-Reconnect`	Legt fest, ob die RDP-Clientkomponente versucht, erneut eine Verbindung mit einem Remote-Desktop herzustellen, nachdem ein RDP-Verbindungsfehler aufgetreten ist. Diese Einstellung hat keine Auswirkung, wenn die Option **Sichere Tunnelverbindung zum Desktop verwenden** in Horizon Console aktiviert wurde. Diese Einstellung ist standardmäßig deaktiviert.
`Font smoothing`	Legt fest, ob Anti-Aliasing auf die Schriftarten auf dem Remote-Desktop angewendet wird.
`Menu and window animation`	Legt fest, ob die Animation für Menüs und Fenster aktiviert ist, wenn Clients eine Verbindung zu einem Remote-Desktop herstellen.
`Redirect clipboard`	Legt fest, ob die Informationen in der lokalen Zwischenablage umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen.
`Redirect drives`	Legt fest, ob lokale Festplattenlaufwerke umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen. Lokale Laufwerke werden standardmäßig umgeleitet. Durch Aktivieren oder Nichtkonfigurieren dieser Einstellung können Daten auf dem umgeleiteten Laufwerk des Remote-Desktops auf das Laufwerk des Clientcomputers kopiert werden. Deaktivieren Sie diese Einstellung, wenn das Übertragen von Daten vom Remote-Desktop zu den Clientcomputern des Benutzers ein mögliches Sicherheitsrisiko für Ihre Bereitstellung darstellt. Alternativ können Sie auch die Ordnerumleitung in der virtuellen Maschine des Remote-Desktops deaktivieren, indem Sie die Microsoft Windows-Gruppenrichtlinieneinstellung `Do not allow drive redirection` aktivieren. Die Einstellung `Redirect drives` wirkt sich nur auf RDP aus.
`Redirect printers`	Legt fest, ob lokale Drucker umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen.
`Redirect serial ports`	Legt fest, ob lokale COM-Ports umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen.
`Redirect smart cards`	Legt fest, ob lokale Smartcards umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen. **Hinweis** Diese Einstellung gilt sowohl für RDP- als auch für PCoIP-Verbindungen.
`Redirect supported plug-and-play devices`	Legt fest, ob lokale Plug & Play- sowie POS-Geräte (Point of Sale) umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen. Dieses Verhalten unterscheidet sich von der Umleitung, die durch die Agent-Komponente für die USB-Umleitung verwaltet wird.
`Shadow bitmaps`	Legt fest, ob Schattenbitmaps verwendet werden. Diese Einstellung hat im Vollbildmodus keine Auswirkung.

Tabelle 3-7. ADM-Vorlage für Horizon Client-Konfiguration: RDP-Einstellungen (Fortsetzung)

Einstellung	Beschreibung
`Show contents of window while dragging`	Legt fest, ob Ordnerinhalte angezeigt werden, wenn der Benutzer einen Ordner an einen neuen Speicherort zieht.
`Themes`	Legt fest, ob Designs angezeigt werden, wenn Clients eine Verbindung zu einem Remote-Desktop herstellen.
`Windows key combination redirection`	Legt fest, wo Windows-Tastenkombinationen angewendet werden. Mit dieser Einstellung können Sie Tastenkombinationen an die virtuelle Remote-Maschine senden oder lokal Tastenkombinationen anwenden. Tastenkombinationen werden standardmäßig lokal angewendet.
`Enable Credential Security Service Provider`	Gibt an, ob die Remote-Desktop-Verbindung die Authentifizierung auf Netzwerkebene (Network Level Authentication, NLA) verwendet. Wenn das Gastbetriebssystem für Remote-Desktop-Verbindungen NLA erfordert, müssen Sie diese Einstellung aktivieren. Andernfalls kann Horizon Client eventuell keine Verbindung zum Remote-Desktop herstellen. Zusätzlich zur Aktivierung dieser Einstellung müssen Sie sicherstellen, dass die folgenden Bedingungen erfüllt sind: ■ Sowohl das Client- als auch das Gastbetriebssystem unterstützen NLA. ■ Für die Verbindungsserver-Instanz sind direkte Clientverbindungen aktiviert. Tunnelverbindungen werden mit NLA nicht unterstützt.

Allgemeine Einstellungen für Client-GPOs

Zu den allgemeinen Einstellungen zählen Proxy-Optionen, Zeitzonenweiterleitung, Multimediabeschleunigung und sonstige Anzeigeeinstellungen.

Allgemeine Einstellungen

In der folgenden Tabelle werden die in der ADMX-Vorlagendatei für die Horizon Client-Konfiguration enthaltenen allgemeinen Einstellungen beschrieben. Zu den allgemeinen Einstellungen gehören sowohl Einstellungen für die Computerkonfiguration als auch Einstellungen für die Benutzerkonfiguration. Die Einstellung für die Benutzerkonfiguration setzt hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft. Die Einstellungen befinden sich im Ordner **VMware Horizon Client-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 3-8. Horizon Client-Konfigurationsvorlage: Allgemeine Einstellungen

Einstellung	Computer	Benutzer	Beschreibung
`Allow Blast connections to use operating system proxy settings`	X		Konfiguriert die Verwendung des Proxy-Servers für VMware Blast-Verbindungen. Wenn diese Einstellung aktiviert ist, kann VMware Blast eine Verbindung über einen Proxy-Server herstellen. Wenn diese Einstellung deaktiviert ist, kann VMware Blast keinen Proxy-Server verwenden. Wenn diese Einstellung nicht konfiguriert ist (Standardeinstellung), können Benutzer konfigurieren, ob VMware Blast-Verbindungen einen Proxy-Server auf der Horizon Client-Benutzeroberfläche verwenden können. Siehe Konfigurieren der VMware Blast-Optionen.
`Allow data sharing`	X		Wenn diese Einstellung aktiviert ist, ist die Einstellung für den Datenfreigabemodus in der Horizon Client-Benutzeroberfläche eingeschaltet und Endbenutzer können die Einstellung nicht ändern. Wenn diese Einstellung deaktiviert ist, ist die Einstellung für den Datenfreigabemodus in der Horizon Client-Benutzeroberfläche ausgeschaltet und Endbenutzer können die Einstellung nicht ändern. Wenn diese Einstellung nicht konfiguriert ist (Standardeinstellung), können Endbenutzer die Einstellung für den Datenfreigabemodus in der Horizon Client-Benutzeroberfläche ändern.
`Allow display scaling`	X	X	Wenn diese Einstellung aktiviert ist, ist die Funktion zur Anzeigeskalierung für alle Remote-Desktops und veröffentlichten Anwendungen aktiviert. Wenn diese Einstellung deaktiviert ist, ist die Funktion zur Anzeigeskalierung für alle Remote-Desktops und veröffentlichten Anwendungen deaktiviert. Wenn diese Einstellung nicht konfiguriert ist (Standardeinstellung), können Endbenutzer die Anzeigeskalierung in der Horizon Client-Benutzeroberfläche aktivieren und deaktivieren. Sie haben auch die Möglichkeit, die Einstellung für die Anzeigeskalierung in der Horizon Client-Benutzeroberfläche durch Aktivierung der Gruppenrichtlinieneinstellung **Gesperrte Gastgröße** auszublenden. Weitere Informationen finden Sie unter Einstellungen für die Skriptdefinition für Client-GPOs.
`Allow user to skip Horizon Client update`	X		Legt fest, ob Benutzer im Horizon Client-Fenster „Aktualisieren“ auf die Schaltfläche **Überspringen** klicken können. Wenn Benutzer auf **Überspringen** klicken, wird keine weitere Updatebenachrichtigung angezeigt, bis die nächste Horizon Client-Version verfügbar ist.

Tabelle 3-8. Horizon Client-Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
Always hide the remote floating language (IME) bar for Hosted Apps	X	X	Schaltet die flexibel platzierbare Sprachleiste für Anwendungssitzungen aus. Wenn diese Einstellung aktiviert ist, wird die flexibel platzierbare Sprachleiste in Sitzungen von veröffentlichten Anwendungen nicht angezeigt, unabhängig von der Aktivierung der lokalen IME-Funktion. Wenn diese Einstellung deaktiviert ist, wird die flexibel platzierbare Sprachleiste nur angezeigt, wenn die lokale IME-Funktion deaktiviert ist. Diese Einstellung ist standardmäßig deaktiviert.
Always on top		X	Legt fest, ob das Horizon Client-Fenster immer im Vordergrund angezeigt wird. Durch Aktivierung dieser Einstellung wird verhindert, dass die Windows-Taskleiste ein Horizon Client-Fenster im Vollbildmodus überlappt. Diese Einstellung ist standardmäßig deaktiviert.
Automatic input focus in a virtual desktop window	X	X	Wenn diese Einstellung aktiviert ist, sendet Horizon Client automatisch Eingaben an den Remote-Desktop, wenn ein Benutzer den Remote-Desktop in den Vordergrund bringt. Mit anderen Worten: Der Fokus befindet sich nicht im Fensterrahmen und der Benutzer muss nicht innerhalb des Remote-Desktop-Fensters klicken, um den Fokus zu verschieben.
Automatically check for updates	X		Legt fest, ob automatisch nach Horizon Client-Software-Updates gesucht wird. Diese Einstellung steuert das Kontrollkästchen **Nach Updates suchen und Badge-Benachrichtigung anzeigen** im Horizon Client-Updatefenster. Diese Einstellung ist standardmäßig aktiviert.
Automatically install shortcuts when configured on the Horizon server		X	Wenn Verknüpfungen für veröffentlichte Anwendungen und Remote-Desktops auf einer Verbindungsserver-Instanz konfiguriert sind, legt diese Einstellung fest, ob und wie die Verknüpfungen auf Client Computern installiert werden, wenn Benutzer eine Verbindung mit dem Server herstellen. Wenn diese Einstellung aktiviert ist, werden Verknüpfungen auf Clientcomputern installiert. Die Benutzer werden also nicht aufgefordert, die Verknüpfungen zu installieren. Wenn diese Einstellung deaktiviert ist, werden Verknüpfungen nicht auf Clientcomputern installiert. Die Benutzer werden also nicht aufgefordert, die Verknüpfungen zu installieren. Die Benutzer werden aufgefordert, die Verknüpfungen standardmäßig zu installieren.

Tabelle 3-8. Horizon Client-Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Automatically synchronize the keypad, scroll and caps lock keys`	X		Wenn diese Einstellung aktiviert ist, werden die Umschaltstatus der Tasten Num, Rollen und Feststellen vom Clientgerät mit einem Remote-Desktop synchronisiert. In Horizon Client wird das Kontrollkästchen **Tastatur, Bildlauf und Feststelltaste automatisch synchronisieren** aktiviert und die Einstellung ist abgeblendet. Wenn diese Einstellung deaktiviert ist, werden die Zustände der Sperrtasten vom Remote-Desktop mit dem Clientgerät synchronisiert. In Horizon Client wird das Kontrollkästchen **Tastatur, Bildlauf und Feststelltaste automatisch synchronisieren** deaktiviert und die Einstellung ist abgeblendet. Wenn diese Einstellung aktiviert oder deaktiviert ist, können Benutzer die Einstellung **Tastatur, Bildlauf und Feststelltaste automatisch synchronisieren** in Horizon Client nicht verändern. Wenn diese Einstellung nicht konfiguriert ist, kann ein Benutzer die Sperrschlüssel-Synchronisierung für einen Remote-Desktop aktivieren oder deaktivieren, indem er die Einstellung **Tastatur, Bildlauf und Feststelltaste automatisch synchronisieren** in Horizon Client konfiguriert. Siehe Konfigurieren der Synchronisierung von Sperrtasten. Diese Einstellung ist standardmäßig nicht konfiguriert.
`Block multiple Horizon Client instances per Windows session`	X		Verhindert, dass ein Benutzer während einer Windows-Sitzung mehrere Instanzen von Horizon Client startet. Wenn diese Einstellung aktiviert ist, läuft Horizon Client im Einzelinstanzmodus, und ein Benutzer kann nicht mehrere Horizon Client-Instanzen in einer Windows-Sitzung starten. Wenn diese Einstellung deaktiviert ist, kann ein Benutzer mehrere Horizon Client-Instanzen in einer Windows-Sitzung starten. Diese Einstellung ist standardmäßig deaktiviert.
`Configure maximum latency for mouse coalescing`	X		Legt die maximal zulässige Latenz in Millisekunden fest, bei der Mausbewegungen zusammengefügt werden. Gültige Werte sind 0 bis 50. Bei Verwendung des Werts 0 wird die Funktion deaktiviert. Die Zusammenfügung von Mausbewegungen kann zu einer Reduzierung der Bandbreitennutzung des Clients zum Agent führen, möglicherweise jedoch eine geringe Latenz zur Mausbewegung hinzufügen. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 3-8. Horizon Client-Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Custom error screen footer`	X		Ermöglicht Ihnen das Hinzufügen von benutzerdefiniertem Hilfetext am Ende aller Horizon Client-Fehlermeldungen. Sie müssen den Hilfetext in einer reinen Textdatei (`.txt`) auf dem lokalen Clientsystem bereitstellen. Die Textdatei kann bis zu 2.048 Zeichen, einschließlich Steuerzeichen enthalten. Sowohl ANSI- als auch Unicode-Kodierung werden unterstützt. Wenn diese Einstellung aktiviert ist, geben Sie den vollständigen Pfad zu der Datei mit dem benutzerdefinierten Hilfetext im bereitgestellten Textfeld an. Hier ein Beispiel: `C:\myDocs \errorFooter.txt`. Diese Einstellung ist standardmäßig deaktiviert.
`Default value of the "Hide the selector after launching an item" check box`	X	X	Legt fest, ob das Kontrollkästchen **Selektor nach Start eines Elements ausblenden** standardmäßig ausgewählt ist. Diese Einstellung ist standardmäßig deaktiviert.
`Disable desktop disconnect messages`	X	X	Legt fest, ob Meldungen deaktiviert werden, die normalerweise beim Trennen der Verbindung mit Remote-Desktops angezeigt werden. Diese Meldungen werden standardmäßig angezeigt.
`Disable sharing files and folders`		X	Legt fest, ob die Funktionalität der Clientlaufwerksumleitung in Horizon Client verfügbar ist. Wenn diese Einstellung aktiviert ist, wird die gesamte Funktionalität der Clientlaufwerksumleitung in Horizon Client deaktiviert, einschließlich der Möglichkeit, lokale Dateien mit veröffentlichten Anwendungen zu öffnen. Darüber hinaus werden die folgenden Elemente in der Benutzeroberfläche von Horizon Client ausgeblendet: ■ Freigabebereich im Dialogfeld „Einstellungen“. ■ Option **Ordner freigeben** im Menü **Option** eines Remote-Desktops. ■ Option **Freigabe** für Horizon Client in der Taskleiste. ■ Das Dialogfeld „Freigabe“, das angezeigt wird, wenn Sie das erste Mal eine Verbindung mit einem Remote-Desktop oder einer Anwendung herstellen, nachdem Sie sich mit einem Server verbunden haben. Wenn diese Einstellung deaktiviert ist, ist die Funktion der Clientlaufwerksumleitung komplett verwendbar. Diese Einstellung ist standardmäßig deaktiviert.
`Disable time zone forwarding`	X		Legt fest, ob die Zeitzonensynchronisierung des Remote-Desktops mit der des verbundenen Clients deaktiviert ist.

Tabelle 3-8. Horizon Client-Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Disable toast notifications`	X	X	Hierdurch wird festgelegt, ob Toastnachrichten von Horizon Client deaktiviert werden sollen. Aktivieren Sie diese Einstellung, wenn Sie nicht möchten, dass dem Benutzer Toastnachrichten in der Ecke des Bildschirms angezeigt werden. **Hinweis** Wenn Sie diese Einstellung aktivieren, wird für den Benutzer bei Aktivierung der Funktion „Zeitüberschreitung der Sitzung“ keine Fünf-Minuten-Warnung eingeblendet.
`Disallow passing through client information in a nested session`	X		Gibt an, ob verhindert wird, dass Horizon Client durch Clientinformationen in einer verschachtelten Sitzung weitergegeben wird. Wenn Sie diese Option aktivieren und Horizon Client in einer Remotesitzung ausgeführt wird, werden die tatsächlichen Informationen zum physischen Client anstelle der VM-Geräteinformationen gesendet. Diese Einstellung gilt für die folgenden Clientinformationen: Gerätename und Domäne, Clienttyp, IP-Adresse und MAC-Adresse. Diese Einstellung ist standardmäßig deaktiviert. Demnach ist das Weitergeben von Clientinformationen in einer verschachtelten Sitzung zulässig.
`Display modifier function key`	X	X	Gibt die Schalteränderung und Funktionsschlüsselkombination an, mit der Benutzer die Anzeigekonfiguration des Clientcomputers ändern können, wenn sie belegt ist und eine Eingabe bei einer PCoIP- oder VMware Blast-Remote-Desktop-Sitzung vorgenommen wird. Wenn diese Einstellung nicht konfiguriert ist (Standardeinstellung), müssen Endbenutzer die Maus verwenden, um die Belegung des Remote-Desktops aufzuheben, und zum Auswählen eines Präsentationsanzeigemodus anschließend die Windows-Taste + P drücken. Diese Einstellung gilt nicht für Sitzungen veröffentlichter Anwendungen.
`Disable opening local files in hosted applications`		X	Legt fest, ob Horizon Client lokale Handler für Dateierweiterungen registriert, die von gehosteten Anwendungen unterstützt werden. Wenn diese Einstellung aktiviert ist, registriert Horizon Client keine Handler für Dateierweiterungen. Benutzer können diese Einstellung dann nicht überschreiben. Ist diese Einstellung deaktiviert, werden Handler für Dateierweiterungen immer von Horizon Client registriert. Handler für Dateierweiterungen werden standardmäßig registriert. Benutzer haben aber die Möglichkeit, die Funktion in der Benutzeroberfläche von Horizon Client mit der Einstellung **Turn on the ability to open a local file with a remote application from the local file system** (Aktivieren der Möglichkeit, eine lokale Datei mit einer Remoteanwendung aus dem lokalen Dateisystem zu öffnen) im Bereich „Freigabe“ des Dialogfeldes „Einstellungen“ zu deaktivieren. Weitere Informationen finden Sie unter Freigeben lokaler Ordner und Laufwerke. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 3-8. Horizon Client-Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Don't check monitor alignment on spanning`		X	Standardmäßig wird der Client-Desktop nicht in den Mehrfachmonitor-Modus geschaltet, wenn die Bildschirme in Kombination kein exaktes Rechteck bilden (d.h. identische Höhe bei horizontaler Anordnung oder identische Breite bei vertikaler Anordnung). Aktivieren Sie diese Einstellung, um den Standardwert außer Kraft zu setzen. Diese Einstellung ist standardmäßig deaktiviert.
`Enable multi-media acceleration`		X	Legt fest, ob die Multimedia-Umleitung (Multimedia Redirection, MMR) auf dem Client aktiviert ist. MMR funktioniert nicht ordnungsgemäß, wenn die Horizon Client-Hardware zur Videoanzeige keine Overlay-Unterstützung bietet.
`Enable relative mouse`	X	X	Aktiviert die relative Maus, wenn das PCoIP-Anzeigeprotokoll verwendet wird. Der Modus für relative Mausbewegungen optimiert das Mausverhalten für bestimmte Grafikanwendungen und Spiele. Falls der Modus für relative Mausbewegungen nicht vom Remote-Desktop unterstützt wird, wird diese Einstellung nicht verwendet. Diese Einstellung ist standardmäßig deaktiviert.
`Enable the shade`		X	Legt fest, ob die Schatten-Menüleiste im oberen Bereich des Horizon Client-Fensters sichtbar ist. Diese Einstellung ist standardmäßig aktiviert. **Hinweis** Die Schatten-Menüleiste im oberen Bereich ist für den Kiosk-Modus standardmäßig deaktiviert.
`Enable Horizon Client online update`	X		Aktiviert die Funktion für die Onlineaktualisierung. Diese Einstellung ist standardmäßig aktiviert. **Hinweis** Sie können die Funktion für die Onlineaktualisierung auch durch Festlegung der Eigenschaft `AUTO_UPDATE_ENABLED` auf 0 deaktivieren, wenn Sie Horizon Client über die Befehlszeile installieren. Weitere Informationen finden Sie unter Installationseigenschaften für Horizon Client.

Tabelle 3-8. Horizon Client-Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Hide items in application context menu`	X	X	Verwenden Sie diese Einstellung, um Elemente im Kontextmenü auszublenden, das angezeigt wird, wenn Sie im Fenster für die Desktop- und Anwendungsauswahl mit der rechten Maustaste auf eine veröffentlichte Anwendung klicken. Wenn diese Einstellung aktiviert ist, können Sie die folgenden Optionen konfigurieren: ■ **Einstellungen ausblenden** – Wählen Sie **Ja** aus, um das Element **Einstellungen** im Kontextmenü auszublenden. ■ **„Verknüpfung für Desktop erstellen“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Verknüpfung für Desktop erstellen** im Kontextmenü auszublenden. ■ **„Zum Startmenü hinzufügen“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Zum Startmenü hinzufügen** im Kontextmenü auszublenden. ■ **„Als Favorit markieren“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Als Favorit markieren** im Kontextmenü auszublenden. Diese Einstellung ist standardmäßig deaktiviert.
`Hide items in desktop context menu`	X	X	Verwenden Sie diese Einstellung, um Elemente im Kontextmenü auszublenden, das angezeigt wird, wenn Sie im Fenster für die Desktop- und Anwendungsauswahl mit der rechten Maustaste auf einen Remote-Desktop klicken. Wenn diese Einstellung aktiviert ist, können Sie die folgenden Optionen konfigurieren: ■ **„Desktop zurücksetzen“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Desktop zurücksetzen** im Kontextmenü auszublenden. ■ **„Desktop neu starten“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Desktop neu starten** im Kontextmenü auszublenden. ■ **Anzeige ausblenden** – Wählen Sie **Ja** aus, um das Element **Anzeige** im Kontextmenü auszublenden. ■ **Einstellungen ausblenden** – Wählen Sie **Ja** aus, um das Element **Einstellungen** im Kontextmenü auszublenden. ■ **„Verknüpfung für Desktop erstellen“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Verknüpfung für Desktop erstellen** im Kontextmenü auszublenden. ■ **„Zum Startmenü hinzufügen“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Zum Startmenü hinzufügen** im Kontextmenü auszublenden. ■ **„Als Favorit markieren“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Als Favorit markieren** im Kontextmenü auszublenden. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 3-8. Horizon Client-Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Hide items in desktop toolbar`	X	X	Verwenden Sie diese Einstellung, um Elemente in der Menüleiste eines Remote-Desktop-Fensters auszublenden. Wenn diese Einstellung aktiviert ist, können Sie die folgenden Optionen konfigurieren. ■ **Hilfe ausblenden** – Wählen Sie **Ja** aus, um das Element **Hilfe** im Menü **Optionen** auszublenden. ■ **Support-Informationen ausblenden** – Wählen Sie **Ja** aus, um das Element **Supportinformationen** im Menü **Optionen** auszublenden. ■ **„Relative Maus aktivieren“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Relative Maus aktivieren** im Menü **Optionen** auszublenden. ■ **„Ordner freigeben“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Ordner freigeben** im Menü **Optionen** auszublenden. ■ **„Anzeigeskalierung zulassen“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Anzeigeskalierung zulassen** im Menü **Optionen** auszublenden. ■ **„Desktop zurücksetzen“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Desktop zurücksetzen** im Menü **Optionen** auszublenden. ■ **„Desktop neu starten“ ausblenden** – Wählen Sie **Ja** aus, um das Element **Desktop neu starten** im Menü **Optionen** auszublenden. ■ **„USB-Gerät verbinden“ ausblenden** – Wählen Sie **Ja** aus, um das Menü **USB-Gerät verbinden** in der Menüleiste auszublenden. Diese Einstellung ist standardmäßig deaktiviert.
`Hide items in system tray menu`	X	X	Verwenden Sie diese Einstellung, um Elemente im Kontextmenü auszublenden, das angezeigt wird, wenn Sie in der Taskleiste auf dem lokalen Clientsystem mit der rechten Maustaste auf das Horizon Client-Symbol klicken. Wenn diese Einstellung aktiviert ist, können Sie die folgenden Optionen konfigurieren. ■ **Freigabe ausblenden** – Wählen Sie **Ja** aus, um das Horizon Client-Element **Freigabe** auszublenden. ■ **Einstellungen ausblenden** – Wählen Sie **Ja** aus, um das Horizon Client-Element **Einstellungen** auszublenden. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 3-8. Horizon Client-Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Hide items in the client toolbar menu`	X	X	Verwenden Sie diese Einstellung, um Elemente in der Symbolleiste oben im Fenster für die Desktop- und Anwendungsauswahl auszublenden. Wenn diese Einstellung aktiviert ist, können Sie die folgenden Optionen konfigurieren. ■ **Favoritenumschalter ausblenden** – Wählen Sie **Ja** aus, um das Sternsymbol **Favoriten anzeigen** auszublenden. ■ **Einstellungszahnrad ausblenden** – Wählen Sie **Ja** aus, um das Zahnradsymbol **Einstellungen** auszublenden. Diese Einstellung ist standardmäßig deaktiviert.
`Hotkey combination to grab input focus`	X	X	Konfiguriert eine Tastenkombination, um den Eingabefokus für die zuletzt verwendete PCoIP- oder VMware Blast-Remote-Desktopsitzung zu erfassen. Eine Tastenkombination besteht aus einer oder zwei Modifikatortasten und einer Buchstabentaste. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, kann der Benutzer den Fokus durch Klicken in das Remote-Desktopfenster erfassen. Diese Einstellung ist standardmäßig nicht konfiguriert.
`Hotkey combination to release input focus`	X	X	Konfiguriert eine Tastenkombination, um den Eingabefokus für eine PCoIP- oder VMware Blast-Remote-Desktopsitzung freizugeben. Eine Tastenkombination besteht aus einer oder zwei Modifikatortasten und einer Funktionstaste. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, kann der Benutzer den Fokus mithilfe von Strg + Alt oder durch Klicken außerhalb des Remote-Desktopfensters freigeben. Diese Einstellung ist standardmäßig nicht konfiguriert.
`Pin the shade`		X	Legt fest, ob die Fixierung der Menüleiste im oberen Bereich des Horizon Client-Fensters aktiviert ist, sodass die Menüleiste nicht automatisch ausgeblendet wird. Diese Einstellung hat keine Auswirkung, wenn die Menüleiste deaktiviert wurde. Diese Einstellung ist standardmäßig aktiviert.
`Save resolution and DPI to server`	X		Legt fest, ob Horizon Client die Einstellungen für die benutzerdefinierte Anzeigeauflösung und die Anzeigeskalierung auf dem Server speichert. Informationen zum Anpassen der Einstellungen für die Anzeigeauflösung und Anzeigeskalierung für einen Remote-Desktop finden Sie unter Anpassen der Anzeigeauflösung und Anzeigeskalierung für einen Remote-Desktop. Wenn diese Einstellung aktiviert ist und die Anzeigeauflösung oder Anzeigeskalierung für einen Remote-Desktop angepasst wurde, werden die benutzerdefinierten Einstellungen bei jedem Öffnen des Remote-Desktops automatisch angewendet, unabhängig vom Clientgerät, das der Benutzer zur Anmeldung auf dem Remote-Desktop verwendet. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 3-8. Horizon Client-Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Tunnel proxy bypass address list`	X		Gibt eine Liste von Tunneladressen an. Der Proxy-Server wird für diese Adressen nicht verwendet. Verwenden Sie ein Semikolon (;) zum Trennen mehrerer Einträge.
`Update message pop-up`	X		Gibt an, ob die Update-Popup-Nachricht für Endbenutzer automatisch angezeigt wird, wenn eine neue Version von Horizon Client verfügbar ist. Diese Einstellung steuert das Kontrollkästchen **Popup-Meldung anzeigen, wenn ein Update vorliegt** im Horizon Client-Update-Fenster. Diese Einstellung ist standardmäßig deaktiviert.
`URL for Horizon Client online help`	X		Gibt eine alternative URL an, von der Horizon Client Hilfeseiten abrufen kann. Diese Einstellung ist zur Verwendung in Umgebungen gedacht, die das remote gehostete Hilfesystem nicht abrufen können, da kein Internetzugriff verfügbar ist.
`URL for Horizon Client online update`	X		Gibt eine alternative URL an, von der Horizon Client Aktualisierungen abrufen kann. Diese Einstellung soll in einer Umgebung verwendet werden, die ihr eigenes privates/ persönliches Aktualisierungszentrum aufweist. Wenn sie nicht aktiviert ist, wird der offizielle VMware-Aktualisierungsserver verwendet.

USB-Einstellungen für Client-GPOs

Sie können USB-Richtlinieneinstellungen für Horizon Agent und Horizon Client definieren. Bei der Verbindung lädt Horizon Client die USB-Richtlinieneinstellungen von Horizon Agent herunter und verwendet diese Einstellungen zusammen mit den Horizon Client-USB-Richtlinieneinstellungen, um zu bestimmen, welche Geräte für die Umleitung vom Hostcomputer zur Verfügung stehen.

Richtlinieneinstellungen zum Splitten von USB-Verbundgeräten

In der folgenden Tabelle werden die Richtlinieneinstellungen zum Splitten von USB-Verbundgeräten in der ADMX-Vorlagendatei für die Horizon Client-Konfiguration beschrieben. Die Einstellungen gelten auf Computerebene. Die Einstellungen aus dem GPO auf Computerebene haben Vorrang vor der Registrierung unter `HKLM\Software\Policies\VMware, Inc \VMware VDM\Client\USB`. Die Einstellungen befinden sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.

Weitere Informationen zur Verwendung von Richtlinien zur Steuerung der USB-Umleitung finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Tabelle 3-9. Konfigurationsvorlage für Horizon Client: Einstellungen für die USB-Aufteilung

Einstellung	Beschreibung
`Allow Auto Device Splitting`	Lässt das automatische Splitten von Composite USB-Geräten zu. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
`Exclude Vid/Pid Device From Split`	Schließt ein Composite USB-Gerät vom Splitten aus, das durch Anbieter- und Produkt-IDs angegeben ist. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (**`*`**) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid-0781_pid-55**`** Der Standardwert ist nicht definiert.
`Split Vid/Pid Device`	Behandelt die Komponenten eines Composite USB-Gerätes, die durch Anbieter- und Produkt-IDs angegeben sind, als separate Geräte. Das Format der Einstellung ist `vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*`[;exintf:`*ww* `])` Sie können das Stichwort `exintf` verwenden, um Komponenten durch Angabe ihrer Schnittstellennummer von der Umleitung auszuschließen. Sie müssen hexadezimale ID-Nummern und dezimale Schnittstellennummern einschließlich der 0 am Anfang angeben. Sie können das Platzhalterzeichen (**`*`**) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid-0781_pid-554c(exintf:01;exintf:02)`** **Hinweis** Horizon schließt nicht automatisch die Komponenten ein, die Sie nicht explizit ausgeschlossen haben. Sie müssen eine Filterrichtlinie wie z. B. `Include Vid/Pid Device` angeben, um diese Komponenten einzuschließen. Der Standardwert ist nicht definiert.

Richtlinieneinstellungen zum Filtern von USB-Geräten

In der folgenden Tabelle werden die in der ADMX-Vorlagendatei für die Horizon Client-Konfiguration enthaltenen Richtlinieneinstellungen für die Filterung von USB-Geräten beschrieben. Die Einstellungen gelten auf Computerebene. Die Einstellungen aus dem GPO auf Computerebene haben Vorrang vor der Registrierung unter `HKLM\Software\Policies\VMware, Inc \VMware VDM\Client\USB`.

Weitere Informationen zur Konfiguration von Filterrichtlinieneinstellungen für die USB-Umleitung finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Tabelle 3-10. Konfigurationsvorlage für Horizon Client: Einstellungen für USB-Filter

Einstellung	Beschreibung
`Allow Audio Input Devices`	Lässt zu, dass Audioeingabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.
`Allow Audio Output Devices`	Lässt zu, dass Audioausgabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 3-10. Konfigurationsvorlage für Horizon Client: Einstellungen für USB-Filter (Fortsetzung)

Einstellung	Beschreibung
`Allow HID-Bootable`	Ermöglicht die Umleitung anderer Eingabegeräte als Tastaturen und Mäusen, die zur Startzeit verfügbar sind (auch als „HID-startfähige Geräte“ bezeichnet). Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.
`Allow Device Descriptor Failsafe Behavior`	Ermöglicht die Umleitung der Geräte, auch wenn Horizon Client die Konfigurations-/Gerätebeschreibungen nicht abrufen kann. Um ein Gerät trotz Fehler in der Konfiguration/Beschreibung zuzulassen, muss dieses in den Filter „Include“ eingeschlossen werden, zum Beispiel in `IncludeVidPid` oder `IncludePath`. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration > Einstellungen können nicht vom Agenten konfiguriert werden** im Gruppenrichtlinienverwaltungs-Editor.
`Allow Other Input Devices`	Lässt zu, dass Eingabegeräte außer HID-startfähigen Geräten oder Tastaturen mit integrierten Zeigegeräten umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.
`Allow Keyboard and Mouse Devices`	Lässt zu, dass Tastaturen mit eingebauten Zeigegeräten (Maus, Trackball oder Touchpad) umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.
`Allow Smart Cards`	Lässt zu, dass Smartcard-Geräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.
`Allow Video Devices`	Lässt zu, dass Videogeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.
`Disable Remote Configuration`	Deaktiviert die Verwendung der Agent-Einstellungen beim Durchführen der USB-Gerätefilterung. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration > Einstellungen können nicht vom Agenten konfiguriert werden** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 3-10. Konfigurationsvorlage für Horizon Client: Einstellungen für USB-Filter (Fortsetzung)

Einstellung	Beschreibung
`Exclude All Devices`	Schließt alle USB-Geräte von der Umleitung aus. Wenn für diese Einstellung **`true`** festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zuzulassen, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn für diese Einstellung **`false`** festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zu verhindern, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn Sie den Wert von `Exclude All Devices` im Agent auf **`true`** setzen und diese Einstellung an Horizon Client weitergegeben wird, überschreibt die Agent-Einstellung die Horizon Client-Einstellung. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.

`Exclude Automatically Connection Device Family`	Schließt Gerätefamilien automatisch von der Weiterleitung aus. Verwenden Sie die folgende Syntax:
	`family_name[;...]`
	Beispiel:
	`storage;hid`

`Exclude Automatically Connection Vid/Pid Device`	Schließt Geräte, auf denen bestimmte Anbieter und Produkt-IDs vorhanden sind, von der automatischen Weiterleitung aus. Verwenden Sie die folgende Syntax:
	`vid-xxxx_pid-xxxx|*[;...]`
	Beispiel:
	`vid-0781_pid-554c;vid-0781_pid-9999`

`Exclude Device Family`	Schließt Gerätefamilien von der Umleitung aus. Das Format der Einstellung lautet *Familienname_1*[`;`*Familienname_2*]... Beispiel: **`bluetooth;smart-card`** Wenn Sie das automatische Gerätesplitten aktiviert haben, prüft Horizon die Gerätefamilie jeder Schnittstelle eines USB-Verbundgeräts, um zu entscheiden, welche Schnittstellen ausgeschlossen werden. Wenn Sie das automatische Gerätesplitten deaktiviert haben, prüft Horizon die Gerätefamilie des gesamten Composite USB-Gerätes. Der Standardwert ist nicht definiert. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.
`Exclude Vid/Pid Device`	Schließt Geräte mit spezifischen Anbieter- oder Produkt-IDs von der Umleitung aus. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (**`*`**) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid-0781_pid-****;vid-0561_pid-554c`** Der Standardwert ist nicht definiert. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 3-10. Konfigurationsvorlage für Horizon Client: Einstellungen für USB-Filter (Fortsetzung)

Einstellung	Beschreibung
`Exclude Path`	Schließt Geräte an angegebenen Hub- oder Portpfaden von der Umleitung aus. Das Format der Einstellung lautet `bus-`*x1*`[/`*y1*`]…/port-`*z1*`[;bus-`*x2*`[/`*y2*`]…/port-`*z2*`]…` Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden. Beispiel: **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** Der Standardwert ist nicht definiert. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration > Einstellungen können nicht vom Agenten konfiguriert werden** im Gruppenrichtlinienverwaltungs-Editor.
`Include Device Family`	Bestimmt Gerätefamilien, die umgeleitet werden können. Das Format der Einstellung lautet *Familienname_1*`[;`*Familienname_2*`]…` Beispiel: **`storage`** Der Standardwert ist nicht definiert. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.
`Include Path`	Schließt Geräte an angegebenen Hub- oder Portpfaden in die Umleitung ein. Das Format der Einstellung lautet `bus-`*x1*`[/`*y1*`]…/port-`*z1*`[;bus-`*x2*`[/`*y2*`]…/port-`*z2*`]…` Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden. Beispiel: **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** Der Standardwert ist nicht definiert. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration > Einstellungen können nicht vom Agenten konfiguriert werden** im Gruppenrichtlinienverwaltungs-Editor.
`Include Vid/Pid Device`	Gibt USB-Geräte mit einer angegebenen Anbieter- und Produkt-ID an, die umgeleitet werden können. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]…` Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (**`*`**) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid-0561_pid-554c`** Der Standardwert ist nicht definiert. Diese Einstellung befindet sich im Ordner **VMware Horizon Client-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.

Überlegungen zu geschachtelten Sitzungen

Im geschachtelten Modus oder in einem Doppelhop-Szenario stellt ein Benutzer eine Verbindung von seinem physischen Clientsystem mit einem Remote-Desktop her, startet Horizon Client innerhalb des Remote-Desktops (die geschachtelte Sitzung) und stellt eine Verbindung mit einem anderen Remote-Desktop her. Damit das Gerät wie erwartet in der geschachtelten Sitzung funktioniert, müssen Sie die USB-Richtlinieneinstellungen auf dem physischen Client Computer so konfigurieren wie in der geschachtelten Sitzung.

VMware Browser-Umleitungseinstellungen für Client-GPOs

Sie können Gruppenrichtlinieneinstellungen für die Browser-Umleitungsfunktion konfigurieren.

In der folgenden Tabelle werden die in der ADMX-Vorlagendatei für die Horizon Client-Konfiguration enthaltenen Einstellungen für die Browser-Umleitung beschrieben. Alle Einstellungen für die Browser-Umleitung sind Computer-Konfigurationseinstellungen. Die Einstellungen befinden sich im Ordner **VMware Horizon Client-Konfiguration > VMware Browserumleitung** im Gruppenrichtlinienverwaltungs-Editor.

Informationen zu den Einstellungen für die Agent-seitige Browser-Umleitung finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Tabelle 3-11. Horizon Client-Konfigurationsvorlage: VMware Browser-Umleitungseinstellungen

Einstellung	Beschreibung
`Enable WebRTC camera and microphone access for browser redirection`	Wenn diese Einstellung aktiviert ist, haben umgeleitete Seiten, die WebRTC verwenden, Zugriff auf die Kamera und das Mikrofon des Clientsystems. Diese Einstellung ist standardmäßig aktiviert.
`Ignore certificate errors for browser redirection`	Wenn diese Einstellung aktiviert ist, werden Zertifikatsfehler, die auf der umgeleiteten Seite auftreten, ignoriert und das Browsing wird fortgesetzt. Diese Einstellung ist standardmäßig deaktiviert.
`Enable cache for browser redirection`	Wenn diese Einstellung aktiviert ist, wird der Browsing-Verlauf, einschließlich der Cookies, auf dem Clientsystem gespeichert. **Hinweis** Durch das Deaktivieren dieser Einstellung wird der Cache nicht gelöscht. Wenn Sie diese Einstellung deaktivieren und dann erneut aktivieren, wird der Cache wieder verwendet. Diese Einstellung ist standardmäßig aktiviert.

Einstellungen für VMware Integrated Printing für Client-GPOs

Sie können Gruppenrichtlinieneinstellungen für die Funktion „VMware Integrated Printing“ konfigurieren.

In der folgenden Tabelle werden die in der ADMX-Vorlagendatei für die Horizon Client-Konfiguration enthaltenen Einstellungen für VMware Integrated Printing beschrieben. Die Tabelle zeigt, ob die Konfiguration sowohl die Einstellung „Computer-Konfiguration“ als auch die Einstellung „Benutzerkonfiguration“ enthält oder nur die Einstellung „Computerkonfiguration“. Bei den Einstellungen, die beide Einstellungstypen einschließen, setzt die Einstellung für die Benutzerkonfiguration hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft. Die Einstellungen befinden sich im Ordner **VMware Horizon Client-Konfiguration > VMware Integrated Printing** im Gruppenrichtlinienverwaltungs-Editor.

Informationen zu den Agent-seitigen Einstellungen für VMware Integrated Printing finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Tabelle 3-12. Horizon Client-Konfigurationsvorlage: Einstellungen für VMware Integrated Printing

Einstellung	Computer	Benutzer	Beschreibung
`Do not redirect client printer(s)`	X	X	Bestimmt, ob Clientdrucker umgeleitet werden. Wenn diese Einstellung aktiviert ist, werden keine Clientdrucker umgeleitet. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, werden alle Clientdrucker umgeleitet. Diese Einstellung ist standardmäßig nicht konfiguriert.
`Allow to redirect L1 local printers to inner session`	X	X	Legt fest, ob die Option „bis Umleiten von lokalen L1-Druckern an interne Sitzung“ zugelassen wird. VMware unterstützt das Ausführen von Horizon Client auf einem Remotedesktop. Diese Konfiguration, allgemein als „geschachtelter Modus“ bezeichnet, umfasst drei Schichten und zwei Hops, und zwar wie folgt: ■ L0 (Endpoint): Physischer Computer, auf dem Horizon Client installiert ist. ■ L1 (Remotedesktop des ersten Hops): Der Remote-Desktop, auf dem Horizon Client und Horizon Agent installiert sind. ■ L2 (veröffentlichter Desktop oder veröffentlichte Anwendung für zweiten Hop): Der veröffentlichte Desktop oder die veröffentlichte Anwendung, mit der der Client für den zweiten Hop eine Verbindung herstellt. Wenn diese Einstellung aktiviert ist, werden die lokalen L1-Drucker zur inneren Sitzung umgeleitet. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, werden die lokalen L1-Drucker nicht an die interne Sitzung umgeleitet. Diese Einstellung ist standardmäßig nicht konfiguriert.

ADMX-Vorlageneinstellungen für PCoIP-Client-Sitzungsvariablen

Die ADMX-Vorlagendatei für PCoIP-Client-Sitzungsvariablen (`pcoip.client.admx`) enthält Richtlinieneinstellungen in Bezug auf das PCoIP-Anzeigeprotokoll. Sie können Computerstandardwerte konfigurieren, die ein Administrator außer Kraft setzen kann, oder Sie können Benutzereinstellungen konfigurieren, die ein Administrator nicht außer Kraft setzen kann. Die Einstellungen, die außer Kraft gesetzt werden können, befinden sich im Ordner **PCoIP Client Session Variables > Overridable Administrator Defaults** im Gruppenrichtlinienverwaltungs-Editor. Die Einstellungen, die nicht außer Kraft gesetzt werden können, befinden sich im Ordner **PCoIP Client Session Variables > Not Overridable Settings** im Gruppenrichtlinienverwaltungs-Editor.

Die ADMX-Dateien stehen in `VMware-Horizon-Extras-Bundle-`*`YYMM-x.x.x-yyyyyyyy`*`.zip` zur Verfügung. Diese Datei können Sie von der VMware-Download-Site unter https://my.vmware.com/web/vmware/downloads herunterladen. Wählen Sie unter „Desktop und End-User Computing“ den VMware Horizon-Download, der das GPO-Bundle mit der ZIP-Datei enthält.

Tabelle 3-13. PCoIP-Client-Sitzungsvariablen

Einstellung	Beschreibung
`Configure PCoIP client image cache size policy`	Reguliert die Größe des PCoIP-Client-Bildcaches. Der Client verwendet die Bild-Zwischenspeicherung, um Teile der vorab übertragenen Anzeige zu speichern. Durch die Bild-Zwischenspeicherung wird die Menge der erneut übermittelten Daten minimiert. Ist diese Einstellung deaktiviert, verwendet PCoIP eine Standard-Clientbildcachegröße von 250 MB. Bei Aktivierung dieser Einstellung können Sie die Client-Bildcachegröße von mindestens 50 MB auf 300 MB konfigurieren. Der Standardwert ist 250 MB. Diese Einstellung ist standardmäßig deaktiviert.
`Configure PCoIP event log cleanup by size in MB`	Aktiviert die Konfiguration der PCoIP-Ereignisprotokollbereinigung nach Größe in MB. Wenn diese Einstellung konfiguriert ist, wird damit die Bereinigung der Protokolldateien nach Größe in MB gesteuert. So werden beispielsweise bei einer Einstellung von *m* ungleich null Protokolldateien größer als *m* MB unbeaufsichtigt gelöscht. Die Einstellung 0 legt fest, dass keine Dateibereinigung nach Größe durchgeführt wird. Wenn diese Einstellung deaktiviert ist, gilt für die Ereignisprotokollbereinigung nach Größe in MB standardmäßig der Wert 100. Diese Einstellung ist standardmäßig deaktiviert.
`Configure PCoIP event log cleanup by time in days`	Aktiviert die Konfiguration der PCoIP-Ereignisprotokollbereinigung nach Zeit in Tagen. Wenn diese Einstellung konfiguriert ist, wird damit die Bereinigung der Protokolldateien nach Zeit in Tagen gesteuert. So werden beispielsweise bei einer Einstellung von *n* ungleich null Protokolldateien älter als *n* Tage unbeaufsichtigt gelöscht. Die Einstellung 0 legt fest, dass keine zeitlich festgelegte Dateibereinigung durchgeführt wird. Wenn diese Richtlinie deaktiviert ist, gilt für die Ereignisprotokollbereinigung nach Zeit in Tagen standardmäßig der Wert 7. Diese Einstellung ist standardmäßig deaktiviert. Die Bereinigung der Protokolldatei wird einmal beim Start der Sitzung ausgeführt. Jede Änderung der Einstellung wird erst bei der nächsten Sitzung angewendet.
`Configure PCoIP event log verbosity`	Legt die Ausführlichkeit der PCoIP-Ereignisprotokolle fest. Sie können einen Wert zwischen 0 (geringste Ausführlichkeit) und 3 (höchste Ausführlichkeit) festlegen. Wenn diese Einstellung aktiviert ist, können Sie die Ausführlichkeit von 0 auf 3 ändern. Wenn diese Einstellung deaktiviert ist, gilt für die Ausführlichkeit des Ereignisprotokolls standardmäßig der Wert 2. Diese Einstellung ist standardmäßig deaktiviert. Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, ist die neue Einstellung umgehend wirksam.
`Configure PCoIP session encryption algorithms`	Steuert die Verschlüsselungsalgorithmen, die vom PCoIP-Endpunkt während der Sitzungsaushandlung angeboten werden. Durch Aktivierung eines Kontrollkästchens wird der entsprechende Verschlüsselungsalgorithmus deaktiviert. Sie müssen mindestens einen Algorithmus aktivieren. Diese Einstellung gilt sowohl für den Agenten als auch für den Client. Die Endpunkte handeln den tatsächlich verwendeten Algorithmus für die Sitzungsverschlüsselung aus. Wenn der FIPS140-2-validierte Modus aktiviert ist, wird der Wert für **Disable AES-128-GCM encryption (AES-128-GCM-Verschlüsselung deaktivieren)** außer Kraft gesetzt, wenn sowohl die AES-128-GCM- als auch die AES-256-GCM-Verschlüsselung deaktiviert ist. Wenn die `Configure SSL Connections`-Einstellung deaktiviert wurde, stehen die Algorithmen Salsa20-256round12 und AES-128-GCM zur Aushandlung durch diesen Endpunkt zur Verfügung. Diese Einstellung ist standardmäßig deaktiviert. Unterstützte Verschlüsselungsalgorithmen sind in der bevorzugten Reihenfolge SALSA20/12-256, AES-GCM-128 und AES-GCM-256. Standardmäßig sind alle unterstützten Verschlüsselungsalgorithmen zur Aushandlung durch diesen Endpunkt verfügbar.

Tabelle 3-13. PCoIP-Client-Sitzungsvariablen (Fortsetzung)

Einstellung	Beschreibung
`Configure PCoIP virtual channels`	Gibt die virtuellen Kanäle an, die bei PCoIP-Sitzungen verwendet bzw. nicht verwendet werden können. Diese Einstellung legt auch fest, ob die Zwischenablageverarbeitung auf dem PCoIP-Host deaktiviert wird. Virtuelle Kanäle, die in PCoIP-Sitzungen verwendet werden, müssen in der Tabelle der autorisierten virtuellen Kanäle aufgeführt sein. Virtuelle Kanäle, die in der Ausschlussliste für virtuelle Kanäle erscheinen, können in PCoIP-Sitzungen nicht verwendet werden. Sie können maximal 15 virtuelle Kanäle zur Verwendung in PCoIP-Sitzungen angeben. Trennen Sie mehrere Kanäle durch einen senkrechten Strich (|) voneinander. Die Zeichenfolge zum Zulassen der virtuellen Kanäle „mksvchan“ und „vdp_rdpvcbridge“ lautet z.B. **`mksvchan|vdp_rdpvcbridge`**. Wenn ein Kanalname einen senkrechten Strich oder einen umgekehrten Schrägstrich (\) enthält, fügen Sie vor dem Kanalnamen einen umgekehrten Schrägstrich ein. Der Kanalname „awk|ward\channel“ wird beispielsweise folgendermaßen eingegeben: **`awk\\|ward\\channel`**. Ist die Tabelle der autorisierten virtuellen Kanäle leer, ist die Verwendung von virtuellen Kanälen nicht zulässig. Ist die Ausschlusstabelle für virtuelle Kanäle leer, sind alle virtuellen Kanäle zugelassen. Die Einstellung der virtuellen Kanäle gilt sowohl für den Agenten als auch für den Client. Zum Verwenden virtueller Kanäle müssen diese sowohl auf dem Agenten als auch auf dem Client aktiviert werden. Bei Festlegung der virtuellen Kanäle wird ein separates Kontrollkästchen angezeigt, mit dem Sie die Remote-Zwischenablageverarbeitung auf dem PCoIP-Host deaktivieren können. Dieser Wert gilt nur für den Agent. Standardmäßig sind alle virtuellen Kanäle aktiviert, einschließlich der Zwischenablageverarbeitung.
`Configure SSL cipher list`	Konfiguriert eine TLS/SSL-Verschlüsselungsliste, um die Verwendung der Verschlüsselungs-Suites zu beschränken, bevor eine verschlüsselte TLS/SSL-Verbindung hergestellt wird. Die Verschlüsselungsliste besteht aus einer oder mehreren Zeichenfolgen der Verschlüsselungs-Suite, die durch Doppelpunkte voneinander getrennt werden. Bei allen Zeichenfolgen der Verschlüsselungs-Suite muss die Groß- und Kleinschreibung beachtet werden. Der Standardwert lautet: ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH. Wenn diese Einstellung konfiguriert ist, wird das Kontrollkästchen **AES-256 oder stärkere Verschlüsselungen für die Aushandlung der SSL-Verbindung erzwingen** in der Einstellung `Configure SSL connections to satisfy Security Tools` ignoriert. Diese Einstellung muss sowohl auf den PCoIP Server wie auf den PCoIP Client angewendet werden.

Tabelle 3-13. PCoIP-Client-Sitzungsvariablen (Fortsetzung)

Einstellung	Beschreibung
`Configure SSL connections to satisfy Security Tools`	Legt fest, wie Verbindungen mit TLS-Sitzungsaushandlung aufgebaut werden. Aktivieren Sie diese Einstellung für Sicherheitstools wie Portscanner und führen Sie folgende Schritte durch: 1 Speichern Sie das Zertifikat der Zertifizierungsstelle, die alle Serverzertifikate zur Verwendung mit PCoIP im Zertifikatspeicher für vertrauenswürdige Stammzertifikate signiert hat. 2 Konfigurieren Sie den Agenten zum Laden von Zertifikaten aus dem Zertifikatspeicher. Wenn der persönliche Informationsspeicher für den lokalen Computer verwendet wird, belassen Sie den Namen des CA-Zertifikatspeichers bei ROOT, solange in Schritt 1 kein anderer Speicherort verwendet wurde. Wenn diese Einstellung deaktiviert ist, ist die AES-128-Verschlüsselungs-Suite nicht verfügbar, und der Endpoint verwendet Zertifizierungsstellenzertifikate aus dem MY Store des Computerkontos und aus dem ROOT Store. Diese Einstellung ist standardmäßig deaktiviert.
`Configure SSL protocols`	Konfiguriert das OpenSSL-Protokoll, um die Verwendung bestimmter Protokolle zu unterbinden, bevor eine verschlüsselte TLS-Verbindung hergestellt wird. Die Protokollliste besteht aus mindestens einer durch Doppelpunkte getrennten OpenSSL-Protokollzeichenfolge. Bei allen Verschlüsselungszeichenfolgen muss die Groß-und Kleinschreibung beachtet werden. Der Standardwert lautet: `TLS1.1:TLS1.2`. Damit wird Folgendes festgelegt: TLS v1.1 und TLS v1.2 sind aktiviert, SSL v2.0, SSL v3.0 und TLS v1.0 sind deaktiviert. Wenn diese Einstellung sowohl im Client als auch im Agent festgelegt ist, wird die Regel für die OpenSSL-Protokollaushandlung angewendet.
`Configure the Client PCoIP UDP port`	Gibt den UDP-Port an, der von Software-PCoIP-Clients verwendet wird. Der Wert des UDP-Ports gibt den zu verwendenden Basisport vor. Wenn der Basisport nicht verfügbar ist, bestimmt der Wert des UDP-Portbereichs, wie viele zusätzliche Ports ausprobiert werden. Der Bereich erstreckt sich vom Basisport bis zur Summe aus Basisport und Portbereich. Wenn der Basisport beispielsweise 50002 lautet und der Portbereich auf 64 festgelegt ist, umfasst der Bereich die Ports 50002 bis 50066. Diese Einstellung gilt nur für den Client. Standardmäßig lautet der Basisport 50002 und der Portbereich ist auf 64 festgelegt.

Tabelle 3-13. PCoIP-Client-Sitzungsvariablen (Fortsetzung)

Einstellung	Beschreibung
`Configure the maximum PCoIP session bandwidth`	Legt die maximale Bandbreite für eine PCoIP-Sitzung in Kilobits pro Sekunde fest. Die Bandbreite umfasst den gesamten Sitzungsdatenverkehr, Bilddarstellung, Audio, virtuelle Kanäle, USB und PCoIP-Steuerung eingeschlossen. Legen Sie diesen Wert auf die Gesamtkapazität der Verbindung fest, mit der Ihr Endpunkt verbunden ist, und berücksichtigen Sie dabei die Anzahl der erwarteten gleichzeitigen PCoIP-Sitzungen. Beispiel: Legen Sie diesen Wert bei einer Einzelbenutzer-VDI-Konfiguration (eine einzelne PCoIP-Sitzung), die über eine Internetverbindung mit 4 MBit/s verbunden ist, auf 4 MBit oder auf 90 % dieses Werts fest, um etwas Spielraum für anderen Netzwerkdatenverkehr zu lassen. Wenn Sie erwarten, dass sich mehrere gleichzeitige PCoIP-Sitzungen, die entweder mehrere VDI-Benutzer oder eine RDS-Konfiguration umfassen, einen Link teilen, können Sie die Einstellung entsprechend anpassen. Durch eine Senkung dieses Werts wird jedoch die maximale Bandbreite für jede aktive Sitzung beschränkt. Durch eine Festlegung dieses Werts verhindern Sie, dass der Agent eine die Verbindungskapazität übersteigende Übertragungsrate wählt – was zu einem übermäßigen Paketverlust und einem schlechteren Benutzererlebnis führen würde. Dieser Wert ist symmetrisch. Client und Agent werden gezwungen, den niedrigeren der beiden Werte zu verwenden, die auf Client- und Agentseite festgelegt sind. Beispielsweise wird der Agent bei Festlegung einer maximalen Bandbreite von 4 MBit/s gezwungen, eine niedrigere Übertragungsrate zu verwenden – auch wenn die Einstellung auf dem Client konfiguriert ist. Wenn diese Einstellung auf einem Endpunkt deaktiviert wurde, legt der Endpunkt keine Bandbreiteneinschränkungen fest. Wenn diese Einstellung konfiguriert ist, wird sie als maximale Bandbreiteneinschränkung des Endpunkts in KBit/s verwendet. Der Standardwert lautet 900.000 KBit (1 GBit) pro Sekunde. Diese Einstellung gilt sowohl für den Agenten als auch für den Client. Haben die beiden Endpunkte unterschiedliche Einstellungen, wird der niedrigere Wert verwendet.
`Configure the PCoIP session bandwidth floor`	Legt die Mindestbandbreite in Kilobits pro Sekunde fest, die von der PCoIP-Sitzung reserviert wird. Mit dieser Einstellung wird die minimale erwartete Bandbreitenübertragungsrate für den Endpunkt konfiguriert. Wenn Sie diese Einstellung zum Reservieren der Bandbreite für einen Endpunkt verwenden, muss der Benutzer nicht warten, bis Bandbreite verfügbar ist, was die Reaktionszeit während der Sitzung verbessert. Achten Sie jedoch darauf, dass Sie allen Endpunkten gemeinsam nicht mehr Bandbreite zuweisen, als insgesamt zur Verfügung steht. Die Summe der Mindestbandbreitenwerte für alle Verbindungen in Ihrer Konfiguration darf die Netzwerkkapazität nicht überschreiten. Der Standardwert lautet 0, d.h. es wird keine Mindestbandbreite reserviert. Wenn diese Einstellung deaktiviert wurde, wird keine Mindestbandbreite reserviert. Diese Einstellung ist standardmäßig deaktiviert. Diese Einstellung gilt sowohl für den Agenten als auch für den Client, wirkt sich allerdings nur auf den Endpunkt aus, für den sie konfiguriert wurde. Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, wird die Änderung umgehend wirksam.

Tabelle 3-13. PCoIP-Client-Sitzungsvariablen (Fortsetzung)

Einstellung	Beschreibung
`Configure the PCoIP session MTU`	Legt die Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, MTU) für UDP-Pakete bei einer PCoIP-Sitzung fest. Die MTU-Größe umfasst den IP- und UDP-Paketvorspann. TCP verwendet den standardmäßigen MTU-Ermittlungsmechanismus zum Festlegen der MTU. Diese Einstellung hat keine Auswirkung darauf. Die maximale MTU-Größe beträgt 1.500 Byte. Die minimale MTU-Größe beträgt 500 Byte. Der Standardwert lautet 1.300 Byte. Normalerweise muss die MTU-Größe nicht geändert werden. Ändern Sie diesen Wert, wenn Sie in einer nicht standardmäßig eingerichteten Netzwerkumgebung arbeiten, die zu einer PCoIP-Paketfragmentierung führt. Diese Einstellung gilt sowohl für den Agenten als auch für den Client. Unterscheiden sich die MTU-Größeneinstellungen der beiden Endpunkte, wird der niedrigere Wert verwendet. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, verwendet der Client bei der Aushandlung mit dem Agenten den Standardwert.
`Configure the PCoIP transport header`	Konfiguriert den PCoIP-Übertragungsheader und legt die Priorität der Transportsitzung fest. Der PCoIP-Übertragungsheader ist ein 32-Bit-Header, der zu allen PCoIP-UDP-Paketen hinzugefügt wird (sofern der Übertragungsheader aktiviert ist und von beiden Seiten unterstützt wird). Anhand des PCoIP-Übertragungsheaders können Netzwerkgeräte bei Netzwerkkonflikten eine bessere Priorisierung vornehmen bzw. bessere QoS-Entscheidungen treffen. Der Übertragungsheader ist standardmäßig aktiviert. Die Priorität einer Transportsitzung bestimmt die PCoIP-Sitzungspriorität, die im PCoIP-Übertragungsheader angegeben wird. Netzwerkgeräte können basierend auf der angegebenen Priorität einer Transportsitzung eine bessere Priorisierung vornehmen und bessere QoS-Entscheidungen treffen. Bei Aktivierung der Einstellung `Configure the PCoIP transport header` sind die folgenden Prioritäten für eine Transportsitzung verfügbar: ■ **Hoch** ■ **Mittel** (Standardwert) ■ **Niedrig** ■ **Nicht definiert** Der PCoIP-Agent und der Client handeln den Prioritätswert der Transportsitzung aus. Wenn der PCoIP-Agent einen Prioritätswert für die Transportsitzung angibt, wird die vom Agent angegebene Sitzungspriorität für die Sitzung verwendet. Wenn nur auf dem Client eine Priorität für die Transportsitzung angegeben ist, wird die vom Client angegebene Priorität für die Sitzung verwendet. Wenn weder der Agent noch der Client eine Priorität für die Transportsitzung angibt oder der Wert **Nicht definiert** festgelegt wurde, wird der Standardwert (**Mittel**) für die Sitzung verwendet.
`Enable/disable audio in the PCoIP session`	Legt fest, ob die Audiofunktion während PCoIP-Sitzungen aktiviert ist. Die Audiofunktion muss für beide Endpunkte aktiviert sein. Ist diese Einstellung aktiviert, ist die Verwendung von PCoIP-Audio zulässig. Wurde diese Einstellung deaktiviert, kann die PCoIP-Audiofunktion nicht verwendet werden. Audio ist standardmäßig aktiviert.

Ausführen von Horizon Client über die Befehlszeile

Sie können Horizon Client von der Befehlszeile aus oder über Skripte ausführen. Sie sollten Horizon Client möglicherweise über die Befehlszeile ausführen, wenn Sie eine kioskbasierte

Anwendung implementieren, die Endbenutzern Zugriff auf Remote-Desktop-Anwendungen gewährt.

Um Horizon Client über die Befehlszeile auszuführen, verwenden Sie den Befehl `vmware-view.exe`. Der Befehl `vmware-view.exe` umfasst Optionen, die Sie angeben können, um das Verhalten von Horizon Client zu ändern.

Horizon Client-Befehlsverwendung

Die Syntax des Befehls `vmware-view` legt fest, wie Horizon Client ausgeführt wird.

Verwenden Sie den Befehl `vmware-view` an einer Windows-Eingabeaufforderung mit dem folgenden Format.

```
vmware-view [Befehlszeilenoption [Argument]] ...
```

Der Standardpfad zur ausführbaren Datei des Befehls `vmware-view` ist vom Clientsystem abhängig. Sie können diesen Pfad auf dem Clientsystem zur Umgebungsvariable *PATH* hinzufügen.

- 32-Bit-Systeme: `C:\Programme\VMware\VMware Horizon View Client\`
- 64-Bit-Systeme: `C:\Programme (x86) \VMware\VMware Horizon View Client\`

In der folgenden Tabelle sind die Befehlszeilenoptionen aufgeführt, die mit dem Befehl `vmware-view` verwendet werden können.

Tabelle 3-14. Horizon Client-Befehlszeilenoptionen

Option	Beschreibung
`/?`	Zeigt die Liste der Befehlsoptionen an.
`-appName` *Anwendungsname*	Gibt den Namen der veröffentlichten Anwendung an, der im Dialogfeld zur Desktop- und Anwendungsauswahl angezeigt wird. Hierbei handelt es sich um den Anzeigenamen, der für den Anwendungspool im Assistenten zur Poolerstellung angegeben wurde.
`-appProtocol` *Protokoll*	Legt das Anzeigeprotokoll fest, das für die veröffentlichte Anwendung verwendet wird, falls verfügbar. Die gültigen Protokolle lauten wie folgt: ■ **`VMware Blast`** ■ **`PCoIP`**

Tabelle 3-14. Horizon Client-Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung
`–appSessionReconnectionBehavior` *argument*	Legt die Einstellung für das Wiederverbindungsverhalten von veröffentlichten Anwendungen fest. Die gültigen Argumente lauten wie folgt: **`always`** Implementiert die Einstellung **Neuverbindung zum Öffnen von Anwendungen automatisch herstellen**. **`never`** Implementiert die Einstellung **Vor Neuverbindung nicht fragen und nicht automatisch neu verbinden**. **`ask`** Implementiert die Einstellung **Vor Neuverbindung zum Öffnen von Anwendungen fragen**. Wenn Sie diese Option verwenden, werden die Einstellungen für die Wiederverbindung von veröffentlichten Anwendungen in Horizon Client deaktiviert.
`–args` *argument*	Gibt Befehlszeilenargumente zum Hinzufügen an, wenn eine veröffentlichte Anwendung gestartet wird. Beispiel: `vmware–view.exe ––serverURL 10.10.10.10 ––appName "My Notepad++" ––args "\"my new.txt\""`
`–connectUSBOnStartup`	Wenn dies auf `true` gesetzt ist, werden alle mit dem Host verbundenen USB-Geräte an den Remote-Desktop bzw. die veröffentlichte Anwendung umgeleitet. Diese Option wird bei Angabe der Option `–unattended` für einen Remote-Desktop implizit festgelegt. Die Standardeinstellung ist `false`.
`–connectUSBOnInsert`	Verbindet bei aktivierter Option `true` ein USB-Gerät beim Anschließen des Geräts mit dem im Vordergrund angezeigten Remote-Desktop bzw. der veröffentlichten Anwendung. Diese Option wird bei Angabe der Option `–unattended` für einen Remote-Desktop implizit festgelegt. Die Standardeinstellung ist `false`.
`–desktopLayout` *Fenstergröße*	Gibt an, wie das Remote-Desktop-Fenster angezeigt werden soll. Die gültigen Werte für die Fenstergröße lauten wie folgt: **`fullscreen`** Vollbildanzeige. **`multimonitor`** Mehrfachmonitoranzeige. **`windowLarge`** Großes Fenster. **`windowSmall`** Kleines Fenster. **`length X width`** Benutzerdefinierte Größe, z. B. 800 x 600.
`–desktopName` *Desktop-Name*	Gibt den Namen des Remote-Desktops an, der im Dialogfeld zur Desktop- und Anwendungsauswahl angezeigt wird. Hierbei handelt es sich um den Anzeigenamen, der für den Pool im Assistenten zur Poolerstellung angegeben wurde. **Wichtig** Geben Sie diese Option für Clients im Kiosk-Modus nicht an. Diese Option bleibt wirkungslos, wenn der Remote-Desktop im Kiosk-Modus ausgeführt wird. Im Kiosk-Modus wird die Verbindung zum ersten Remote-Desktop in der Liste der berechtigten Remote-Desktops hergestellt.

Tabelle 3-14. Horizon Client-Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung
`–desktopProtocol` *Protokoll*	Gibt den Namen des zu verwendenden Anzeigeprotokolls an, der im Dialogfeld zur Desktop- und Anwendungsauswahl angezeigt wird. Die gültigen Anzeigeprotokolle lauten wie folgt: ■ **`Blast`** ■ **`PCoIP`** ■ **`RDP`**
`–domainName` *Domänenname*	Gibt die NETBIOS-Domäne an, die der Endbenutzer zur Anmeldung bei Horizon Client verwendet. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.
`–file` *Dateipfad*	Gibt den Pfad einer Konfigurationsdatei mit zusätzlichen Befehlsoptionen und -argumenten an. Siehe Horizon Client-Konfigurationsdatei.
`–h`	Zeigt Hilfeoptionen an.
`–hideClientAfterLaunchSession`	Wenn diese Option auf `true` gesetzt ist, werden das Fenster für Desktop- und Anwendungsauswahl und das Menü **VMware Horizon Client anzeigen** nach dem Starten einer Remotesitzung ausgeblendet. Wenn diese Option auf `false` gesetzt ist, werden das Fenster für Desktop- und Anwendungsauswahl und das Menü **VMware Horizon Client anzeigen** nach dem Starten einer Remotesitzung angezeigt. Die Standardeinstellung ist `true`.

`–installShortcutsThenQuit`	Verwenden Sie diese Option, um Desktop- und Anwendungsverknüpfungen zu installieren, die auf dem-Server konfiguriert sind. Wenn Sie diese Option mit ausreichenden Informationen zur Serverauthentifizierung verwenden, stellt Horizon Client eine automatische Verbindung mit dem Server her, installiert die Verknüpfungen und wird dann beendet. Wenn die Serverauthentifizierung fehlschlägt, wird Horizon Client automatisch beendet.
	Um Verknüpfungen automatisch auf dem Clientsystem zu installieren, erstellen Sie ein Skript, das beim Start des Clientsystems ausgeführt wird. Beispiel:
	`vmware-view.exe –serverURL` *`serverurl`* `–userName` *`user`* `–domainName` *`domain`*
	`–password` *`password`* `–installShortcutsThenQuit`
	
	`vmware-view.exe –serverURL` *`serverurl`* `–loginAsCurrentUser true –installShortcutsThenQuit`
	
	Informationen zu vom Server erstellten Verknüpfungen finden Sie unter Verwenden von Verknüpfungen, die vom Server erstellt wurden.

`–languageId` *Gebietsschema-ID*	Bietet Lokalisierungsunterstützung für verschiedene Sprachen in Horizon Client. Wenn eine Ressourcenbibliothek verfügbar ist, geben Sie die zu verwendende Gebietsschema-ID (Locale ID, LCID) an. Für Englisch (USA) geben Sie 0x409 ein.
`–launchMinimized`	Startet Horizon Client im minimierten Modus. Wenn Sie die Option `–appName` oder `–desktopName` angeben, bleibt Horizon Client minimiert, bis die veröffentlichte Anwendung oder der Remote-Desktop gestartet wird, die bzw. der angegeben wurde. Sie können diese Option nicht mit der Option `–unattended` oder `–nonInteractive` verwenden.

Tabelle 3-14. Horizon Client-Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung

`–listMonitors`	Führt die Indexwerte auf und zeigt die Layoutinformationen für die verbundenen Monitore an. Beispiel:
	`1: (0, 0, 1920, 1200)`
	`2: (1920, 0, 3840, 1200)`
	`3: (–900, –410, 0, 1190)`
	Sie können diese Indexwerte in der Option `–monitors` verwenden.

`–logInAsCurrentUser`	Wenn hier `true` angegeben ist, werden die Anmeldedaten des Endbenutzers, die dieser zur Anmeldung beim Clientsystem eingegeben hat, zur Anmeldung beim Server und schließlich beim Remote-Desktop verwendet. Die Standardeinstellung ist `false`.
`–monitors "`*n*`[,`*n*`,`*n*`,`*n*`]"`	Gibt die Monitore an, die in einer Mehrfachmonitorumgebung verwendet werden sollen, wobei *n* der Indexwert eines Monitors ist. Sie können mit der Option `–listMonitors` die Indexwerte der verbundenen Monitore bestimmen. Es lassen sich bis zu vier Indexwerte, durch Kommas getrennt, angeben. Beispiel: `–monitors "1,2"` Diese Option ist nur wirksam, wenn für `–desktopLayout` die Einstellung `multimonitor` festgelegt ist.
`–nonInteractive`	Unterdrückt Fehlermeldungen beim Starten von Horizon Client über ein Skript. Diese Option wird bei Angabe der Option `–unattended` implizit festgelegt. **Hinweis** Wenn Sie sich bei einem Server im nicht interaktiven Modus anmelden, werden Sie nicht aufgefordert, Verknüpfungen (sofern verfügbar) für das **Startmenü** zu installieren. Die Verknüpfungen werden dann standardmäßig installiert.
`–noVMwareAddins`	Verhindert das Laden von VMware-spezifischen virtuellen Kanälen, z. B. für virtuelles Drucken.
`–password` *Kennwort*	Gibt das Kennwort an, das der Endbenutzer zur Anmeldung an Horizon Client verwendet. Das Kennwort wird von der Befehlskonsole und von jedem Skripttool im Textformat weiterverarbeitet. Wenn Sie das Kennwort automatisch generieren, müssen Sie diese Option für Clients im Kiosk-Modus nicht angeben. Zur Erhöhung der Sicherheit sollten Sie diese Option nicht angeben. Benutzer können das Kennwort interaktiv eingeben.
`–printEnvironmentInfo`	Zeigt die IP-Adresse, die MAC-Adresse und den Maschinennamen des Clientgeräts an.
`–serverURL` *Verbindungsserver*	Gibt die URL, die IP-Adresse oder den FQDN des Servers an.
`–shutdown`	Fährt alle Remote-Desktops und veröffentlichten Anwendungen sowie relevante Benutzeroberflächenkomponenten herunter.
`–singleAutoConnect`	Wenn der Benutzer nur für einen Remote-Desktop oder eine veröffentlichte Anwendung berechtigt ist, wird die Verbindung mit diesem Remote-Desktop oder dieser veröffentlichten Anwendung hergestellt, nachdem der Benutzer sich beim Server authentifiziert hat. So muss der Benutzer nicht einen Remote-Desktop oder eine veröffentlichte Anwendung aus einer Liste auswählen, die nur ein Element enthält.

Tabelle 3-14. Horizon Client-Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung
`–smartCardPIN` *PIN*	Gibt die PIN an, wenn ein Endbenutzer eine Smartcard zur Anmeldung einführt.
`–usernameHint` *Benutzername*	Gibt den Kontonamen an, der als Benutzernamenhinweis verwendet werden soll.
`–standalone`	Startet eine zweite Instanz von Horizon Client, die eine Verbindung mit demselben oder einem anderen Server herstellen kann. Diese Option wird für die Abwärtskompatibilität unterstützt. Die Angabe von `–standalone` ist nicht erforderlich, da dies das Standardverhalten für den Client ist. Für mehrere Remote-Desktop-Verbindungen zu demselben oder einem anderen Server wird der sichere Tunnel unterstützt. **Hinweis** Die zweite Remote-Desktop-Verbindung hat möglicherweise keinen Zugriff auf die lokale Hardware, wie USB-Geräte, Smartcards, Drucker und mehrere Monitore.
`–supportText` *file_name*	Gibt den vollständigen Pfad einer Textdatei an. Der Inhalt der Datei wird im Dialogfeld „Support-Informationen“ angezeigt.
`–unattended`	Startet Horizon Client im nicht interaktiven Modus, der sich für Clients im Kiosk-Modus eignet. Sie müssen auch die folgenden Informationen angeben: ■ Der Kontoname des Clients, wenn dieser nicht über die MAC-Adresse des Clientgeräts generiert wurde. Der Name muss mit der Zeichenfolge „custom-“ oder einem alternativen Präfix beginnen, das Sie in ADAM konfiguriert haben. ■ Das Kennwort des Clients, wenn dieses nicht automatisch beim Einrichten des Clientkontos generiert wurde. Über die Option `–unattended` werden die Optionen `–nonInteractive`, `–connectUSBOnStartup`, `–connectUSBOnInsert` und `–desktopLayout multimonitor` implizit festgelegt.
`–unauthenticatedAccessAccount`	Legt ein Benutzerkonto für einen nicht authentifizierten Zugriff zur anonymen Anmeldung beim Server fest, wenn der nicht authentifizierte Zugriff aktiviert ist. Wenn der nicht authentifizierte Zugriff nicht aktiviert ist, wird diese Option ignoriert. Beispiel: `vmware–view.exe –serverURL view.mycompany.com –unauthenticatedAccessEnabled true –unauthenticatedAccessAccount anonymous1`

Tabelle 3-14. Horizon Client-Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung
`–unauthenticatedAccessEnabled`	Bei Festlegung auf `true` wird der nicht authentifizierte Zugriff ermöglicht. Wenn der nicht authentifizierte Zugriff nicht verfügbar ist, kann der Client auf eine andere Authentifizierungsmethode zurückgreifen. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** wird in Horizon Client angezeigt, deaktiviert und ausgewählt. Bei `false` ist die Eingabe Ihrer Anmeldedaten für die Anmeldung bei Ihren Anwendungen und den Zugriff darauf erforderlich. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** wird in Horizon Client ausgeblendet und nicht ausgewählt. Wenn Sie diese Option nicht festlegen, haben Sie die Möglichkeit, den nicht authentifizierten Zugriff in Horizon Client zu aktivieren. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** wird angezeigt, aktiviert und nicht ausgewählt.

`–useExisting`	Ermöglicht den Start mehrerer Remote-Desktops und veröffentlichter Anwendungen aus einer einzelnen Horizon Client-Sitzung.
	Wenn Sie diese Option festlegen, ermittelt Horizon Client, ob eine Sitzung mit dem gleichen Benutzernamen, der gleichen Domäne und der gleichen Server-URL bereits vorhanden ist. Ist dies der Fall, wird diese Sitzung wiederverwendet, anstatt eine neue zu erstellen.
	Im nachfolgend aufgeführten Befehl startet user-1 beispielsweise die Anwendung „Berechnung“, und eine neue Sitzung wird erstellt.
	`vmware–view.exe –userName user–1 –password secret –domainName domain –appName Calculator –serverURL view.mycompany.com –useExisting`
	Im nächsten Befehl startet user-1 die Paint-Anwendung mit dem gleichen Benutzernamen, der gleichen Domäne und der gleichen Server-URL. Dieselbe Sitzung wird verwendet.
	`vmware–view.exe –userName user–1 –password secret –domainName domain –appName Paint –serverURL view.mycompany.com –useExisting`

`–userName` *Benutzername*	Gibt den Kontonamen an, den der Endbenutzer zur Anmeldung an Horizon Client verwendet. Wenn Sie den Kontonamen aus der MAC-Adresse des Clientgeräts generieren, müssen Sie diese Option für Clients im Kiosk-Modus nicht angeben.

Mit Ausnahme von `–file`, `–languageId`, `–printEnvironmentInfo`, `–smartCardPIN` und `–unattended` können Sie alle Optionen über Active Directory-Gruppenrichtlinien angeben.

Hinweis Gruppenrichtlinieneinstellungen haben Vorrang vor Einstellungen, die Sie über die Befehlszeile angeben.

Horizon Client-Konfigurationsdatei

Sie können Befehlszeileninformationen für Horizon Client aus einer Konfigurationsdatei auslesen.

Sie können den Pfad der Konfigurationsdatei als Argument der `–file` *file_path*-Option des Befehls `vmware–view` angeben. Bei der Datei muss es sich um eine Unicode- (UTF-16) oder um eine ASCII-Textdatei handeln.

Beispiel: Beispiel einer Konfigurationsdatei für eine nicht interaktive Anwendung

Das folgende Beispiel zeigt die Inhalte einer Konfigurationsdatei für eine nicht interaktive Anwendung.

```
–serverURL https://view.yourcompany.com
–userName autouser
–password auto123
–domainName companydomain
–desktopName autodesktop
–nonInteractive
```

Beispiel: Beispiel einer Konfigurationsdatei für einen Client im Kioskmodus

Das folgende Beispiel zeigt einen Client im Kiosk-Modus, dessen Kontoname auf seiner MAC-Adresse basiert. Der Client verwendet ein automatisch generiertes Kennwort.

```
–serverURL 145.124.24.100
–unattended
```

Konfigurieren des Horizon Client mithilfe der Windows-Registrierung

Sie können Standardeinstellungen für Horizon Client in der Windows-Registrierung definieren, anstatt diese Einstellungen über die Befehlszeile anzugeben. Gruppenrichtlinieneinstellungen haben Vorrang vor Windows-Registrierungseinstellungen. Windows-Registrierungseinstellungen haben wiederum Vorrang vor der Befehlszeile.

Hinweis In einer zukünftigen Horizon Client-Version werden Windows-Registrierungseinstellungen möglicherweise nicht mehr unterstützt. Stattdessen müssen dann Gruppenrichtlinieneinstellungen verwendet werden.

Die folgende Tabelle enthält die Registrierungseinstellungen für die Anmeldung bei Horizon Client. Diese Einstellungen befinden sich in der Registrierung unter „`HKEY_CURRENT_USER \Software\VMware, Inc.\VMware VDM\Client\`“. Dieser Speicherort ist benutzerspezifisch. Die `HKEY_LOCAL_MACHINE`-Einstellungen, die in der nächsten Tabelle beschrieben werden, sind computerweite Einstellungen und beziehen sich auf alle lokalen Benutzer und alle Domänenbenutzer, die berechtigt sind, sich in einer Windows-Domänenumgebung beim Computer anzumelden.

Tabelle 3-15. Horizon Client Registrierungseinstellungen für Anmeldedaten

Registrierungseinstellung	Beschreibung
`Password`	Standardkennwort.
`UserName`	Standardbenutzername.

Die folgende Tabelle enthält die Registrierungseinstellungen für Horizon Client, die keine Anmeldedaten beinhalten. Der Speicherort dieser Einstellungen hängt wie folgt vom Systemtyp ab:

- Für 32-Bit-Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\`
- Für 64-Bit-Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\`

Tabelle 3-16. Horizon Client-Registrierungseinstellungen

Registrierungseinstellung	Beschreibung
`DomainName`	Standardmäßiger NetBIOS-Domänenname. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.
`EnableShade`	Bestimmt, ob die Menüleiste (Shade) am oberen Rand des Horizon Client-Fensters aktiviert ist. Die Menüleiste ist standardmäßig aktiviert, mit Ausnahme bei Clients im Kiosk-Modus. Mit dem Wert **`false`** wird die Menüleiste deaktiviert. **Hinweis** Diese Einstellung ist nur verfügbar, wenn das Anzeigelayout auf **Alle Monitore** oder **Vollbild** festgelegt ist.
`ServerURL`	Gibt die URL, die IP-Adresse oder den FQDN der Standard-Verbindungsserver-Instanz an.
`EnableSoftKeypad`	Wenn dies auf **`true`** eingestellt ist und ein Horizon Client-Fenster den Fokus aufweist, werden Ereignisse auf der physischen Tastatur, auf der Bildschirmtastatur, mit der Maus und im Schreibbereich an den Remote-Desktop oder die veröffentlichte Anwendung gesendet, selbst wenn sich die Maus oder die Bildschirmtastatur außerhalb des Horizon Client-Fensters befindet. Die Standardeinstellung ist **`false`**.

Die folgende Tabelle enthält Sicherheitseinstellungen, die Sie hinzufügen können. Der Speicherort dieser Einstellungen hängt wie folgt vom Systemtyp ab:

- Für 32-Bit-Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- Für 64-Bit-Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Tabelle 3-17. Sicherheitseinstellungen

Registrierungseinstellung	Beschreibung und gültige Werte
`CertCheckMode`	Zertifikatsprüfungsmodus. Folgende Werte sind gültig: ■ **`0`** implementiert `Do not verify server identity certificates`. ■ **`1`** implementiert `Warn before connecting to untrusted servers`. ■ **`2`** implementiert `Never connect to untrusted servers`.
`SSLCipherList`	Konfiguriert die Verschlüsselungsliste, um die Verwendung bestimmter kryptografischer Algorithmen und Protokolle zu beschränken, bevor Sie eine verschlüsselte TLS-Verbindung herstellen. Die Verschlüsselungsliste besteht aus einer oder mehreren Verschlüsselungszeichenfolgen, die durch Doppelpunkte voneinander getrennt werden. Für alle Verschlüsselungszeichenfolgen wird die Groß-/Kleinschreibung berücksichtigt. Der Standardwert ist **TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**. Der Standardwert bedeutet, dass TLS v1.1 und TLS v1.2 aktiviert sind und SSL v.2.0, SSL v3.0 und TLS v1.0 deaktiviert sind. SSL v2.0, SSL v3.0 und TLS v1.0 sind nicht mehr die genehmigten Protokolle und werden dauerhaft deaktiviert. Verschlüsselungs-Suites verwenden 128- oder 256-Bit-AES, entfernen anonyme DH-Algorithmen und sortieren die aktuelle Verschlüsselungsliste nach der Schlüssellänge des Verschlüsselungsalgorithmus. Referenzinformationen zur Konfiguration finden Sie unter http://www.openssl.org/docs/apps/ciphers.html.

Verwalten der Remote-Desktop- und veröffentlichten Anwendungsverbindungen

4

Endbenutzer können mit Horizon Client eine Verbindung mit einem Server herstellen, sich bei Remote-Desktops an- bzw. abmelden und veröffentlichte Anwendungen verwenden. Zur Fehlerbehebung können Endbenutzer Remote-Desktops und veröffentlichte Anwendungen auch neu starten und zurücksetzen.

Je nachdem, wie Sie die Richtlinien festlegen, können die Endbenutzer viele verschiedene Vorgänge auf ihren Remote-Desktops und in ihren veröffentlichten Anwendungen durchführen.

Dieses Kapitel enthält die folgenden Themen:

Verbindung zu einem Remote-Desktop oder einer veröffentlichten Anwendung herstellen

Zum Herstellen einer Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung müssen Sie den Namen eines Servers und die Anmeldedaten für Ihr Benutzerkonto angeben.

Bevor Endbenutzer auf ihre Remote-Desktops und veröffentlichten Anwendungen zugreifen, sollten Sie testen, ob Sie über ein Clientgerät eine Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung herstellen können. Sie müssen eventuell einen Server angeben und die Anmeldedaten für Ihr Benutzerkonto eingeben.

Voraussetzungen

- Besorgen Sie sich die Anmeldedaten, etwa einen Benutzernamen und das zugehörige Kennwort, den RSA SecurID-Benutzernamen und -Passcode, RADIUS-Authentifizierungsdaten oder die Smartcard-PIN.
- Besorgen Sie sich den NETBIOS-Domänennamen für die Anmeldung. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.
- Führen Sie die unter Vorbereiten des Verbindungsservers für Horizon Client beschriebenen administrativen Aufgaben aus.
- Wenn Sie außerhalb des Unternehmensnetzwerks eine VPN-Verbindung benötigen, um auf Remote Desktops und veröffentlichte Anwendungen zuzugreifen, vergewissern Sie sich, dass das Clientgerät zur Verwendung von VPN-Verbindungen eingerichtet ist, und aktivieren Sie diese Verbindung.
- Stellen Sie sicher, dass Sie über den vollqualifizierten Domänennamen (FQDN) des Servers verfügen, der Zugriff auf den Remote Desktop oder die veröffentlichte Anwendung gewährt. Unterstriche (_) werden in Servernamen nicht unterstützt. Wenn es sich nicht um Port 443 handelt, benötigen Sie auch die Portnummer.
- Wenn Sie beabsichtigen, das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem Remote-Desktop zu verwenden, müssen Sie sicherstellen, dass die Gruppenrichtlinieneinstellung AllowDirectRDP des Agenten aktiviert ist. Informationen hierzu finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.
- Konfigurieren Sie den Zertifikatsprüfungsmodus für das Zertifikat, das vom Server präsentiert wird. Informationen zur Bestimmung des zu verwendenden Modus finden Sie unter Festlegen des Zertifikatsprüfungsmodus in Horizon Client.

Verfahren

1. Sollte eine VPN-Verbindung erforderlich sein, müssen Sie das VPN aktivieren.
2. Starten Sie Horizon Client.
3. (Optional) Um sich als derzeit angemeldeter Windows-Domänenbenutzer anzumelden, klicken Sie in der oberen rechten Ecke der Menüleiste auf die Schaltfläche **Optionen** und wählen Sie **Als aktueller Benutzer anmelden** aus.

   Diese Einstellung ist nur verfügbar, wenn die Funktion **Als aktueller Benutzer anmelden** auf dem Clientsystem installiert ist.

4 Stellen Sie eine Verbindung mit einem Server her.

Option	Aktion
Verbindung mit einem neuen Server herstellen	Doppelklicken Sie auf die Schaltfläche **+ Server hinzufügen** oder klicken Sie in der Menüleiste auf **Neuer Server**, geben Sie den Namen eines Servers ein und klicken Sie auf **Verbinden**.
Verbindung mit einem vorhandenen Server herstellen	Doppelklicken Sie auf das Serversymbol oder klicken Sie mit der rechten Maustaste auf das Serversymbol und wählen Sie **Verbinden**aus.

Verbindungen zwischen Horizon Client und dem Server verwenden immer TLS. Der Standardport für TLS-Verbindungen ist 443. Wenn der Server nicht zur Verwendung des Standardports konfiguriert ist, verwenden Sie das Format *Servername*:*Port* (Beispiel: `view.company.com:1443`).

Es wird eventuell eine Meldung eingeblendet, die Sie bestätigen müssen, bevor das Anmeldedialogfeld angezeigt wird.

5 Wenn Sie zur Eingabe von RSA SecurID- oder RADIUS-Authentifizierungsdaten aufgefordert werden, geben Sie die Anmeldedaten ein und klicken Sie auf **Weiter**.

6 Geben Sie die Anmeldedaten eines Benutzers ein, der für die Verwendung von mindestens einem Remote-Desktop oder einer veröffentlichten Anwendung berechtigt ist, wählen Sie die Domäne aus und klicken Sie auf **Anmelden**.

Wenn Sie den Benutzernamen als **Benutzername@Domäne** eingeben, behandelt Horizon Client ihn als Benutzerprinzipalnamen (User Principal Name, UPN). Das Dropdown-Menü **Domäne** wird dann deaktiviert.

Wenn das Dropdown-Menü **Domäne** ausgeblendet ist, müssen Sie den Benutzernamen in der Form ***Benutzername@Domäne*** oder ***Domäne**Benutzername*** eingeben.

7 Wenn Horizon Client Sie auffordert, veröffentlichte Anwendungen oder Remote-Desktops auf dem Windows-**Start**-Menü zu installieren, klicken Sie auf **Ja** oder **Nein**.

Diese Aufforderung kann angezeigt werden, wenn Sie zum ersten Mal eine Verbindung mit einem Server herstellen, auf dem Verknüpfungen für veröffentlichte Anwendungen oder Remote-Desktops konfiguriert wurden. Wenn Sie auf **Ja**klicken, werden im **Startmenü** des Clientsystems Verknüpfungen für diese veröffentlichten Anwendungen oder Remote-Desktops installiert, wenn Sie zu deren Verwendung berechtigt sind. Wenn Sie auf **Nein** klicken, werden die Verknüpfungen nicht im **Startmenü** installiert.

Ein Horizon-Administrator kann die Gruppenrichtlinieneinstellung **Verknüpfungen automatisch installieren, wenn diese auf Horizon Server konfiguriert wurden** so konfigurieren, dass Endbenutzer zur Installation von Verknüpfungen aufgefordert werden (Standardeinstellung), Verknüpfungen automatisch installiert werden oder Verknüpfungen nie installiert werden.

8 (Optional) Klicken Sie zum Konfigurieren von Anzeigeeinstellungen für einen Remote Desktop mit der rechten Maustaste auf das Symbol des Remote Desktops und wählen Sie **Einstellungen** aus.

Option	Aktion
Anzeigeprotokoll auswählen	Wenn ein Horizon Administrator dies gestattet, können Sie anhand des Dropdown-Menüs **Verbinden über** das Anzeigeprotokoll auswählen.
Anzeigelayout auswählen	Verwenden Sie das Dropdown-Menü **Anzeige**, um eine Fenstergröße auszuwählen oder mehrere Monitore zu verwenden.

9 Um eine Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung herzustellen, doppelklicken Sie im Fenster für die Desktop- und Anwendungsauswahl auf das Symbol für den Remote-Desktop oder die veröffentlichte Anwendung.

Wenn Sie eine Verbindung mit einem veröffentlichten Desktop herstellen und für den veröffentlichten Desktop bereits die Verwendung eines anderen Anzeigeprotokolls festgelegt ist, kann die Verbindung nicht sofort hergestellt werden. Horizon Client fordert Sie auf, das festgelegte Protokoll zu verwenden oder sich abzumelden, damit Horizon Client die Verbindung mit einem anderen Anzeigeprotokoll herstellen kann.

Ergebnisse

Nachdem Sie verbunden sind, wird der Remote-Desktop oder die veröffentlichte Anwendung geöffnet.

Wenn Sie für mehrere Remote-Desktops oder veröffentlichte Anwendungen auf dem Server berechtigt sind, bleibt das Fenster für die Desktop- und Anwendungsauswahl geöffnet, damit Sie Verbindungen mit mehreren Remote-Desktops und veröffentlichten Anwendungen herstellen können.

Wenn die Funktion der Clientlaufwerksumleitung aktiviert ist, wird das Dialogfeld „Freigabe“ angezeigt, und Sie können darin den Zugriff auf Dateien des lokalen Dateisystems zulassen oder unterbinden. Weitere Informationen finden Sie unter Freigeben lokaler Ordner und Laufwerke.

Wenn Sie zum ersten Mal eine Verbindung mit einem Server herstellen, speichert Horizon Client eine Verknüpfung mit dem Server im Horizon Client-Startfenster. Wenn Sie die Serververbindung das nächste Mal herstellen müssen, können Sie auf diese Serververknüpfung doppelklicken.

Wenn keine Authentifizierung beim Server möglich ist oder wenn der Client keine Verbindung mit dem Remote-Desktop oder der veröffentlichten Anwendung herstellen kann, führen Sie die folgenden Aufgaben aus:

- Stellen Sie eine ordnungsgemäße Funktionsweise des Zertifikats für den Server sicher. Wenn dies nicht zutrifft, wird in Horizon Console möglicherweise angezeigt, dass der Agent auf Remote-Desktops nicht erreichbar ist. Diese sind Hinweise auf zusätzliche Verbindungsprobleme, die durch Zertifikatprobleme verursacht werden.
- Stellen Sie sicher, dass die für die Verbindungsserverinstanz festgelegten Kennzeichen Verbindungen von diesem Benutzer erlauben. Siehe das Dokument *Horizon-Verwaltung*.

- Stellen Sie sicher, dass der Benutzer zum Zugriff auf diesen Remote-Desktop oder diese veröffentlichte Anwendung berechtigt ist. Weitere Erläuterungen finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.
- Wenn Sie das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem Remote-Desktop verwenden, müssen Sie sicherstellen, dass das Betriebssystem des Remote-Desktops Remote-Desktop-Verbindungen zulässt.

Nächste Schritte

Konfigurieren Sie Starteinstellungen. Wenn Sie nicht möchten, dass Endbenutzer den Hostnamen des Servers eingeben müssen, oder wenn Sie andere Starteinstellungen konfigurieren möchten, verwenden Sie eine Befehlszeilenoption zum Erstellen einer Remote-Desktop-Verknüpfung. Siehe Ausführen von Horizon Client über die Befehlszeile.

Verwenden des nicht authentifizierten Zugriffs zur Verbindungsherstellung mit veröffentlichten Anwendungen

Wenn Sie ein Benutzerkonto für einen nicht authentifizierten Zugriff haben, können Sie sich anonym bei einem Server anmelden und eine Verbindung mit Ihren veröffentlichten Anwendungen herstellen.

Bevor Endbenutzer mit der Funktion für den nicht authentifizierten Zugriff auf eine veröffentlichte Anwendung zugreifen, sollten Sie testen, ob sich über ein Clientgerät eine Verbindung mit der veröffentlichten Anwendung herstellen lässt. Sie müssen eventuell einen Server angeben und die Anmeldedaten für Ihr Benutzerkonto eingeben.

Standardmäßig wählen Benutzer die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** aus dem Menü **Optionen** und ein Benutzerkonto für eine anonyme Anmeldung aus. Ihr Horizon-Administrator hat die Möglichkeit, Gruppenrichtlinieneinstellungen zur Vorauswahl der Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** zu konfigurieren und Benutzer mit einem bestimmten Benutzerkonto für den nicht authentifizierten Zugriff anzumelden.

Voraussetzungen

- Führen Sie die unter Vorbereiten des Verbindungsservers für Horizon Client beschriebenen administrativen Aufgaben aus.
- Richten Sie Benutzer für einen nicht authentifizierten Zugriff auf der Verbindungsserver-Instanz ein. Informationen dazu finden Sie unter „Bereitstellen eines nicht authentifizierten Zugriffs für veröffentlichte Anwendungen“ im Dokument *Horizon-Verwaltung*.
- Wenn Sie sich außerhalb des Unternehmensnetzwerks befinden, stellen Sie sicher, dass Ihr Clientgerät zur Verwendung einer VPN-Verbindung eingerichtet ist, und aktivieren Sie diese Verbindung.

- Stellen Sie sicher, dass Sie über den vollqualifizierten Domänennamen (FQDN) des Servers verfügen, der Zugriff auf diese veröffentlichte Anwendung gewährt. Unterstriche (_) werden in Servernamen nicht unterstützt. Wenn es sich nicht um Port 443 handelt, benötigen Sie auch die Portnummer.
- Konfigurieren Sie den Zertifikatsprüfungsmodus für das Zertifikat, das vom Server in Horizon Client präsentiert wird. Informationen zur Bestimmung des zu verwendenden Modus finden Sie unter Festlegen des Zertifikatsprüfungsmodus in Horizon Client.
- (Optional) Konfigurieren Sie die Gruppenrichtlinieneinstellungen **Konto für einen nicht authentifizierten Zugriff** und **Anonym mit nicht authentifiziertem Zugriff anmelden**, um das Standardverhalten für einen nicht authentifizierten Zugriff zu ändern. Weitere Informationen hierzu finden Sie unter Einstellungen für die Skriptdefinition für Client-GPOs.

Verfahren

1. Sollte eine VPN-Verbindung erforderlich sein, müssen Sie das VPN aktivieren.
2. Starten Sie Horizon Client.
3. Klicken Sie in der Menüleiste auf die Schaltfläche **Optionen** und wählen Sie **Anonym mit nicht authentifiziertem Zugriff anmelden** aus.

   Je nach Konfiguration des Clientsystems ist diese Einstellung eventuell bereits ausgewählt.
4. Stellen Sie eine Verbindung mit dem Server her, auf dem Sie über einen nicht authentifizierten Zugriff verfügen.

Option	Aktion
Verbindung mit einem neuen Server herstellen	Doppelklicken Sie auf die Schaltfläche **+ Server hinzufügen** oder klicken Sie auf die Schaltfläche **+ Neuer Server** in der Menüleiste, geben Sie den Namen des Servers ein und klicken Sie auf **Verbinden**.
Verbindung mit einem vorhandenen Server herstellen	Doppelklicken Sie auf das Serversymbol im Horizon Client-Startfenster.

   Verbindungen zwischen Horizon Client und dem Server verwenden immer TLS. Der Standardport für TLS-Verbindungen ist 443. Wenn der Server nicht zur Verwendung des Standardports konfiguriert ist, muss das in folgendem Beispiel gezeigte Format verwendet werden: `view.firma.com:1443`.

   Es wird eventuell eine Meldung eingeblendet, die Sie bestätigen müssen, bevor das Anmeldedialogfeld angezeigt wird.
5. Wenn das Anmeldedialogfeld angezeigt wird, wählen Sie ein Konto aus dem Dropdown-Menü **Benutzerkonto** aus, falls erforderlich.

   Wenn nur ein Benutzerkonto verfügbar ist, ist das Dropdown-Menü deaktiviert und das Benutzerkonto bereits ausgewählt.

6 (Optional) Wenn das Kontrollkästchen **Immer dieses Konto verwenden** verfügbar ist, aktivieren Sie dieses zur Umgehung des Anmeldedialogfeldes bei der nächsten Herstellung einer Verbindung mit dem Server.

   Um diese Einstellung zu deaktivieren, bevor Sie das nächste Mal eine Verbindung mit dem Server herstellen, klicken Sie mit der rechten Maustaste auf das Serversymbol im Horizon Client-Startfenster und wählen Sie **Gespeichertes Konto mit nicht authentifiziertem Zugriff löschen** aus.

7 Klicken Sie auf **Anmelden**, um sich beim Server anzumelden.

   Das Auswahlfenster für Anwendungen wird angezeigt.

8 Um eine veröffentlichte Anwendung zu starten, doppelklicken Sie auf das Symbol der veröffentlichten Anwendung.

Informationen zum Speicherort der Freigabe

Wenn die Funktion der Geolocation-Umleitung für einen Remote-Desktop oder eine veröffentlichte Anwendung aktiviert ist, können Sie Informationen zum Ort des Clientsystems für den Remote-Desktop oder die veröffentlichte Anwendung freigeben.

Um Standortinformationen zum Clientsystem freizugeben, müssen Sie eine Einstellung in Horizon Clientkonfigurieren.

Voraussetzungen

Horizon Administratoren müssen die Funktion der Geolocation-Umleitung für den Remote-Desktop oder die veröffentlichte Anwendung konfigurieren.

Diese Aufgabe beinhaltet die Aktivierung der Funktion der Geolocation-Umleitung, wenn Sie Horizon Agentinstallieren. Sie enthält auch die Einrichtung von Gruppenrichtlinien zur Konfiguration der Funktion der Geolocation-Umleitung und die Aktivierung des Internet Explorer-Plug-ins für die VMware Horizon-Geolocation-Umleitung. Die vollständigen Informationen zu den Systemanforderungen finden Sie unter Systemanforderungen für die Geolocation-Umleitung.

Verfahren

1 Stellen Sie eine Verbindung mit einem Server her.

2 Öffnen Sie das Dialogfeld **Einstellungen** und wählen Sie im linken Bereich **Geolocation** aus.

   - Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Zahnradsymbol **Einstellungen**.
   - Klicken Sie mit der rechten Maustaste auf einen Remote-Desktop oder eine veröffentlichte Anwendung im Fenster für die Desktop- und Anwendungsauswahl und wählen Sie **Einstellungen** aus.

3 Konfigurieren Sie die Geolocation-Einstellungen.

Option	Aktion
Freigeben von Standortinformationen zum Clientsystem für Remote-Desktops und veröffentlichte Anwendungen	Aktivieren Sie das Kontrollkästchen **Ihren Standort freigeben**.
Dialogfeld „Geolocation“ beim Herstellen einer Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung nicht anzeigen	Aktivieren Sie das Kontrollkästchen **Dialogfeld bei der Verbindung mit einem Desktop oder einer Anwendung nicht anzeigen**. Beim Dialogfeld „Geolocation“ werden Sie gefragt, ob Sie Standortinformationen für einen Remote-Desktop oder eine veröffentlichte Anwendung freigeben möchten. Wenn dieses Kontrollkästchen deaktiviert ist, wird das Dialogfeld „Geolocation“ angezeigt, wenn Sie zum ersten Mal eine Verbindung zu einem Remote-Desktop oder einer veröffentlichten Anwendung herstellen. Wenn Sie sich beispielsweise bei einem Server anmelden und eine Verbindung zu einem Remote-Desktop herstellen, wird das Dialogfeld „Geolocation“ angezeigt. Wenn Sie dann eine Verbindung zu einem anderen Remote-Desktop oder zu einer anderen veröffentlichten Anwendung herstellen, wird das Dialogfeld nicht erneut angezeigt. Um das Dialogfeld wieder anzuzeigen, müssen Sie die Verbindung zum Server trennen und sich erneut anmelden.

4 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

5 Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Ausblenden des VMware Horizon Client-Fensters

Sie können das VMware Horizon Client-Fenster nach dem Öffnen eines Remote Desktops oder einer veröffentlichten Anwendung ausblenden.

Sie können anhand einer Gruppenrichtlinieneinstellung konfigurieren, ob nach dem Öffnen von Remote Desktops oder veröffentlichten Anwendungen das Fenster immer ausgeblendet wird. Mehr Informationen finden Sie unter Allgemeine Einstellungen für Client-GPOs.

Verfahren

- Zum Ausblenden des VMware Horizon Client-Fensters nach dem Öffnen eines Remote Desktops oder einer veröffentlichten Anwendung klicken Sie in der Ecke des VMware Horizon Client-Fensters auf die Schaltfläche **Schließen**.
- Um eine Einstellung zu konfigurieren, die dafür sorgt, dass das VMware Horizon Client-Fenster nach dem Öffnen eines Remote Desktops oder einer veröffentlichten Anwendung immer ausgeblendet wird, klicken Sie vor der Verbindungsherstellung mit einem Server in der Menüleiste auf **Optionen** und wählen Sie **Selektor nach Start eines Elements ausblenden** aus.

- Um das VMware Horizon Client-Fenster anzuzeigen, nachdem es ausgeblendet wurde, klicken Sie mit der rechten Maustaste auf das VMware Horizon Client-Symbol im Infobereich und wählen Sie **VMware Horizon Client** aus oder klicken Sie, wenn Sie bei einem Remote Desktop angemeldet sind, in der Menüleiste auf die Schaltfläche **Optionen** und wählen Sie **Zu einem anderen Desktop wechseln** aus.

Herstellen einer erneuten Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung

Aus Sicherheitsgründen kann ein Horizon-Administrator Zeitüberschreitungen festlegen, damit Sie von einem Server abgemeldet werden, und eine veröffentlichte Anwendung nach einer gewissen Zeit der Inaktivität gesperrt wird.

Standardmäßig müssen Sie sich erneut anmelden, wenn Horizon Client geöffnet und Sie seit mehr als 10 Stunden mit einem bestimmten Server verbunden sind. Diese Zeitüberschreitung gilt für Verbindungen mit Remote-Desktops und mit veröffentlichten Anwendungen.

Sie erhalten 30 Sekunden, bevor eine veröffentlichte Anwendung automatisch gesperrt wird, eine Warnung. Wenn Sie nicht auf diese Warnung reagieren, wird die veröffentlichte Anwendung gesperrt. Standardmäßig erfolgt die Zeitüberschreitung nach 15 Minuten Inaktivität. Ein Horizon-Administrator kann diesen Zeitraum aber ändern.

Wenn Sie z. B. eine oder mehrere veröffentlichte Anwendungen geöffnet haben und sich von Ihrem Computer entfernen, kann es sein, dass nach einer Stunde Abwesenheit die Anwendungsfenster nicht mehr geöffnet sind. Stattdessen wird möglicherweise ein Dialogfeld angezeigt, in dem Sie zum Klicken auf **OK** aufgefordert werden, damit die Fenster der veröffentlichten Anwendungen erneut geöffnet werden.

Um diese Zeitüberschreitungseinstellungen in der Horizon Console zu konfigurieren, wählen Sie **Einstellungen > Globale Einstellungen** aus, klicken Sie auf die Registerkarte **Allgemeine Einstellungen** und dann auf **Bearbeiten**.

Erstellen einer Verknüpfung auf dem Windows-Client-Desktop oder im Startmenü

Sie können eine Verknüpfung für einen Remote-Desktop oder eine veröffentlichte Anwendung erstellen. Verknüpfungen werden auf dem Desktop des Clientsystems angezeigt, genauso wie Verknüpfungen für lokal installierte Anwendungen. Sie können auch eine Verknüpfung im Windows-Startmenü erstellen.

Verfahren

1. Starten Sie Horizon Client und melden Sie sich beim Server an.
2. Klicken Sie im Fenster für die Desktop und Anwendungsauswahl mit der rechten Maustaste auf einen Remote-Desktop oder eine veröffentlichte Anwendung und wählen Sie **Verknüpfung für Desktop erstellen** oder **Zum Startmenü hinzufügen** im Kontextmenü aus.

Ergebnisse

Je nach dem ausgewählten Befehl erstellt Horizon Client eine Verknüpfung auf dem Desktop oder im Windows-Startmenü auf dem Clientsystem.

Nächste Schritte

Sie können eine Verknüpfung umbenennen, löschen oder andere Aktionen für sie ausführen, die sich auf lokal installierte Anwendungen anwenden lassen. Wenn Sie die Verknüpfung verwenden und noch nicht beim Server angemeldet sind, werden Sie von Horizon Client zur Anmeldung aufgefordert, bevor der Remote-Desktop oder die veröffentlichte Anwendung geöffnet wird.

Verwenden von Verknüpfungen, die vom Server erstellt wurden

Ein Horizon-Administrator kann Startmenü- oder Desktop-Verknüpfungen für bestimmte Remote-Desktops und veröffentlichte Anwendungen konfigurieren.

Wenn Sie Berechtigungen für einen Remote-Desktop oder eine veröffentlichte Anwendung mit Verknüpfungen haben, platziert Horizon Client die Verknüpfungen im Startmenü, auf dem Desktop oder in beidem auf dem Clientsystem, wenn Sie eine Verbindung zum Server herstellen.

Auf Windows 10-Systemen platziert Horizon Client Verknüpfungen in der Apps-Liste. Wenn Ihr Horizon-Administrator einen Kategorienordner für eine Verknüpfung erstellt, wird dieser Ordner unter dem Ordner „VMware Applications“ oder als Kategorie in der Apps-Liste angezeigt.

Sie können eine Gruppenrichtlinieneinstellung verwenden, die festlegt, ob Horizon Client Verknüpfungen automatisch installiert, Endbenutzer zur Bestätigung der Installation der Verknüpfungen auffordert oder keine Verknüpfungen installiert. Weitere Informationen finden Sie unter der Gruppenrichtlinieneinstellung **Verknüpfungen automatisch installieren, wenn diese auf Horizon Server konfiguriert wurden** in Allgemeine Einstellungen für Client-GPOs.

Sie können den Befehl `vmware-view` mit der Option `-installShortcutsThenQuit` verwenden, um ein Skript zu erstellen, das ausgeführt wird, wenn das Clientsystem gestartet wird, und Verknüpfungen automatisch installiert. Weitere Informationen finden Sie unter Horizon Client-Befehlsverwendung.

Wenn Sie auf eine vom Server erstellte Verknüpfung klicken und noch nicht beim Server angemeldet sind, werden Sie von Horizon Client zur Anmeldung aufgefordert, bevor der Remote-Desktop oder die veröffentlichte Anwendung geöffnet wird.

Wenn ein Horizon Administrator Verknüpfungen für Remote-Desktops und veröffentlichte Anwendungen auf dem Server ändert, werden die Verknüpfungen standardmäßig auf dem Clientsystem aktualisiert, wenn Sie das nächste Mal eine Verbindung mit diesem Server herstellen. Sie können das Standardverhalten beim Aktualisieren von Verknüpfungen in Horizon Client ändern. Weitere Informationen finden Sie unter Konfigurieren von Startmenü-Verknüpfungsaktualisierungen.

Um vom Server erstellte Verknüpfungen vom Clientsystem zu entfernen, können Sie den Server im Horizon Client-Serverauswahlfenster löschen oder Horizon Client deinstallieren.

Hinweis Auf Clients im Kiosk-Modus werden Benutzer nicht zur Installation von auf dem Server erstellten Verknüpfungen aufgefordert, und auf dem Server erstellte Verknüpfungen werden nicht angelegt.

Konfigurieren von Startmenü-Verknüpfungsaktualisierungen

Sie können festlegen, ob Änderungen der Verknüpfungen für Remote-Desktops und veröffentlichte Anwendungen auf dem Server für das Clientsystem übernommen werden, wenn Sie eine Verbindung mit dem Server herstellen.

Voraussetzungen

Sie können die Einstellung für die Verknüpfungsaktualisierung nur dann ändern, wenn Sie zuvor eine Verknüpfung von einem Server installiert haben.

Verfahren

1. Starten Sie Horizon Client und stellen Sie eine Verbindung mit einem Server her.
2. Öffnen Sie das Dialogfeld „Einstellungen“ und wählen Sie die Option **Verknüpfungen** aus.
   - Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Zahnradsymbol **Einstellungen**.
   - Klicken Sie mit der rechten Maustaste auf das Symbol eines Remote-Desktops oder einer veröffentlichten Anwendung und wählen Sie **Einstellungen** aus.
3. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Liste der Anwendungs- und Desktop-Verknüpfungen automatisch aktualisieren** und klicken Sie auf **OK**.

Konfigurieren der automatischen Verbindungsfunktion für einen Remote-Desktop

Sie können einen Server so konfigurieren, dass ein bestimmter Remote-Desktop automatisch geöffnet wird, wenn Sie eine Verbindung mit diesem Server herstellen. Sie können einen Server nicht so konfigurieren, dass eine veröffentlichte Anwendung automatisch geöffnet wird.

Voraussetzungen

Besorgen Sie sich die Anmeldedaten zur Herstellung einer Verbindung mit dem Server, etwa den Benutzernamen und das Kennwort, den RSA SecurID-Benutzernamen und die -Kennung, den RADIUS-Authentifizierungsbenutzernamen und die -Kennung oder die Smartcard-PIN.

Verfahren

1. Starten Sie Horizon Client und melden Sie sich beim Server an.

2 Klicken Sie im Fenster für die Desktop- und Anwendungsauswahl mit der rechten Maustaste auf den Remote-Desktop und wählen Sie **Verbindung mit diesem Desktop automatisch herstellen**.

3 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

4 Um das Dialogfeld zu schließen, klicken Sie auf **OK**.

5 Trennen Sie die Verbindung mit dem Server.

6 Stellen Sie erneut ein Verbindung mit dem Server her.

   Horizon Client startet den Remote-Desktop automatisch.

7 (Optional) Wenn Sie die automatische Verbindungsfunktion für den Remote-Desktop deaktivieren müssen, klicken Sie im Dropdown-Menü **Optionen** in der Menüleiste auf den Remote-Desktop und deaktivieren Sie die Option **Verbindung mit diesem Desktop automatisch herstellen**.

Abmelden oder trennen

Wenn Sie die Verbindung mit einem Remote Desktop trennen, ohne sich abzumelden, bleiben die Anwendungen auf dem Remote Desktop möglicherweise geöffnet. Sie können auch die Verbindung mit einem Server trennen und veröffentlichte Anwendungen geöffnet lassen.

Sie können sich von einem Remote Desktop abmelden, selbst wenn Sie den Remote Desktop nicht geöffnet haben. Diese Funktion hat dasselbe Ergebnis, als wenn Sie Strg+Alt+Entf an den Remote Desktop senden und anschließend auf **Abmelden** klicken.

Hinweis Die Eingabe der Windows-Tastenkombination Strg+Alt+Entf wird für Remote-Desktops nicht unterstützt. Klicken Sie stattdessen in der Menüleiste auf die Schaltfläche **Strg-Alt-Entf senden**. Alternativ können Sie auch die Tastenkombination Strg+Alt+Einfg betätigen.

Verfahren

- Trennen Sie die Verbindung mit einem Remote-Desktop, ohne sich abzumelden.

Option	Aktion
Vom Remote-Desktop-Fenster aus	Führen Sie einen der folgenden Schritte aus: ■ Klicken Sie auf die Schaltfläche **Schließen** in der Ecke des Remote-Desktop-Fensters. ■ Wählen Sie in der Menüleiste des Remote-Desktop-Fensters **Optionen > Trennen** aus.
Im Fenster für die Desktop- und Anwendungsauswahl	Klicken Sie in der oberen linken Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Symbol **Verbindung zu diesem Server trennen** und anschließend im Dialogfeld der Warnung auf **OK**. Wenn Sie zur Verwendung mehrerer Remote Desktops oder veröffentlichter Anwendungen auf dem Server berechtigt sind, ist das Fenster für die Desktop- und Anwendungsauswahl geöffnet.

Hinweis Ein Horizon Administrator kann Remote Desktops so konfigurieren, dass Sie beim Trennen der Verbindung abgemeldet werden. In diesem Fall werden alle geöffneten Anwendungen auf dem Remote Desktop geschlossen.

- Melden Sie sich ab und trennen Sie die Verbindung mit einem Remote-Desktop.

Option	Aktion
Von innerhalb des Remote-Desktops	Melden Sie sich über das Windows-**Start**-Menü ab.
Über die Menüleiste	Wählen Sie **Optionen > Verbindung trennen und abmelden** aus. Bei Verwendung dieser Option werden alle Dateien, die auf dem Remote Desktop geöffnet sind, ohne vorheriges Speichern geschlossen.

- Trennen Sie die Verbindung mit einer veröffentlichten Anwendung.

Option	Aktion
Verbindung mit veröffentlichter Anwendung, aber nicht die Verbindung mit dem Server trennen	Beenden Sie die veröffentlichte Anwendung auf die übliche Weise. Klicken Sie beispielsweise in der Ecke des Anwendungsfensters auf die Schaltfläche **Schließen**.
Verbindung mit veröffentlichter Anwendung und Server trennen	Klicken Sie in der oberen linken Ecke des Fensters für die Anwendungsauswahl auf das Symbol **Verbindung zu diesem Server trennen** und anschließend im Dialogfeld der Warnung auf **OK**.
Fenster für die Anwendungsauswahl schließen, aber veröffentlichte Anwendung geöffnet lassen	Klicken Sie auf die Schaltfläche **Schließen**. Das Fenster für die Anwendungsauswahl wird geschlossen.

- Melden Sie sich ab, wenn kein Remote-Desktop geöffnet ist.

  Bei Verwendung dieser Option werden alle Dateien, die auf dem Remote Desktop geöffnet sind, ohne vorheriges Speichern geschlossen.

  a Starten Sie Horizon Client, stellen Sie eine Verbindung mit dem Server her, der einen Zugriff auf den Remote-Desktop bietet, und geben Sie die Anmeldeinformationen für die Authentifizierung an.

  b Klicken Sie mit der rechten Maustaste auf das Symbol des Remote Desktops und wählen Sie **Abmelden** aus.

Trennen einer Serververbindung

Wenn Sie einen Remote Desktop oder eine veröffentlichte Anwendung nicht mehr verwenden, können Sie die Verbindung mit dem Server trennen.

Um eine Serververbindung zu trennen, klicken Sie auf das Symbol **Verbindung zu diesem Server trennen** in der oberen linken Ecke des Horizon Client-Fensters oder drücken Sie Alt+D.

Arbeiten in einem Remote-Desktop oder einer veröffentlichten Anwendung

5

Horizon Client für Windows bietet eine vertraute, individuell angepasste Umgebung für Desktops und Anwendungen. Endbenutzer können auf an ihren lokalen Windows-Computer angeschlossene USB- und andere Geräte zugreifen, Dokumente an beliebige Drucker senden, die von ihrem lokalen Computer erkannt werden, eine Authentifizierung mithilfe von Smartcards durchführen und mehrere Anzeigemonitore verwenden.

Dieses Kapitel enthält die folgenden Themen:

- Synchronisierung der als Eingabequelle für die Tastatur festgelegten Sprache
- Konfigurieren der Synchronisierung von Sperrtasten

Funktionsunterstützung für Windows-Clients

Bestimmte Gastbetriebssysteme und Remote-Desktopfunktionen erfordern bestimmte Horizon Agent-Versionen. Verwenden Sie diese Informationen bei der Planung, welche Funktionen Ihren Endbenutzern zur Verfügung gestellt werden sollen.

Unterstützte virtuelle Windows Desktops

Virtuelle Desktops unter Windows sind virtuelle Maschinen mit einer einzelnen Sitzung.

Diese Version von Horizon Client funktioniert mit virtuellen Windows-Desktops, auf denen Horizon Agent 7.5 oder höher installiert ist. Zu den unterstützten Gastbetriebssystemen gehören Windows 7, Windows 8.x und Windows 10, Windows Server 2012 R2, Windows Server 2016 und Windows Server 2019, mit den folgenden Einschränkungen:

- Windows Server 2019-Remote-Desktops erfordern Horizon Agent 7.7 oder höher.
- Virtuelle Windows 7-und Windows 8.x-Desktops werden mit Horizon Agent 2006 und höher nicht unterstützt.

Veröffentlichte Desktops auf RDS-Hosts

RDS-Hosts sind Server-Computer, auf denen Windows-Remote-Desktop-Dienste und Horizon Agent installiert sind. Mehrere Benutzer können gleichzeitig über veröffentlichte Desktop-Sitzungen auf einem RDS-Host verfügen. Ein RDS-Host kann ein physischer Computer oder eine virtuelle Maschine sein.

Diese Version von Horizon Client ist mit RDS-Hosts kompatibel, auf denen Horizon Agent 7.5 oder höher installiert ist. Zu den unterstützten Gastbetriebssystemen gehören Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 und Windows Server 2019, mit den folgenden Einschränkungen:

- Windows Server 2019-RDS-Hosts erfordern Horizon Agent 7.7 oder höher.
- Windows Server 2012 RDS-Hosts werden mit Horizon Agent 2006 und höher nicht unterstützt.

Anforderungen für bestimmte Remote-Desktopfunktionen

Die meisten Remote-Desktopfunktionen funktionieren mit Horizon Agent 7.5, einige Funktionen erfordern jedoch spätere Horizon Agent-Versionen.

Funktion	Anforderungen
Ziehen von Text und Bildern	Horizon Agent 7.9 oder höher
Ziehen von Dateien und Ordnern	Horizon Agent 7.7 oder höher

Funktion	Anforderungen
Geolocation-Umleitung	Horizon Agent 7.6 oder höher
Browser-Umleitung	Horizon Agent 7.10 oder höher
VMware Integrated Printing und standortbasiertes Drucken	Horizon Agent 7.7 oder höher

Diese Version von Horizon Client für Windows bietet keine Unterstützung für die folgenden Remote-Desktopfunktionen, die in Horizon Agent 7.x-Versionen unterstützt werden:

- Virtueller Druck (auch als ThinPrint bezeichnet)
- Flash URL-Umleitung
- Flash-Umleitung

Unterstützte Linux Desktops

Eine Liste der unterstützten Linux-Gastbetriebssysteme und Informationen zu den unterstützten Funktionen finden Sie im Dokument *Einrichten von Linux-Desktops in Horizon*.

Anpassen der Größe des Remote-Desktop-Fensters

Wenn Sie eine Ecke des Remote-Desktop-Fensters ziehen, um dessen Größe zu ändern, wird eine QuickInfo eingeblendet, die die Bildschirmauflösung rechts unten im Fenster anzeigt.

Wenn Sie das VMware Blast- oder PCoIP-Anzeigeprotokoll verwenden, zeigt die QuickInfo unterschiedliche Bildschirmauflösungen an, wenn Sie die Größe des Remote-Desktop-Fensters ändern. Diese Informationen sind hilfreich, wenn Sie die Größe des Remote-Desktop-Fensters auf eine bestimmte Auflösung ändern müssen.

Wenn ein Horizon-Administrator die Gastgröße gesperrt hat oder Sie das RDP-Anzeigeprotokoll verwenden, können Sie die Auflösung des Remote-Desktop-Fensters nicht ändern. In diesem Fall zeigt die Auflösungsquickinfo die ursprüngliche Auflösung an.

Wenn Sie mehrere Monitore verwenden, können Sie die Monitore auswählen, auf denen ein Remote-Desktop-Fenster angezeigt werden soll. Weitere Informationen finden Sie unter Auswahl bestimmter Monitore zum Anzeigen eines Remote-Desktops. Sie können das Remote-Desktop-Fenster auch so konfigurieren, dass es auf nur einem Monitor geöffnet wird. Weitere Informationen finden Sie unter Anzeigen eines Remote-Desktops auf einem Monitor in einer Mehrfachmonitorumgebung.

Monitore und Bildschirmauflösung

Sie können einen Remote-Desktop oder eine veröffentlichte Anwendung auf mehrere Monitore erweitern. Wenn Sie einen hochauflösenden Monitor besitzen, können Sie den Remote-Desktop oder die veröffentlichte Anwendung in voller Auflösung sehen.

Unterstützte Konfigurationen für mehrere Monitore

Horizon Client unterstützt die folgenden Mehrfachmonitorkonfigurationen:

- Ab Horizon 7 Version 7.8 werden sechs Monitore mit einer Auflösung von 2560 x 1600 mit virtuellen Desktops unterstützt, auf denen Windows 10 Version 1703 oder höher ausgeführt wird. Aktualisierte Windows-Anzeigespezifikationen erfordern Windows 10 Version 1803 oder höher für die Unterstützung von sechs Monitoren auf Horizon 7 Version 7.9 und höher.
- Mit Instant-Clone-Desktop-Pools ist die maximale Anzahl an Monitoren mit 4K-Auflösung 4.
- Bei mindestens zwei Monitoren müssen sich die Monitore nicht im gleichen Modus befinden. Wenn Sie zum Beispiel einen Laptop verwenden, der mit einem externen Monitor verbunden ist, kann sich der externe Monitor sowohl im Quer- als auch im Hochformat befinden.
- Mit der Hardwareversion 13 oder früher können Monitore nur dann nebeneinander, in Zweiergruppen oder vertikal übereinander platziert werden, wenn Sie zwei Monitore verwenden und die maximale Gesamtlänge weniger als 4096 Pixel beträgt.
- Um die Funktion zur selektiven Festlegung mehrerer Monitore nutzen zu können, muss das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll verwendet werden. Weitere Informationen dazu finden Sie unter Auswahl bestimmter Monitore zum Anzeigen eines Remote-Desktops und Wählen bestimmter Monitore zur Anzeige veröffentlichter Anwendungen.
- Um die vSGA-3D-Wiedergabefunktion nutzen zu können, müssen Sie das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll verwenden. Sie können bis zu zwei Monitore mit einer Auflösung von bis zu 1920x1200 verwenden. Für eine Auflösung von 4K (3840 X 2160) wird nur ein Monitor unterstützt.
- Für vGPU oder andere GPU-Passthrough-Modi bestimmen die Anbieterhardware und -treiber die Anzahl der Monitore und die maximale Auflösung. Weitere Informationen finden Sie im *Benutzerhandbuch für NVIDIA GRID Virtual GPU* oder auf der Website des Anbieters.
- Wenn Sie mindestens fünf Monitore verwenden und per VMware Blast eine Verbindung mit einer Remotesitzung herstellen und zudem dieselben Benutzeranmeldedaten verwenden, um von einem anderen Gerät per PCoIP eine Verbindung mit der Sitzung herzustellen (ohne Abmeldung von der ursprünglichen Sitzung), schlägt die erste Verbindung mit der neuen Sitzung fehl.
- Mit dem VMware Blast-Anzeigeprotokoll wird eine Bildschirmauflösung von 8K (7680 x 4320) für den Remote-Desktop unterstützt. Es werden zwei 8K-Anzeigen unterstützt. Die Hardwareversion der virtuellen Desktop-Maschine muss 14 (ESXi 6.7 oder höher) sein. Sie müssen ausreichend Systemressourcen in der virtuellen Maschine zuteilen, um eine 8K-Anzeige zu unterstützen. Informationen zu unterstützten Monitorkonfigurationen für GRID-basierte Desktops und für NVIDIA vGPU-Profile finden Sie im *Benutzerhandbuch für virtuelle GPU-Software* auf der NVIDIA-Website. Diese Funktion wird nur mit dem Windows-Client unterstützt.

- Mit dem VMware Blast- oder dem PCoIP-Anzeigeprotokoll wird eine Bildschirmauflösung von 4K (3840 x 2160) für den Remote-Desktop unterstützt. Die Anzahl der unterstützten 4K-Bildschirme hängt von der Hardwareversion der virtuellen Maschine des Desktops und der Windows-Version ab.

Hardwareversion	Windows-Version	Anzahl der unterstützten 4K-Bildschirme
10 (ESXi 5.5.x-kompatibel)	7, 8, 8.x, 10	1
11 (ESXi 6.0-kompatibel)	7 (3D-Rendern-Funktion deaktiviert und Windows Aero deaktiviert)	3
11	7 (3D-Rendern-Funktion aktiviert)	1
11	8, 8.x, 10	1
13 oder 14	7, 8, 8.x, 10 (3D-Rendern-Funktion aktiviert)	1
13 oder 14	7, 8, 8.x, 10	4

  Für eine optimale Leistung muss die virtuelle Maschine mindestens über 2 GB RAM und 2 vCPUs verfügen. Diese Funktion kann gute Netzwerkbedingungen erfordern, wie eine Bandbreite von 1000 Mbit/s mit niedriger Netzwerklatenz und geringen Paketverlusten.

  Hinweis Wenn die Bildschirmauflösung des Remote-Desktop auf 3840 x 2160 (4K) eingestellt ist, können Elemente auf dem Bildschirm kleiner erscheinen. Möglicherweise können Sie auch das Dialogfeld zur Bildschirmauflösung im Remote-Desktop verwenden, um Text und andere Elemente zu vergrößern. In diesem Szenario können Sie für den DPI-Wert des Clientcomputers die passende Einstellung festlegen und die DPI-Synchronisierung aktivieren, damit die DPI-Einstellung des Clientcomputers an den Remote-Desktop umgeleitet wird.

- Wenn Sie Microsoft RDP 7 verwenden, können Sie maximal 16 Monitore verwenden, um einen Remote-Desktop anzuzeigen.
- Wenn Sie das Microsoft RDP-Anzeigeprotokoll verwenden, muss Microsoft Remote Desktop Connection (RDC) 6.0 oder höher auf dem Remote-Desktop installiert sein.

Auswahl bestimmter Monitore zum Anzeigen eines Remote-Desktops

Wenn Sie zwei oder mehr Monitore verwenden, können Sie die Monitore auswählen, auf denen ein Remote-Desktop-Fenster angezeigt werden soll. Wenn Sie beispielsweise über zwei Monitore verfügen, können Sie festlegen, dass das Fenster des Remote-Desktops nur auf einem dieser zwei Monitore angezeigt wird.

Ab Horizon 7 Version 7.8 können Sie bis zu sechs benachbarte Monitore mit virtuellen Desktops auswählen, auf denen Windows 10 Version 1703 und höher ausgeführt wird. Ab Horizon 7 Version 7.9 können Sie bis zu sechs benachbarte Monitore mit virtuellen Desktops auswählen, auf denen Windows 10 Version 1803 und höher ausgeführt wird. Die Monitore lassen sich nebeneinander oder übereinander anordnen. Beispielsweise könnten Sie zwei Reihen mit je drei Monitoren konfigurieren. Mit anderen Windows-Versionen oder früheren VMware Horizon-Versionen können Sie bis zu vier benachbarte Monitore verwenden.

Voraussetzungen

Sie müssen über mindestens zwei Monitore verfügen.

Verfahren

1. Starten Sie Horizon Client und stellen Sie eine Verbindung mit einem Server her.
2. Öffnen Sie das Dialogfeld „Einstellungen“ für den Remote-Desktop.
   - Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Symbol für **Einstellungen** (Zahnrad) und wählen Sie im linken Bereich den Remote-Desktop aus.
   - Klicken Sie im Fenster für die Desktop- und Anwendungsauswahl mit der rechten Maustaste auf den Remote-Desktop und wählen Sie **Einstellungen** aus.
3. Wählen Sie im Dropdown-Menü **Verbinden über** die Option **PCoIP** oder **VMware Blast** aus.

   Das Dropdown-Menü **Verbinden über** wird nur angezeigt, wenn es von einem Horizon-Administrator aktiviert wurde.
4. Wählen Sie im Dropdown-Menü **Anzeige** die Option **Alle Monitore** aus.

   Unter den Anzeigeeinstellungen finden Sie Miniaturbilder der Monitore, die aktuell mit dem Clientsystem verbunden sind. Die Anzeigetopologie entspricht den Anzeigeeinstellungen auf dem Clientsystem.
5. Klicken Sie zur Aktivierung oder Deaktivierung eines Monitors für die Anzeige des Remote Desktops auf ein Miniaturbild.

   Nach der Auswahl eines Monitors ändert dessen Miniaturbild die Farbe. Wenn Sie gegen eine Regel der Anzeigeauswahl verstoßen, wird eine Warnmeldung eingeblendet.
6. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.
7. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.
8. Stellen Sie eine Verbindung mit dem Remote-Desktop her.

   Ihre Änderungen werden sofort wirksam, wenn Sie eine Verbindung mit dem Remote-Desktop herstellen. Horizon Client speichert Anzeigeeinstellungen in einer Einstellungsdatei für den Remote Desktop, nachdem Sie Horizon Client beendet haben.

Anzeigen eines Remote-Desktops auf einem Monitor in einer Mehrfachmonitorumgebung

Wenn Sie über zwei oder mehr Monitore verfügen, das Fenster eines Remote-Desktops aber nur auf einem Monitor angezeigt werden soll, können Sie das Remote-Desktop-Fenster so konfigurieren, dass es nur auf einem Monitor geöffnet wird.

Voraussetzungen

Sie müssen über mindestens zwei Monitore verfügen.

Verfahren

1. Starten Sie Horizon Client und stellen Sie eine Verbindung mit einem Server her.
2. Öffnen Sie das Dialogfeld „Einstellungen“ für den Remote-Desktop.
   - Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Symbol für **Einstellungen** (Zahnrad) und wählen Sie im linken Bereich den Remote-Desktop aus.
   - Klicken Sie im Fenster für die Desktop- und Anwendungsauswahl mit der rechten Maustaste auf den Remote-Desktop und wählen Sie **Einstellungen** aus.
3. Wählen Sie im Dropdown-Menü **Verbinden über** die Option **PCoIP** oder **VMware Blast** aus.

   Das Dropdown-Menü **Verbinden über** wird nur angezeigt, wenn es von einem Horizon-Administrator aktiviert wurde.
4. Wählen Sie im Dropdown-Menü **Anzeige** die Option **Vollbild**, **Fenster – groß**, **Fenster – klein** oder **Benutzerdefiniert** aus.

   Fenster - groß legt die Größe des Fensters auf 1904 x 978 Pixel fest. **Fenster - klein** legt die Größe des Fensters auf 640 x 480 Pixel fest. Bei Auswahl von **Benutzerdefiniert** können Sie eine bestimmte Fenstergröße festlegen.
5. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.
6. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Ergebnisse

Standardmäßig wird das Remote-Desktop-Fenster auf dem primären Monitor geöffnet. Sie können das Remote-Desktop-Fenster auch zu einem nicht primären Monitor ziehen. Beim nächsten Öffnen des Remote-Desktops wird dann das Remote-Desktop-Fenster wieder auf diesem Monitor angezeigt. Das Fenster wird nach dem Öffnen in der Mitte des Monitors platziert. Es verwendet die für den Anzeigemodus ausgewählte Fenstergröße und nicht eine eventuell von Ihnen durch Ziehen angepasste Fenstergröße.

Wählen bestimmter Monitore zur Anzeige veröffentlichter Anwendungen

Wenn Sie über zwei oder mehr Monitore verfügen, können Sie die Monitore auswählen, auf denen die Fenster der veröffentlichten Anwendungen angezeigt werden sollen. Wenn Sie beispielsweise über zwei Monitore verfügen, können Sie festlegen, dass das Fenster der veröffentlichten Anwendungen nur auf einen dieser zwei Monitore angezeigt wird.

Es lassen sich bis zu vier benachbarte Monitore auswählen. Die Monitore können nebeneinander, jeweils zwei gestapelt oder vertikal gestapelt angeordnet sein. Es lassen sich maximal zwei Monitore vertikal stapeln.

Voraussetzungen

Sie müssen über mindestens zwei Monitore verfügen.

Verfahren

1. Starten Sie Horizon Client und stellen Sie eine Verbindung mit einem Server her.
2. Öffnen Sie das Dialogfeld „Einstellungen“ für veröffentlichte Anwendungen.
   - Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Symbol für **Einstellungen** (Zahnrad) und wählen Sie **Anwendungen** aus.
   - Klicken Sie mit der rechten Maustaste im Fenster für die Desktop- und Anwendungsauswahl auf eine veröffentlichte Anwendung und wählen Sie **Einstellungen** aus.
3. Wählen Sie in den Anzeigeeinstellungen einen Monitor aus, auf dem das Fenster der veröffentlichten Anwendung angezeigt werden soll, bzw. heben Sie die Auswahl auf.

   Nach der Auswahl eines Monitors ändert dessen Miniaturbild die Farbe. Wenn Sie gegen eine Regel der Anzeigeauswahl verstoßen, wird eine Warnmeldung eingeblendet.
4. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.
5. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Verwenden der Anzeigeskalierung

Benutzer mit einem schlechten Sehvermögen oder mit Bildschirmen mit hoher Auflösung wie z. B. 4K-Monitoren haben im Allgemeinen die Anzeigeskalierung durch Festlegung des DPI-Werts (Dots per Inch, Punkte pro Zoll) auf dem Clientsystem auf mehr als 100 Prozent aktiviert. Die DPI-Einstellung steuert die Größe des Texts, der Apps und der Symbole. Durch eine niedrigere DPI-Einstellung erscheinen sie kleiner und durch eine höhere größer. Durch die Funktion der Anzeigeskalierung unterstützen Remote-Desktops und veröffentlichte Anwendungen die Skalierungseinstellungen des Clientsystems, sodass die Anzeige in normaler Größe und nicht zu klein erfolgt.

Horizon Client vergleicht die DPI-Einstellung, die von dem Remote-Desktop oder der veröffentlichten Anwendung empfangen wird, mit der DPI-Einstellung des Clientsystems. Wenn die DPI-Einstellungen nicht übereinstimmen und die Funktion für die Anzeigeskalierung aktiviert ist, berechnet Horizon Client den Skalierungsfaktor. Beispiel: Wenn die DPI-Einstellung eines Remote-Desktops 100 % beträgt und die DPI-Einstellung des Clientsystems 200 %, skaliert Horizon Client die DPI-Einstellung des Remote-Desktops um einen Faktor von 2 (200/100 = 2) hoch.

Horizon Client speichert die Einstellung für die Anzeigeskalierung für jeden Remote-Desktop separat. Für veröffentlichte Anwendungen ist die Einstellung für die Anzeigeskalierung für alle veröffentlichten Anwendungen gültig, die für den aktuell angemeldeten Benutzer verfügbar sind.

In einer Mehrfachmonitorumgebung wirkt sich die Anzeigeskalierung nicht auf die von Horizon Client unterstützte Anzahl der Monitore und die maximale Auflösung aus. Wenn die Anzeigeskalierung zugelassen und aktiviert ist, basiert die Skalierung auf der DPI-Einstellung des Clientsystems.

Sie haben die Möglichkeit, die Einstellung für die Anzeigeskalierung durch Aktivierung der Gruppenrichtlinieneinstellung Horizon Client **Gesperrte Gastgröße** auszublenden.

Sie können die Anzeigeskalierung für alle Remote-Desktops und veröffentlichten Anwendungen durch Festlegung der Gruppenrichtlinieneinstellung **Anzeigeskalierung zulassen** aktivieren oder deaktivieren. Weitere Informationen hierzu finden Sie unter Allgemeine Einstellungen für Client-GPOs. **Anzeigeskalierung zulassen** ist standardmäßig aktiviert, und die Option ist in der Benutzeroberfläche ausgewählt.

Dieser Vorgang beschreibt, wie Sie die Funktion der Anzeigeskalierung vor der Herstellung einer Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung aktivieren. Sie können nach dem Herstellen der Verbindung mit einem Remote-Desktop die Funktion für die Anzeigeskalierung aktivieren, indem Sie **Optionen > Anzeigeskalierung zulassen** in der Horizon Client-Menüleiste auswählen.

Verfahren

1. Starten Sie Horizon Client und stellen Sie eine Verbindung mit einem Server her.
2. Klicken Sie im Desktop- und Anwendungsauswahlfenster mit der rechten Maustaste auf den Remote-Desktop oder die veröffentlichte Anwendung und wählen Sie **Einstellungen** aus.
3. Aktivieren Sie das Kontrollkästchen **Anzeigeskalierung zulassen**.

   Wenn ein Administrator die Anzeigeskalierung vorkonfiguriert hat, wird das Kontrollkästchen ausgegraut dargestellt. Wenn ein Administrator die Einstellung für die Anzeigeskalierung ausgeblendet hat, wird das Kontrollkästchen nicht angezeigt.
4. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.
5. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Verwendung der DPI-Synchronisierung

Die DPI-Synchronisierungsfunktion stellt sicher, dass die DPI-Einstellung eines Remote-Desktops oder einer veröffentlichten Anwendung der DPI-Einstellung des Clientsystems entspricht.

Wie die Funktion für die Anzeigeskalierung kann die Funktion für die DPI-Synchronisierung die Lesbarkeit von Text und Symbolen auf Anzeigen mit hohem DPI-Wert verbessern. Im Gegensatz zur Anzeigeskalierung, die die Größe von Schriftarten und Bildern vergrößert und diese unscharf machen kann, vergrößert die Funktion „DPI-Synchronisierung“ die Schriftgröße und Bilder, während diese scharf bleiben. Aus diesem Grund wird die Funktion „DPI-Synchronisierung“ in der Regel für eine optimale Benutzererfahrung bevorzugt.

Falls sowohl die DPI-Synchronisierungsfunktion als auch die Anzeigeskalierungsfunktion aktiviert ist, ist jeweils nur eine Funktion verfügbar.

Die Gruppenrichtlinieneinstellung **DPI-Synchronisierung** des Agenten bestimmt, ob die DPI-Synchronisierungsfunktion aktiviert ist. Die Funktion ist standardmäßig aktiviert.

Verhaltensweisen der DPI-Synchronisierung mit Remote-Desktops

Das standardmäßige DPI-Synchronisierungsverhalten hängt von der Horizon Agent-Version ab, die auf dem Agent-Computer installiert ist.

Beginnend mit Horizon Agent 2012 wird die Einstellung „DPI pro Monitor“ des Clients mit dem Agent synchronisiert und die Änderungen werden bei einer Remotesitzung standardmäßig sofort wirksam. Diese Funktion wird durch die Agent-Gruppenrichtlinieneinstellung **DPI-Synchronisierung pro Monitor** gesteuert. Die Funktion „DPI-Synchronisierung pro Monitor“ wird standardmäßig für virtuelle und physische Desktops unterstützt. Sie wird für veröffentlichte Desktops nicht unterstützt.

Bei früheren Horizon Agent-Versionen unterstützt Horizon Client die Synchronisierung nur für die System-DPI-Einstellung. Die DPI-Synchronisierung erfolgt während der anfänglichen Verbindung, und die Anzeigeskalierung wird im Falle einer erneuten Verbindung, falls erforderlich, ausgeführt. Wenn die DPI-Synchronisierung funktioniert und die DPI-Einstellung des Clientsystems mit der DPI-Einstellung des Remote-Desktops übereinstimmt, kann die Anzeigeskalierung auch dann nicht in Kraft treten, wenn Sie die Option **Anzeigeskalierung zulassen** in der Benutzeroberfläche auswählen. Windows lässt nicht zu, dass Benutzer die DPI-Einstellung auf Systemebene für die aktuelle Benutzersitzung ändern, und die DPI-Synchronisierung wird nur durchgeführt, wenn sie sich anmelden und eine Remote-Sitzung starten. Wenn Benutzer die DPI-Einstellung während einer-Remote-Sitzung ändern, müssen sie sich abmelden und erneut anmelden, damit die DPI-Einstellung des Remote-Desktops mit der neuen DPI-Einstellung des Clientsystems übereinstimmt.

Die DPI-Einstellung des Agents befindet sich in der Windows-Registrierung unter `Computer \HKEY_CURRENT_USER\Control Panel\Desktop: logPixels`.

Hinweis Die System-DPI-Einstellung ist möglicherweise nicht dieselbe wie die DPI-Einstellung des Hauptmonitors. Wenn Sie beispielsweise den Hauptmonitor schließen und das System zu einer externen Anzeige wechselt, die eine andere DPI-Einstellung als der Hauptmonitor aufweist, ist die DPI-Einstellung des Systems immer noch identisch mit der DPI-Einstellung des zuvor geschlossenen Hauptmonitors.

Diese Version von Horizon Client unterstützt nicht die Agent-Gruppenrichtlinieneinstellung **DPI-Synchronisierung pro Verbindung**, die mit Horizon Agent-Versionen 7.8 bis 2006 bereitgestellt wird.

Weitere Informationen zu den Gruppenrichtlinieneinstellungen für DPI-Synchronisierungsrichtlinien finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon* für Ihre Horizon Agent-Version.

Unterstützte Gastbetriebssysteme für virtuelle Desktops

Für virtuelle Desktops wird die DPI-Synchronisierungsfunktion auf folgenden Gastbetriebssystemen unterstützt:

- Windows 7, 32 oder 64 Bit
- Windows 8.x, 32 oder 64 Bit
- Windows 10, 32 oder 64 Bit
- Windows Server 2008 R2, als Desktop konfiguriert
- Windows Server 2012 R2, als Desktop konfiguriert
- Windows Server 2016, als Desktop konfiguriert
- Windows Server 2019, als Desktop konfiguriert

Hinweis Für Windows-Servercomputer, die als Desktop konfiguriert sind, wird die Funktion „DPI-Synchronisierung pro Monitor“ nicht unterstützt.

Unterstützte RDS-Hosts für veröffentlichte Desktops und veröffentlichte Anwendungen

Für veröffentlichte Desktops und Anwendungen wird DPI-Synchronisierungsfunktion auf folgenden RDS-Hosts unterstützt:

- Windows Server 2012 R2
- Windows Server 2016

- Windows Server 2019

Hinweis Für RDS-Hosts wird die Funktion „DPI-Synchronisierung pro Monitor“ nicht unterstützt. Diese Einschränkung gilt nicht für veröffentlichte Anwendungen, die auf Desktop-Pools mit der Funktion für VM-gehostete Anwendungen ausgeführt werden.

Ändern des Anzeigemodus für einen Remote-Desktop

Sie können den Anzeigemodus vor oder nach der Verbindung mit einem Remote-Desktop ändern, wie z. B. vom Modus **Alle Monitore** in den **Vollbild**-Modus. Diese Funktion wird für veröffentlichte Anwendungen nicht unterstützt.

Verfahren

1. Starten Sie Horizon Client und stellen Sie eine Verbindung mit einem Server her.
2. Öffnen Sie das Dialogfeld „Einstellungen“ für den Remote-Desktop.
   - Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Symbol für **Einstellungen** (Zahnrad) und wählen Sie im linken Bereich den Remote-Desktop aus.
   - Klicken Sie im Fenster für die Desktop- und Anwendungsauswahl mit der rechten Maustaste auf den Remote-Desktop und wählen Sie **Einstellungen** aus.
3. Wählen Sie im Dropdown-Menü **Anzeigen** den Anzeigemodus aus.

Option	Beschreibung
Alle Monitore	Zeigt das Remote-Desktop-Fenster auf mehreren Monitoren an. Das Remote-Desktop-Fenster wird standardmäßig auf allen Monitoren dargestellt.
Vollbild	Zeigt das Remote-Desktop-Fenster so an, dass es den ganzen Bildschirm ausfüllt.
Fenster - groß	Legt die Größe des Remote-Desktop-Fensters auf 1.904 x 978 Pixel fest.
Fenster - klein	Legt die Größe des Remote-Desktop-Fensters auf 640 x 480 Pixel fest.
Benutzerdefiniert	Zeigt einen Schieberegler an, mit dem Sie eine benutzerdefinierte Größe für das Remote-Desktop-Fenster konfigurieren können.

4. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.
5. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

   Wenn Sie mit dem Remote-Desktop verbunden sind, werden Ihre Änderungen sofort übernommen. Wenn Sie nicht mit dem Remote-Desktop verbunden sind, werden die Änderungen angewendet, wenn Sie sich verbinden. Horizon Client speichert Anzeigeeinstellungen in einer Einstellungsdatei für den Remote Desktop, nachdem Sie Horizon Client beendet haben.

Ergebnisse

Wenn Sie im Modus **Alle Monitore** auf die Schaltfläche **Minimieren** klicken und das Fenster dann wieder maximieren, wechselt es zurück in den Modus **Alle Monitore**. Dies gilt ebenso für ein minimiertes Fenster im **Vollbild**-Modus: Nach der Maximierung wird wieder der **Vollbild**-Modus auf einem Monitor angezeigt.

Hinweis Wenn Horizon Client alle Monitore verwendet und Sie das Fenster einer veröffentlichten Anwendung maximieren, wird das Fenster nur in dem Monitor auf die Vollbildansicht erweitert, der das Fenster enthält.

Anpassen der Anzeigeauflösung und Anzeigeskalierung für einen Remote-Desktop

Sie können Horizon Client verwenden, um die Anzeigeauflösung und die Anzeigeskalierung für einen Remote-Desktop anzupassen. Die Anzeigeauflösung bestimmt die Schärfe des Texts und der Bilder. Bei höheren Auflösungen, z. B. 1600 x 1200 Pixel, werden die Elemente schärfer angezeigt. Die Anzeigeskalierung, die als Prozentsatz dargestellt wird, erhöht oder verringert die Größe von Text, Symbolen und Navigationselementen.

Standardmäßig werden die Einstellungen für die benutzerdefinierte Anzeigeauflösung und die Anzeigeskalierung nur auf dem lokalen Clientsystem gespeichert. Ein Administrator kann die Gruppenrichtlinieneinstellung **Auflösung und DPI-Wert auf Server speichern** verwenden, um diese Einstellungen auf dem Server zu speichern, sodass sie immer angewendet werden, unabhängig vom Clientgerät, mit dem Sie sich beim Remote-Desktop anmelden. Weitere Informationen finden Sie unter Allgemeine Einstellungen für Client-GPOs.

Für diese Funktion sollten die im Folgenden aufgeführten Einschränkungen und Überlegungen beachtet werden.

- Das Anpassen und Skalieren der Anzeigeauflösung für einen Remote-Desktop wird im Modus für mehrere Monitore nicht unterstützt.
- Wenn Sie eine benutzerdefinierte Auflösung auswählen, die höher oder niedriger als die Auflösung des Clients ist, passt Horizon Client die Größe des Remote-Desktop-Fensters an das Clientfenster an.
- Wenn Sie die Anzeigeauflösung während einer Remote-Desktop-Sitzung anpassen, werden Ihre Änderungen sofort wirksam. Wenn Sie die Anzeigeskalierung während einer Remote-Desktop-Sitzung anpassen, müssen Sie sich ab- und erneut anmelden, damit Ihre Änderungen wirksam werden.
- Die Horizon Client-Gruppenrichtlinieneinstellung **Gesperrte Gastgröße** hat Vorrang vor der Anpassung der Anzeigeauflösung. Weitere Informationen finden Sie unter Einstellungen für die Skriptdefinition für Client-GPOs.

Verfahren

1 Starten Sie Horizon Client und stellen Sie eine Verbindung mit einem Server her.

2 Klicken Sie im Fenster für die Desktop- und Anwendungsauswahl mit der rechten Maustaste auf den Remote Desktop und wählen Sie **Einstellungen** aus.

3 Wählen Sie im Menü **Verbindung über** die Option **VMware Blast** oder **PCoIP** aus.

4 Wählen Sie im Dropdown-Menü **Anzeige** die Option **Vollbild**, **Fenster – groß**, **Fenster – klein** oder **Benutzerdefiniert** aus.

5 Um die Anzeigeauflösung anzupassen, wählen Sie eine Auflösung aus dem Dropdown-Menü **Auflösung** aus.

   Wenn Sie **Automatisch** (Standardeinstellung) auswählen, passt Horizon Client den Remote-Desktop der Fenstergröße des Clients an. Wenn der Remote-Desktop die von Ihnen ausgewählte Anzeigeauflösung nicht unterstützt, wird die Standardeinstellung verwendet.

6 Um die Anzeigeskalierung anzupassen, wählen Sie eine Skalierungsgröße aus dem Dropdown-Menü **Skalierung** aus.

   Wenn Sie **Automatisch** (Standardeinstellung) auswählen, synchronisiert Horizon Client die Anzeigeskalierung des Client Systems mit dem Remote-Desktop.

7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Verwenden von USB-Geräten

Mit der USB-Umleitungsfunktion können Sie lokal angeschlossene USB-Geräte wie Thumb-Flashlaufwerke auf einem Remote Desktop oder in einer veröffentlichten Anwendung verwenden.

Wenn Sie die USB-Umleitungsfunktion verwenden, stehen die meisten USB-Geräte, die an das lokale Clientsystem angeschlossen sind, in Menüs in Horizon Client zur Verfügung. Über diese Menüs können Sie die Geräte verbinden oder deren Verbindung trennen.

Informationen zu den Anforderungen an USB-Geräte und Einschränkungen für die USB-Umleitung finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Sie können USB-Geräte sowohl manuell als auch automatisch mit einem Remote-Desktop oder einer veröffentlichten Anwendung verbinden.

Dieser Vorgang beschreibt, wie Sie mit Horizon Client die automatische Verbindung von USB-Geräten mit einem Remote Desktop oder mit einer veröffentlichten Anwendung konfigurieren. Sie können die automatische Verbindung auch konfigurieren, indem Sie die Horizon Client-Befehlszeilenschnittstelle verwenden oder eine Gruppenrichtlinie konfigurieren.

Weitere Informationen über die Befehlszeilenschnittstelle finden Sie unter Ausführen von Horizon Client über die Befehlszeile. Weitere Informationen zur Konfiguration von Gruppenrichtlinien finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Voraussetzungen

- Um USB-Geräte mit einem Remote-Desktop oder mit einer veröffentlichten Anwendung verwenden zu können, muss ein Horizon-Administrator die Funktion der USB-Umleitung aktivieren.

Diese Aufgabe schließt die Installation der USB-Umleitungskomponente von Horizon Agent ein und kann auch die Einrichtung von Richtlinien hinsichtlich der USB-Umleitung umfassen. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon* und unter USB-Einstellungen für Client-GPOs.

- Die USB-Umleitungskomponente muss in Horizon Client installiert sein. Wenn Sie diese Komponente bei der Installation nicht berücksichtigt haben, deinstallieren Sie Horizon Client und führen Sie das Installationsprogramm erneut aus, um die USB-Umleitungskomponente mit einzuschließen.

  Anweisungen zur Installation finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*.

- Machen Sie sich mit Einschränkungen der USB-Umleitung vertraut.

Verfahren

- Verbinden Sie das USB-Gerät manuell mit einem Remote-Desktop.
  a. Schließen Sie das USB-Gerät an das lokale Clientsystem an.
  b. Klicken Sie in der VMware Horizon Client-Menüleiste auf dem Remote Desktop auf **USB-Gerät verbinden**.
  c. Wählen Sie das USB-Gerät aus.

  Das Gerät wird manuell vom lokalen System an den Remote-Desktop umgeleitet.

- Verbinden Sie das USB-Gerät mit einer veröffentlichten Anwendung.
  a. Schließen Sie das USB-Gerät an das lokale Clientsystem an.
  b. Starten Sie Horizon Client und stellen Sie eine Verbindung mit der veröffentlichten Anwendung her.
  c. Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Zahnradsymbol **Einstellungen** und dann auf **USB-Geräte**.
  d. Wählen Sie im rechten Bereich das USB-Gerät aus, klicken Sie auf **Verbinden**, wählen Sie die veröffentlichte Anwendung aus und klicken Sie auf **OK**.

     Horizon Client verbindet das USB-Gerät mit der ausgewählten veröffentlichten Anwendung. Das USB-Gerät steht auch für andere Anwendungen in derselben Serverfarm wie die ausgewählte Anwendung zur Verfügung.
  e. (Optional) Um Horizon Client für die automatische Verbindung des USB-Geräts mit der veröffentlichten Anwendung beim Start der Anwendung zu konfigurieren, aktivieren Sie das Kontrollkästchen **Beim Start automatisch verbinden**.

f (Optional) Um Horizon Client für die automatische Verbindung des USB-Geräts mit der veröffentlichten Anwendung zu konfigurieren, wenn das Gerät an das lokale System angeschlossen wird, aktivieren Sie das Kontrollkästchen **Beim Einlegen automatisch verbinden**.

Die veröffentlichte Anwendung muss aktiviert und im Vordergrund sein, damit dieses Verhalten wirksam wird.

g Klicken Sie auf **OK**, um das Dialogfeld „Einstellungen“ zu schließen.

h Wenn Sie die veröffentlichte Anwendung nicht mehr verwenden, öffnen Sie erneut das Dialogfeld „Einstellungen“, wählen Sie **USB-Geräte** und dann **Verbindung trennen** aus.

Sie müssen das USB-Gerät freigeben, damit Sie darauf von Ihrem lokalen System aus zugreifen können.

- Konfigurieren Sie Horizon Client dahingehend, dass USB-Geräte automatisch mit einem Remote-Desktop verbunden werden, wenn Sie diese an das lokale System anschließen.

  Mit der Funktion zur automatischen Verbindung haben Sie die Möglichkeit, Geräte mit MTP-Treibern zu verbinden, so zum Beispiel Android-basierte Samsung-Smartphones und -Tablets.

  a Bevor Sie das USB-Gerät anschließen, starten Sie Horizon Client und stellen Sie die Verbindung mit dem Remote-Desktop her.

  b Klicken Sie in der VMware Horizon Client-Menüleiste auf dem Remote Desktop auf **USB-Gerät verbinden > Beim Einlegen automatisch verbinden**.

  c Schließen Sie das USB-Gerät an.

  USB-Geräte, die Sie nach dem Start von Horizon Client an Ihr lokales System anschließen, werden an den Remote-Desktop umgeleitet.

- Konfigurieren Sie Horizon Client zur automatischen Verbindung von USB-Geräten mit einem Remote-Desktop, wenn Horizon Client gestartet wird.

  a Klicken Sie in der VMware Horizon Client-Menüleiste auf dem Remote Desktop auf **USB-Gerät verbinden > Beim Start automatisch verbinden**.

  b Schließen Sie das USB-Gerät an und starten Sie Horizon Client neu.

  USB-Geräte, die Sie beim Start von Horizon Client an Ihr lokales Clientsystem anschließen, werden an den Remote Desktop umgeleitet.

Ergebnisse

Das USB-Gerät wird im Remote-Desktop oder in der veröffentlichten Anwendung angezeigt. Es kann dabei bis zu 20 Sekunden dauern, bis das USB-Gerät auf dem Remote Desktop oder in der veröffentlichten Anwendung eingeblendet wird. Bei erstmaliger Verbindung des Geräts mit einem Remote-Desktop werden Sie eventuell dazu aufgefordert, bestimmte Treiber zu installieren.

Wird das USB-Gerät auch nach mehreren Minuten nicht auf dem Remote-Desktop in der veröffentlichten Anwendung angezeigt, sollten Sie die Verbindung trennen und das Gerät anschließend erneut mit dem Clientcomputer verbinden.

Nächste Schritte

Bei Problemen mit der USB-Umleitung finden Sie weitere Informationen im Kapitel über die Behebung von Problemen bei der USB-Umleitung im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Einschränkungen der USB-Umleitung

Für die USB-Umleitungsfunktion gelten bestimmte Einschränkungen.

- Beim Zugriff auf ein USB-Gerät von einem Menü in Horizon Client und Verwendung des Geräts in einem Remote-Desktop oder einer veröffentlichten Anwendung können Sie nicht auf dem lokalen Gerät auf das USB-Gerät zugreifen.
- Zu den USB-Geräten, die nicht im Menü angezeigt werden, aber auf dem Remote-Desktop oder in der veröffentlichten Anwendung verfügbar sind, zählen Eingabegeräte (Human Interface Devices) wie zum Beispiel Tastaturen und Zeigegeräte. Der Remote-Desktop oder die veröffentlichte Anwendung und das lokale Gerät verwenden diese Geräte gleichzeitig. Die Interaktion mit diesen USB-Geräten kann aufgrund der Netzwerklatenz manchmal recht langsam sein.
- Große USB-Festplattenlaufwerke können erst nach mehreren Minuten auf dem Remote Desktop oder in der veröffentlichten Anwendung angezeigt werden.
- Manche USB-Geräte erfordern bestimmte Treiber. Wenn der erforderliche Treiber nicht bereits installiert ist, werden Sie möglicherweise bei Verbindung des USB-Geräts mit dem Remote-Desktop oder der veröffentlichten Anwendung zu Installation dieses Treibers aufgefordert.
- Wenn Sie USB-Geräte verbinden möchten, die MTP-Treiber verwenden, so zum Beispiel Android-basierte Samsung-Smartphones und -Tablets, müssen Sie Horizon Client so konfigurieren, dass die USB-Geräte automatisch mit dem Remote Desktop oder der veröffentlichten Anwendung verbunden werden. Anderenfalls wird das USB-Gerät beim Versuch der manuellen Umleitung über ein Menüelement erst umgeleitet, nachdem Sie das Gerät getrennt und neu verbunden haben.
- Stellen Sie keine Verbindung mit Scannern über das Menü **USB-Gerät verbinden** her. Um einen Scanner zu verwenden, nutzen Sie die Scannerumleitungsfunktion. Siehe Verwenden von Scannern.
- Die Umleitung von USB-Audiogeräten ist vom Netzwerkstatus abhängig und daher nicht zuverlässig. Manche Geräte erfordern auch im Ruhezustand einen hohen Datendurchsatz. Audioeingabe- und -ausgabegeräte funktionieren gut mit der Echtzeit-Audio/Video-Funktion. Sie müssen für diese Geräte keine USB-Umleitung verwenden.
- Sie können kein umgeleitetes USB-Laufwerk auf einem veröffentlichten Desktop konfigurieren, solange Sie keine Verbindung als Administrator hergestellt haben.

- Eine automatische Verbindung mit einer veröffentlichten Anwendung beim Start und beim Einstecken ist mit globalen Anwendungsberechtigungen nicht möglich.

Hinweis Leiten Sie keine USB-Geräte wie USB-Ethernet-Geräte und Touchscreen-Geräte an einen Remote-Desktop oder an eine veröffentlichte Anwendung um. Wenn Sie ein USB-Ethernet-Gerät umleiten, verliert Ihr lokales Clientsystem die Verbindung zum Netzwerk. Wenn Sie ein Touchscreen-Gerät umleiten, empfängt der Remote-Desktop oder die veröffentlichte Anwendung Eingaben vom Touchscreen und nicht von der Tastatur. Wenn Sie Ihren Remote-Desktop oder Ihre veröffentlichte Anwendung zur automatischen Verbindung von USB-Geräten konfiguriert haben, können Sie Richtlinien konfigurieren, um bestimmte Geräte auszuschließen.

Verwenden von Webcams und Mikrofonen

Mit der Echtzeit-Audio/Video-Funktion können Sie die Webcam oder das Mikrofon des lokalen Clientsystems auf einem Remote-Desktop oder in einer veröffentlichten Anwendung verwenden. Echtzeit-Audio/Video ist mit Standard-Konferenzanwendungen und browserbasierten Videoanwendungen kompatibel. Die Funktion unterstützt standardmäßige Webcams, USB-Audiogeräte und analoge Audioeingänge.

Informationen zum Einrichten der Echtzeit-Audiovideofunktion auf dem Agent Computer, einschließlich der Konfiguration von Frame-Rate und Bildauflösung, finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Wann Sie eine Webcam mit der Echtzeit-Audiovideofunktion verwenden können

Wenn ein Horizon Administrator die Echtzeit-Audiovideofunktion konfiguriert hat, können Sie eine Webcam verwenden, die in den Client Computer in einem Remote-Desktop oder in einer veröffentlichten Anwendung integriert ist oder damit verbunden ist. Sie können die Webcam in Konferenzanwendungen wie z. B. Skype, Webex oder Google Hangouts verwenden.

Bei der Einrichtung einer Anwendung wie Skype, Webex oder Google Hangouts auf einem Remote-Desktop können Sie Ein- und Ausgabegeräte aus Menüs in der Anwendung auswählen.

Für virtuelle Desktops, auf denen Horizon Agent 7.9 oder früher installiert ist, und für veröffentlichte Desktops und Anwendungen kann mit Echtzeit-Audiovideo nur eine Webcam umgeleitet werden, die in Anwendungen „VMware Virtual Webcam“ heißt. Für virtuelle Desktops, auf denen Horizon Agent 7.10 oder höher installiert ist, kann mit Echtzeit-Audiovideo mehr als eine Webcam umgeleitet werden. Der Name einer umgeleiteten Webcam ist dann der tatsächliche Gerätename mit angehängtem „(VDI)“, z. B. „C670i FHD Webcam (VDI)“.

Für viele Anwendungen müssen Sie kein Eingabegerät auswählen.

Wenn der Client Computer die Webcam verwendet, kann die Remotesitzung sie nicht gleichzeitig verwenden. Wenn die Remotesitzung die Webcam verwendet, kann auch der Client Computer sie nicht gleichzeitig verwenden.

Wichtig Wenn Sie eine USB-Webcam verwenden, verbinden Sie diese nicht über das Menü **USB-Gerät verbinden** in Horizon Client. Durch diesen Vorgang würde das Gerät über die USB-Umleitung geleitet. Die Leistung eignet sich dann nicht für Videochat.

Wenn mehr als eine Webcam mit dem Client Computer verbunden ist, müssen Sie eine bevorzugte Webcam für die Verwendung in Remotesitzungen für veröffentlichte Desktops und Anwendungen sowie für virtuelle Desktops konfigurieren, die mehrere Webcams nicht unterstützen.

Weitere Informationen finden Sie unter Auswählen einer bevorzugten Webcam oder eines Mikrofons auf einem Windows-Clientsystem.

Auswählen einer bevorzugten Webcam oder eines Mikrofons auf einem Windows-Clientsystem

Wenn für die Echtzeit-Audio/Video-Funktion mehrere Webcams oder Mikrofone mit dem Clientsystem verbunden sind, können Sie durch die Konfiguration der Echtzeit-Audio/Video-Einstellungen in Horizon Client festlegen, welche Webcam oder welches Mikrofon bevorzugt werden soll.

Mit der Echtzeit-Audio/Video-Funktion arbeiten Videogeräte, Audioeingabe- und Audioausgabegeräte ohne Verwendung der USB-Umleitung ordnungsgemäß und die erforderliche Netzwerkbandbreite wird erheblich verringert. Analoge Audioeingabegeräte werden ebenfalls unterstützt.

Wenn verfügbar, wird die bevorzugte Webcam oder das bevorzugte Mikrofon im Remote-Desktop oder in der veröffentlichten Anwendung verwendet. Wenn die bevorzugte Webcam oder das bevorzugte Mikrofon nicht verfügbar ist, wird eine andere Webcam oder ein anderes Mikrofon verwendet.

Hinweis Wenn Sie eine USB-Webcam oder ein USB-Mikrofon verwenden, verbinden Sie diese nicht über das Menü **USB-Gerät verbinden** in Horizon Client. In diesem Fall würde das Gerät über die USB-Umleitung umgeleitet, sodass die Echtzeit-Audio/Video-Funktion nicht genutzt werden kann.

Für virtuelle Desktops, auf denen Horizon Agent 7.10 oder höher installiert ist, unterstützt die Funktion „Echtzeit-Audio/Video“ mehrere Webcam- und Mikrofongeräte.

Voraussetzungen

- Stellen Sie sicher, dass eine USB-Webcam, ein USB-Mikrofon oder ein anderer Mikrofontyp auf dem Clientsystem installiert und betriebsbereit ist.
- Stellen Sie sicher, dass das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll für den Remote-Desktop oder die veröffentlichte Anwendung verwendet wird.

- Stellen Sie eine Verbindung mit einem Server her.

Verfahren

1. Öffnen Sie das Dialogfeld **Einstellungen** und wählen Sie im linken Bereich die Option **Echtzeit-Audio/Video** aus.
   - Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Zahnradsymbol **Einstellungen**.
   - Klicken Sie mit der rechten Maustaste auf einen Remote-Desktop oder eine veröffentlichte Anwendung im Fenster für die Desktop- und Anwendungsauswahl und wählen Sie **Einstellungen** aus.
2. Um eine bevorzugte Webcam zu konfigurieren, wählen Sie im Dropdown-Menü **Bevorzugte Webcam** eine Webcam aus.
3. Um ein bevorzugtes Mikrofon zu konfigurieren, wählen Sie ein bestimmtes Mikrofon oder **Alle** im Dropdown-Menü **Bevorzugtes Mikrofon** aus.

   Wenn der Remote-Desktop mehrere Geräte mit der Funktion „Echtzeit-Audio/Video“ unterstützt und Sie ein bestimmtes Mikrofon auswählen, werden nur die ausgewählten Mikrofon- und Webcam-Geräte auf den Remote-Desktop umgeleitet. Wenn Sie **Alle** auswählen, werden alle verfügbaren Mikrofon- und Webcam-Geräte auf den Remote-Desktop umgeleitet.
4. Um die Änderungen zu speichern, klicken Sie auf **OK** oder auf **Anwenden**.

Verwenden mehrerer Geräte mit der Echtzeit-Audio/Video-Funktion

Wenn mehr als eine Webcam oder ein Mikrofon mit dem Client Computer verbunden ist und der Remote-Desktop die Umleitung mehrerer Geräte mit der Echtzeit-Audio/Video-Funktion unterstützt, können Sie alle Webcams und Mikrofone verwenden, die mit dem Clientcomputer am Remote-Desktop verbunden sind.

Diese Funktion wird nur mit virtuellen Desktops unterstützt, auf denen Horizon Agent 7.10 oder höher installiert ist. Sie wird für veröffentlichte Desktops oder Anwendungen nicht unterstützt. Die vollständigen Informationen zu den Systemanforderungen finden Sie unter Systemanforderungen für Echtzeit-Audio/Video.

Im Folgenden finden Sie Tipps zur Verwendung von mehr als einer Webcam oder einem Mikrofon mit der Echtzeit-Audio/Video-Funktion.

- Wenn Sie eine Verbindung mit einem Remote-Desktop herstellen, leitet die Echtzeit-Audio/Video-Funktion alle Webcams und Mikrofone um, die aktuell mit dem Clientcomputer verbunden sind. Der Remote-Desktop entscheidet, welche Webcam und welches Mikrofon jeweils das Standardgerät ist. Sie müssen in Horizon Client keine bevorzugte Webcam bzw. kein bevorzugtes Mikrofon konfigurieren.

- Wenn Sie in Anwendungen wie Skype for Business standardmäßig dasselbe Mikrofon verwenden möchten, müssen Sie ein Standardmikrofon konfigurieren. Anderenfalls werden alle Mikrofone umgeleitet und Sie müssen bei jeder Verwendung der Anwendung ein Mikrofon auswählen. Weitere Informationen finden Sie unter Auswählen einer bevorzugten Webcam oder eines Mikrofons auf einem Windows-Clientsystem.
- Wenn Sie eine Webcam oder ein Mikrofon vom Clientcomputer trennen und das Gerät nicht in einer Anwendung auf dem Remote-Desktop verwendet wird, löscht die Echtzeit-Audio/Video-Funktion das Gerät sofort vom Remote-Desktop. Wenn das Gerät von einer Anwendung auf dem Remote-Desktop verwendet wird, löscht die Echtzeit-Audio/Video-Funktion das Gerät, nachdem es von der Anwendung freigegeben wurde.
- Der Anzeigename eines umgeleiteten Geräts ist der tatsächliche Gerätename mit (VDI) angehängt, z. B. C670i FHD Webcam (VDI).
- Sie können mehrere umgeleitete Geräte gleichzeitig auf einem Remote-Desktop verwenden.

Auswählen eines bevorzugten Lautsprechers für einen Remote-Desktop

Wenn mehrere Lautsprecher mit dem Clientsystem verbunden sind, können Sie angeben, welcher Lautsprecher auf einem Remote Desktop bevorzugt wird.

Für diese Funktion gelten die im Folgenden aufgeführten Einschränkungen.

- Diese Funktion wird nur für virtuelle Desktops unterstützt. Sie wird für veröffentlichte Desktops und Anwendungen nicht unterstützt.
- Wenn Sie während einer Remotesitzung einen Lautsprecher zum Clientsystem hinzufügen oder daraus entfernen, werden die Änderungen auf dem Remote Desktop nicht wirksam.

Voraussetzungen

- Vergewissern Sie sich, ob mehrere Lautsprecher auf dem Clientsystem installiert und betriebsbereit sind.
- Vergewissern Sie sich, dass Sie das VMware Blast-Anzeigeprotokoll für die Verbindung mit dem Remote-Desktop verwenden. Diese Funktion funktioniert nicht mit anderen Anzeigeprotokollen.
- Stellen Sie sicher, dass Horizon Agent 2012 oder höher auf dem Remote-Desktop installiert ist. Bei früheren Horizon Agent-Versionen wird Audio auf dem standardmäßigen Audiogerät wiedergegeben, das an das Clientsystem angeschlossen ist.
- Stellen Sie eine Verbindung mit dem Server her.

Verfahren

1 Öffnen Sie das Dialogfeld **Einstellungen** und wählen Sie im linken Bereich die Option **Echtzeit-Audio/Video** aus.

   - Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Zahnradsymbol **Einstellungen**.
   - Klicken Sie im Fenster für die Desktop- und Anwendungsauswahl mit der rechten Maustaste auf den Remote-Desktop und wählen Sie **Einstellungen** aus.

2 Wählen Sie aus dem Dropdown-Menü **Bevorzugter Lautsprecher** einen Lautsprecher aus.

   Hinweis Diese Funktion ist unabhängig von der Echtzeit-Audio-Video-Funktion, auch wenn Sie auf der Seite **Echtzeit-Audio-Video** angezeigt wird.

   Wenn Sie einen bestimmten Lautsprecher auswählen, wird nur der ausgewählte Lautsprecher an den Remote Desktop umgeleitet. Wenn Sie **Alle** auswählen, werden alle verfügbaren Lautsprecher auf den Remote Desktop umgeleitet. Wenn Sie **Standard** auswählen, wird Audio auf dem standardmäßigen Audiogerät wiedergegeben, das mit dem Clientsystem verbunden ist.

3 Um die Änderungen zu speichern, klicken Sie auf **OK** oder auf **Anwenden**.

Freigeben von Remote-Desktop-Sitzungen

Mit der Funktion „Session Collaboration“ können Sie andere Benutzer zur Teilnahme an einer vorhandenen Remote-Desktop-Sitzung einladen. Eine auf diese Weise freigegebene Remote-Desktop-Sitzung wird als gemeinsame Sitzung bezeichnet. Der Benutzer, der eine Sitzung für einen anderen Benutzer freigibt, wird als Sitzungsbesitzer bezeichnet, und der Benutzer, der einer gemeinsamen Sitzung beitritt, wird als Sitzungsteilnehmer bezeichnet.

Ein Horizon-Administrator muss die Funktion „Session Collaboration“ aktivieren.

Bei Windows-Desktops gehört dazu auch die Aktivierung der Funktion „Session Collaboration“ auf Desktop-Pool- oder Farmebene. Es lassen sich darüber hinaus Gruppenrichtlinien zur Konfiguration von „Session Collaboration“-Funktionen festlegen wie z. B. die verfügbaren Einladungsmethoden. Die vollständigen Informationen zu den Systemanforderungen finden Sie unter Anforderungen für die Funktion „Session Collaboration“.

Informationen zur Aktivierung der Funktion „Session Collaboration“ für Windows-Desktops finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon*. Informationen zur Aktivierung der Funktion „Session Collaboration“ für eine Farm erhalten Sie im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*. Informationen zur Verwendung von Gruppenrichtlinieneinstellungen zur Konfiguration der Funktion „Session Collaboration“ finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Informationen zur Aktivierung der Funktion „Session Collaboration“ für Linux-Desktops finden Sie im Dokument *Einrichten von Linux-Desktops in Horizon*.

Einladen eines Benutzers zu einer Remote-Desktop-Sitzung

Mit der Funktion „Session Collaboration“ können Sie Benutzer zur Teilnahme an einer Remote-Desktop-Sitzung einladen, indem Sie Einladungen zu einer gemeinsamen Sitzung per E-Mail oder Sofortnachricht (nur Windows-Remote-Desktops) versenden oder indem Sie einen Link in die Zwischenablage kopieren und den Link an Benutzer weiterleiten.

Sie können nur Benutzer einer Domäne einladen, für die der Server die Authentifizierung erlaubt. Es lassen sich standardmäßig bis zu fünf Benutzer einladen. Der Horizon-Administrator kann die maximale Anzahl der Benutzer, die eingeladen werden können, ändern.

Für die Funktion „Session Collaboration“ gelten die im Folgenden aufgeführten Einschränkungen.

- Wenn Sie über mehrere Monitore verfügen, wird den Sitzungsteilnehmern nur der primäre Monitor angezeigt.
- Sie müssen beim Erstellen einer Remote-Desktop-Sitzung das VMware Blast-Anzeigeprotokoll für die Freigabe auswählen. Die Funktion „Session Collaboration“ unterstützt keine PCoIP- und RDP-Sitzungen.
- Die H.264-Hardwarecodierung wird nicht unterstützt. Wenn der Besitzer der Sitzung die Hardwarecodierung verwendet und ein Teilnehmer der Sitzung beitritt, wird für beide wieder die Softwarecodierung verwendet.
- Eine anonyme Teilnahme wird nicht unterstützt. Sitzungsteilnehmer müssen durch von Horizon unterstützte Authentifizierungsmechanismen identifizierbar sein.
- Sitzungsteilnehmer müssen Horizon Client oder höher für Windows, Mac oder Linux installiert haben oder HTML Access oder höher verwenden.
- Wenn ein Sitzungsteilnehmer eine nicht unterstützte Version von Horizon Client verwendet, wird eine Fehlermeldung angezeigt, wenn der Benutzer auf einen Teilnahmelink klickt.
- Sie können die Funktion „Session Collaboration“ nicht zur gemeinsamen Nutzung von Sitzungen mit veröffentlichten Anwendungen verwenden.

Voraussetzungen

- Die Funktion „Session Collaboration“ muss aktiviert und konfiguriert sein.
- Um Einladungen per E-Mail zu versenden, muss eine E-Mail-Anwendung installiert sein.
- Zur Verwendung der Methode der Einladung per Sofortnachricht für einen Windows-Remote-Desktop muss Skype for Business installiert und konfiguriert sein.

Verfahren

1. Stellen Sie eine Verbindung mit einem Remote-Desktop her, für den die Funktion „Session Collaboration“ aktiviert ist.

   Sie müssen dafür das VMware Blast-Anzeigeprotokoll verwenden.

2 Klicken Sie in der Taskleiste auf dem Remote-Desktop auf das Symbol **VMware Horizon Collaboration** (z. B. ).

Das Collaboration-Symbol unterscheidet sich je nach verwendeter Version des Betriebssystems.

3 Geben Sie in das geöffnete Dialogfeld „VMware Horizon Collaboration“ den Benutzernamen (z. B. **`Testbenutzer`** oder **`domain\testbenutzer`**) oder die E-Mail-Adresse des Benutzers ein, den Sie zur Remote-Desktop-Sitzung einladen möchten.

Wenn Sie zum ersten Mal den Namen oder die E-Mail-Adresse eines bestimmten Benutzers eingeben, müssen Sie auf **Nach "*Benutzer*" suchen** klicken, ein Komma (,) eingeben oder die **Eingabetaste** drücken, um den Benutzer zu validieren. Bei Windows-Remote-Desktops speichert die Funktion „Session Collaboration“ dann den Benutzer, wenn Sie das nächste Mal seinen Namen oder seine E-Mail-Adresse eingeben.

4 Wählen Sie eine Einladungsmethode aus.

Unter Umständen sind nicht alle Einladungsmethoden verfügbar.

Option	Aktion
E-Mail	Kopiert die Einladung zur Teilnahme in die Zwischenablage und öffnet eine neue E-Mail-Nachricht in der Standard-E-Mail-Anwendung. Für diese Einladungsmethode muss eine E-Mail-Anwendung installiert sein.
Chat	(nur bei Windows-Remote-Desktops) Kopiert die Einladung zur Teilnahme in die Zwischenablage und öffnet ein neues Fenster in Skype for Business. Drücken Sie die Tastenkombination Strg+V, um den Link in das Skype for Business-Fenster einzufügen. Für diese Einladungsmethode muss Skype for Business installiert sein.
Link kopieren	Kopiert die Einladung zur Teilnahme in die Zwischenablage. Sie müssen manuell eine andere Anwendung (wie z. B. Editor) öffnen und darin die Einladung mit Strg+V einfügen.

Ergebnisse

Nach dem Absenden der Einladung wird das Symbol für VMware Horizon Collaboration auch auf dem Desktop angezeigt. Die Benutzeroberfläche von „Session Collaboration“ ändert sich in ein Dashboard, das den aktuellen Status der gemeinsamen Sitzung wiedergibt sowie Optionen für bestimmte Aktionen enthält.

Wenn ein potenzieller Teilnehmer Ihre Einladung annimmt, einer Sitzung auf einem Windows-Remote-Desktop beizutreten, werden Sie über die Funktion „Session Collaboration“ entsprechend informiert. Außerdem wird auf dem Symbol für VMware Horizon Collaboration in der Taskleiste ein roter Punkt angezeigt. Wenn ein Sitzungsteilnehmer Ihre Einladung annimmt, einer Sitzung auf einem Linux-Remote-Desktop beizutreten, wird auf dem Desktop mit der primären Sitzung eine Benachrichtigung angezeigt.

Nächste Schritte

Die Remote-Desktop-Sitzung kann im Dialogfeld „VMware Horizon Collaboration“ verwaltet werden. Siehe Verwalten einer freigegebenen Remote-Desktop-Sitzung.

Verwalten einer freigegebenen Remote-Desktop-Sitzung

Nach dem Absenden einer Einladung zu einer gemeinsamen Sitzung ändert sich die Benutzeroberfläche von „Session Collaboration“ in ein Dashboard, das den aktuellen Status der freigegebenen Remote-Desktop-Sitzung (gemeinsamen Sitzung) wiedergibt sowie Optionen für bestimmte Aktionen enthält.

Ein Horizon-Administrator kann die Übergabe der Steuerung an Sitzungsteilnehmer verhindern. Bei Windows-Remote-Desktops sehen Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon* unter der Gruppenrichtlinieneinstellung **Übergabe der Kontrolle an Kollaboratoren zulassen** nach. Bei Linux-Remote-Desktops sehen Sie im Dokument *Einrichten von Linux-Desktops in Horizon* unter dem Parameter `collaboration.enableControlPassing` nach.

Voraussetzungen

Starten Sie eine gemeinsame Sitzung. Siehe Einladen eines Benutzers zu einer Remote-Desktop-Sitzung.

Verfahren

1. Klicken Sie auf dem Remote-Desktop auf das **VMware Horizon Collaboration**-Symbol in der Taskleiste.

   Die Namen aller Teilnehmer der Sitzung werden in der Spalte „Name“ und deren Status in der Spalte „Status“ angezeigt.

2. Mit dem VMware Horizon Session Collaboration-Dashboard können Sie die gemeinsame Sitzung verwalten.

Option	Aktion
Einladung widerrufen oder Teilnehmer entfernen	Klicken Sie in der Spalte „Status“ auf **Entfernen**.
Kontrolle an Sitzungsteilnehmer übergeben	Nachdem ein Teilnehmer der Sitzung beigetreten ist, setzen Sie die Umschaltoption in der Spalte „Steuerung“ auf **Ein**. Um die Steuerung der Sitzung wieder zu übernehmen, doppelklicken Sie oder drücken Sie eine beliebige Taste. Der Sitzungsteilnehmer kann die Steuerung ebenfalls zurückgeben, indem er die Umschaltoption in der Spalte „Steuerung“ auf **Aus** setzt oder auf die Schaltfläche **Steuerung zurückgeben** klickt.

Option	Aktion
Teilnehmer hinzufügen	Klicken Sie auf **Teilnehmer hinzufügen**.
Gemeinsame Sitzung beenden	Klicken Sie auf **Teilnahme beenden**. Die Verbindung mit allen aktiven Teilnehmern wird getrennt. Bei Windows-Remote-Desktops können Sie die gemeinsame Sitzung auch beenden, indem Sie auf die Schaltfläche **Beenden** neben dem Symbol **VMware Horizon Session Collaboration** klicken. Die Schaltfläche **Beenden** ist bei Linux-Remote-Desktops nicht verfügbar.

Betritt zu einer Remote-Desktop-Sitzung

Mit der Funktion „Session Collaboration“ können Sie auf den Link in einer Einladung zu einer gemeinsamen Sitzung klicken, um einer Remote-Desktop-Sitzung beizutreten. Der Link kann in einer E-Mail-Nachricht, in einer Sofortnachricht oder in einem Dokument enthalten sein, das der Besitzer der Sitzung an Sie weiterleitet. Alternativ haben Sie die Möglichkeit, sich beim Server anzumelden und auf das Symbol für die Sitzung im Fenster für die Remote-Desktop- und Anwendungsauswahl doppelzuklicken.

Dieser Vorgang beschreibt, wie Sie einer Remote-Desktop-Sitzung über eine Einladung zu einer gemeinsamen Sitzung beitreten können.

Hinweis Sie können in einer Umgebung mit Cloud-Pod-Architektur an einer gemeinsamen Sitzung über eine Anmeldung beim Server nur teilnehmen, wenn Sie beim Pod des Sitzungsbesitzers angemeldet sind.

Wenn Sie über die Funktion „Session Collaboration“ einer Remote-Desktop-Sitzung beitreten, können Sie die folgenden Funktionen in der Remote-Desktop-Sitzung nicht verwenden.

- USB-Umleitung
- Echtzeit-Audio/Video (RTAV)
- Multimedia-Umleitung
- Clientlaufwerkumleitung
- Smartcard-Umleitung
- VMware Integrated Printing
- Microsoft Lync-Umleitung
- Dateiumleitung und Funktion „Im Dock behalten“
- Zwischenablagenumleitung

Sie können auch die Auflösung des Remote-Desktops in der Remote-Desktop-Sitzung nicht ändern.

Voraussetzungen

Um über die Funktion „Session Collaboration“ an einer Remote-Desktop-Sitzung teilnehmen zu können, muss auf dem Clientsystem Horizon Client für Windows, Mac oder Linux installiert sein oder HTML Access verwendet werden.

Verfahren

1. Klicken Sie auf den Link in der Einladung zur Teilnahme.

   Horizon Client wird auf dem Clientsystem geöffnet.
2. Geben Sie Ihre Anmeldedaten zur Anmeldung bei Horizon Client ein.

   Nach der erfolgreichen Authentifizierung startet die gemeinsame Sitzung und der Remote-Desktop des Besitzers wird angezeigt. Wenn der Besitzer der Sitzung die Maus- und Tastatursteuerung auf Sie überträgt, können Sie den Remote-Desktop verwenden.
3. Um die Maus- und Tastatursteuerung wieder an den Sitzungsbesitzer zurückzugeben, klicken Sie auf das Symbol **VMware Horizon Collaboration** in der Taskleiste und setzen Sie die Umschaltoption in der Spalte „Steuerung“ auf **Aus** oder klicken Sie auf die Schaltfläche **Steuerung zurückgeben**.
4. Um die gemeinsame Sitzung zu verlassen, klicken Sie auf **Optionen > Verbindung trennen**.

Freigeben lokaler Ordner und Laufwerke

Mit der Funktion der Clientlaufwerkumleitung können Sie Ordner und Laufwerke auf dem lokalen Clientsystem für Remote Desktops und veröffentlichte Anwendungen freigeben.

Zu freigegebenen Laufwerken können auch zugeordnete Laufwerke und USB-Speichergeräte gehören. Zugeordnete Laufwerke können über UNC(Universal Naming Convention)-Pfade verfügen.

Die maximale Länge eines freigegebenen Ordner namens beträgt 117 Zeichen.

Die Funktion der Clientlaufwerkumleitung unterstützt die gemeinsame Nutzung von Microsoft OneDrive, Google Drive und Enterprise-Dateispeicher nicht.

In einem Windows-Remote-Desktop werden freigegebene Ordner und Laufwerke im Ordner **Dieser PC** oder in **Arbeitsplatz** angezeigt, je nach Version des Windows-Betriebssystems. In einer veröffentlichten Anwendung (z. B. Editor) können Sie zu einer Datei in einem freigegeben Ordner oder auf einem freigegebenem Laufwerk wechseln und diese öffnen.

Die Einstellungen für die Clientlaufwerkumleitung gelten für alle Remote Desktops und veröffentlichten Anwendungen.

Voraussetzungen

Zur Freigabe von Ordnern und Laufwerken für einen Remote Desktop oder eine veröffentlichte Anwendung muss die Funktion der Clientlaufwerksumleitung in Horizon Agent installiert sein. Die Funktion der Clientlaufwerksumleitung wird standardmäßig installiert.

Sie können die Funktion der Clientlaufwerkumleitung in Horizon Client durch Aktivierung einer Gruppenrichtlinieneinstellung ausblenden. Weitere Informationen finden Sie unter **Deaktivieren der Freigabe von Dateien und Ordnern** in Allgemeine Einstellungen für Client-GPOs.

Mit Horizon Agent 7.8 und höher können Sie das Verhalten des Laufwerksbuchstabens für Laufwerke konfigurieren, die von der Funktion der Clientlaufwerkumleitung umgeleitet werden, indem Sie die Gruppenrichtlinieneinstellung **Umgeleitetes Gerät mit Laufwerkbuchstaben anzeigen** konfigurieren. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Mit Horizon Agent 7.9 und höher können Sie Ordner auf Geräten, für die Anbieter- und Produkt-IDs angegeben wurden, mit den Gruppenrichtlinieneinstellungen **Vid/Pid-Gerät einschließen** und **Vid/Pid-Gerät ausschließen** einschließen oder ausschließen. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Mit Horizon Agent 7.10 und höher können Sie anhand der Gruppenrichtlinieneinstellungen zum **Laufwerkbuchstaben-Zuordnungsmodus konfigurieren** und zum **Zuordnungstabelle für Laufwerkbuchstaben definieren** festlegen, wie Laufwerkbuchstaben zugeordnet werden. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Wenn der sichere Tunnel auf der Verbindungsserverinstanz aktiviert ist, kann bei der Konfiguration des Browsers auf dem Clientsystem zur Verwendung eines Proxy-Servers die Leistung der Clientlaufwerkumleitung beeinträchtigt werden. Für eine optimale Leistung der Clientlaufwerkumleitung konfigurieren Sie den Browser so, dass kein Proxy-Server verwendet wird oder dass die LAN-Einstellungen automatisch erkannt werden.

Verfahren

1 Öffnen Sie das Dialogfeld „Einstellungen“ und rufen Sie den Bereich „Freigabe“ auf.

Option	Beschreibung
Im Fenster für die Desktop- und Anwendungsauswahl	Klicken Sie mit der rechten Maustaste auf das Symbol eines Remote Desktops oder einer veröffentlichten Anwendung, wählen Sie **Einstellungen** und dann im linken Bereich des eingeblendeten Fensters **Freigabe** aus.
Im bei der Verbindung mit einem Remote Desktop oder einer veröffentlichten Anwendung eingeblendeten Dialogfeld „Freigabe“	Klicken Sie im Dialogfeld auf den Link **Einstellungen > Freigabe**.
Von einem Remote Desktop	Wählen Sie in der Menüleiste **Optionen > Ordner freigeben** aus.

2 Konfigurieren Sie die Einstellungen für die Clientlaufwerkumleitung.

Option	Aktion
Freigeben eines bestimmten Ordners oder Laufwerks für Remote Desktops und veröffentlichte Anwendungen	Klicken Sie auf die Schaltfläche **Hinzufügen**, wechseln Sie zum Ordner oder Laufwerk, der/das freigegeben werden soll und klicken Sie auf **OK**. **Hinweis** Wenn ein USB-Gerät bereits mit einem Remote Desktop oder einer veröffentlichten Anwendung über die USB-Umleitungsfunktion verbunden ist, können Sie keinen Ordner auf dem USB-Gerät freigeben. Darüber hinaus sollten Sie nicht die USB-Umleitungsfunktion aktivieren, die USB-Geräte automatisch beim Start oder beim Anschließen des Geräts verbindet. Wenn Sie dies tun, wird beim nächsten Start von Horizon Client oder beim Anschließen des USB-Geräts die Verbindung mithilfe der USB-Umleitungsfunktion und nicht mithilfe der Funktion zur Clientlaufwerkumleitung hergestellt. Wenn die Zuordnung von Laufwerksbuchstaben konfiguriert ist, werden die in der Freigabeliste konfigurierten Ordner nicht umgeleitet. Weitere Informationen finden Sie unter „Verwenden der Gruppenrichtlinie zum Konfigurieren des Laufwerksbuchstabenverhaltens“ im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.
Freigabe für einen bestimmten Ordner oder ein bestimmtes Laufwerk aufheben	Wählen Sie den Ordner oder das Laufwerk in der Ordnerliste aus und klicken Sie auf die Schaltfläche **Entfernen**.
Remote Desktops und veröffentlichten Anwendungen Zugriff auf Dateien in Ihrem lokalen Benutzerordner gewähren	Aktivieren Sie das Kontrollkästchen **Ihre lokalen Dateien freigeben *Benutzername***.

Option	Aktion
USB-Speichergeräte für Remote Desktops und veröffentlichte Anwendungen freigeben	Aktivieren Sie das Kontrollkästchen **Zugriff auf Wechselmedien erlauben**. Die Funktion der Clientlaufwerkumleitung gibt alle USB-Speichergeräte in Ihrem Clientsystem und alle über FireWire und Thunderbolt verbundenen externen Laufwerke automatisch frei. Die Auswahl eines bestimmten Geräts zur Freigabe ist nicht erforderlich. **Hinweis** USB-Speichergeräte, die bereits über die USB-Umleitungsfunktion mit einem Remote Desktop oder einer veröffentlichten Anwendung verbunden sind, werden nicht freigegeben. Wenn Sie einen verschlüsselten USB-Stick verwenden, müssen Sie Horizon Client vor dem Anschließen des USB-Geräts starten, damit Horizon Client das Gerät erkennen kann. Wenn dieses Kontrollkästchen deaktiviert ist, können Sie mit der USB-Umleitungsfunktion USB-Speichergeräte mit Remote Desktops und veröffentlichten Anwendungen verbinden.
Dialogfeld „Freigabe“ beim Herstellen einer Verbindung mit einem Remote Desktop oder einer veröffentlichten Anwendung nicht anzeigen	Aktivieren Sie das Kontrollkästchen**Dialogfeld bei der Verbindung mit einem Desktop oder einer Anwendung nicht anzeigen**. Wenn dieses Kontrollkästchen deaktiviert ist, wird das Dialogfeld „Freigabe“ angezeigt, wenn Sie zum ersten Mal eine Verbindung zu einem Remote Desktop oder einer veröffentlichten Anwendung herstellen. Wenn Sie sich beispielsweise bei einem Server anmelden und eine Verbindung zu einem Remote Desktop herstellen, wird das Dialogfeld „Freigabe“ angezeigt. Wenn Sie dann eine Verbindung zu einem anderen Remote Desktop oder zu einer anderen veröffentlichten Anwendung herstellen, wird das Dialogfeld nicht angezeigt. Um das Dialogfeld wieder anzuzeigen, müssen Sie die Verbindung zum Server trennen und sich erneut anmelden.

Nächste Schritte

Stellen Sie sicher, dass die freigegebenen Ordner im Remote Desktop oder in der veröffentlichten Anwendung angezeigt werden.

- Öffnen Sie in einem Windows Remote Desktop den Datei-Explorer und suchen Sie im Ordner **Dieser PC** oder öffnen Sie Windows Explorer und suchen Sie im Ordner **Arbeitsplatz**, je nach Version der Windows-Betriebssystemversion.
- Wählen Sie in einer veröffentlichten Anwendung **Datei > Öffnen** oder **Datei > Speichern unter** aus und navigieren Sie zum Ordner oder Laufwerk.

Die Ordner und Laufwerke, die Sie für die Freigabe ausgewählt haben, können eine (oder mehrere) der folgenden Benennungskonventionen verwenden.

Benennungskonvention	Beispiel
Ordnername auf *Desktopname*	jsmith auf JSMITH-W03
Ordnername (*Laufwerksnummer*:)	jsmith (Z:)
Ordnername auf *Desktopname* (*Laufwerksnummer*:)	jsmith auf JSMITH-W03 (Z:)

Für einige Horizon Agent-Versionen kann ein umgeleiteter Ordner zwei Eingänge haben, z. B. unter **Geräte und Laufwerke** und **Netzwerkadressen** auf Windows 10, und beide Eingänge können gleichzeitig angezeigt werden. Wenn alle Volumenbezeichnungen (von A bis Z) bereits verwendet werden, hat der umgeleitete Ordner nur einen Eingang.

Öffnen lokaler Dateien in veröffentlichten Anwendungen

Sie können die Funktion zum Öffnen lokaler Dateien in veröffentlichten Anwendungen direkt aus dem lokalen Dateisystem aktivieren.

Bei dieser Funktion werden auf dem Clientsystem im Menü **Öffnen mit** die verfügbaren veröffentlichten Anwendungen angezeigt, wenn Sie mit der rechten Maustaste auf eine lokale Datei klicken.

Sie können Dateien auch so einstellen, dass sie automatisch in veröffentlichten Anwendungen geöffnet werden, wenn Sie darauf doppelklicken. Bei dieser Funktion werden alle Dateien in Ihrem lokalen Dateisystem mit einer bestimmten Dateierweiterung bei dem Server registriert, auf dem Sie angemeldet sind. Wenn beispielsweise Microsoft Word eine veröffentlichte Anwendung auf dem Server ist, können Sie mit der rechten Maustaste auf eine `.docx`-Datei in Ihrem lokalen Dateisystem klicken und sie mit der veröffentlichten Anwendung Microsoft Word öffnen.

Voraussetzungen

Um lokale Dateien in veröffentlichten Anwendungen zu öffnen, muss ein Horizon-Administrator die Funktion der Clientlaufwerksumleitung in Horizon Agent aktivieren. Die Funktion der Clientlaufwerksumleitung wird standardmäßig installiert. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Sie können die Funktion der Clientlaufwerkumleitung in Horizon Client durch Aktivierung einer Gruppenrichtlinieneinstellung ausblenden. Weitere Informationen finden Sie unter **Deaktivieren der Freigabe von Dateien und Ordnern** in Allgemeine Einstellungen für Client-GPOs.

Verfahren

1 Stellen Sie eine Verbindung mit einem Server her.

2 Öffnen Sie das Dialogfeld „Einstellungen“ und rufen Sie den Bereich „Freigabe“ auf.

Option	Beschreibung
Im Fenster für die Desktop- und Anwendungsauswahl	Klicken Sie mit der rechten Maustaste auf das Symbol eines Remote Desktops oder einer veröffentlichten Anwendung, wählen Sie **Einstellungen** und dann im linken Bereich des eingeblendeten Fensters **Freigabe** aus.
Im bei der Verbindung mit einem Remote Desktop oder einer veröffentlichten Anwendung eingeblendeten Dialogfeld „Freigabe“	Klicken Sie im Dialogfeld auf den Link **Einstellungen > Freigabe**.
Von einem Remote Desktop	Wählen Sie in der Menüleiste **Optionen > Ordner freigeben** aus.

3 Aktivieren Sie das Kontrollkästchen **Lokale Dateien in gehosteten Anwendungen öffnen**.

Wenn diese Option aktiviert ist, können Sie mit der rechten Maustaste auf eine Datei in Ihrem lokalen Dateisystem klicken und diese wahlweise in einer veröffentlichten Anwendung öffnen. Sie können zudem die Eigenschaften der Datei ändern, sodass alle Dateien mit dieser Dateierweiterung standardmäßig mit der veröffentlichten Anwendung geöffnet werden, etwa wenn Sie auf die Datei doppelklicken. Sie können beispielsweise mit der rechten Maustaste auf die Datei klicken, die Option **Eigenschaften** auswählen und auf **Ändern** klicken, um die veröffentlichte Anwendung zum Öffnen dieses Dateityps auszuwählen.

Kopieren und Einfügen

Sie können standardmäßig Elemente vom Clientsystem auf einen Remote Desktop oder in eine veröffentlichte Anwendung kopieren und einfügen.

Wenn Sie das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll verwenden, kann ein Horizon Administrator diese Funktion so konfigurieren, dass Kopier- und Einfügevorgänge nur vom Clientsystem zu einem Remote Desktop oder zu einer veröffentlichten Anwendung oder nur von einem Remote Desktop oder von einer veröffentlichten Anwendung zum Clientsystem zugelassen werden oder beide bzw. keiner der beiden Vorgänge möglich ist.

Ein Horizon Administrator konfiguriert die Möglichkeit zum Kopieren/Einfügen durch die Festlegung von Agent-Gruppenrichtlinien. Je nach installierter Version von Horizon Server und Agent kann ein Administrator auch mit Gruppenrichtlinien Zwischenablageformate für das Kopieren/Einfügen beschränken oder das Kopieren/Einfügen auf Remote Desktops mithilfe von intelligenten Richtlinien steuern. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Kopieren und Einfügen von Text und Bildern

Sie können standardmäßig Elemente vom Clientsystem auf einen Remote Desktop oder in eine veröffentlichte Anwendung kopieren und einfügen. Sie können Elemente auch von einem Remote-Desktop oder einer veröffentlichten Anwendung in das Clientsystem kopieren und einfügen. Dies ist auch zwischen zwei Remote-Desktops oder veröffentlichten Anwendungen möglich, wenn ein Horizon-Administrator die entsprechenden Funktionen aktiviert.

Es werden die im Folgenden aufgeführten Datenformate unterstützt.

- CF_BITMAP
- CF_DIB
- CF_HDROP (Dateityp)
- CF_UNICODETEXT
- Biff12
- Art::GVML ClipFormat
- HTML-Format

- RTF (Rich Text Format)

Wenn Sie beispielsweise Text im Clientsystem kopieren möchten, wählen Sie den Text aus und drücken Sie Strg+C. Um den Text auf einem Remote Desktop einzufügen, drücken Sie auf dem Remote Desktop Strg+V.

Für diese Funktion gelten die im Folgenden aufgeführten Einschränkungen.

- Wenn Sie formatierten Text kopieren, handelt es sich bei den Daten teilweise um Text und teilweise um Formatierungsinformationen. Wenn Sie daher eine große Menge an formatiertem Text oder Text und ein Bild kopieren, kann es beim Einfügen dazu kommen, dass Sie den einfachen Text ganz oder teilweise sehen, nicht aber die Formatierung oder das Bild. Dieses Problem tritt auf, weil die drei Datentypen manchmal getrennt gespeichert werden. Je nach Art des Dokuments können Bilder möglicherweise als Bilder oder als RTF-Daten gespeichert werden.
- Beträgt die Gesamtmenge von Text und RTF weniger als die maximale Größe der Zwischenablage, wird der formatierte Text eingefügt. Es ist häufig der Fall, dass die RTF-Daten nicht gekürzt werden können, sodass die RTF-Daten verworfen werden und nur der reine Text eingefügt wird, sollten Text und Formatierung zusammen mehr als die maximale Größe der Zwischenablage umfassen.
- Sollten Sie nicht in der Lage sein, den gesamten formatierten Text und die von Ihnen ausgewählten Bilder einzufügen, versuchen Sie, geringere Teilmengen zu speichern und einzufügen.

Kopieren und Einfügen von Dateien und Ordnern

Sie können standardmäßig Dateien und Ordner vom Clientsystem auf einen Remote Desktop oder in eine veröffentlichte Anwendung kopieren und einfügen. Sie können auch Dateien und Ordner von einem Remote Desktop oder einer veröffentlichten Anwendung kopieren und in das Clientsystem einfügen, wenn ein Horizon Administrator diese Funktionen aktiviert.

Wenn Sie beispielsweise eine Datei im Clientsystem kopieren möchten, wählen Sie sie aus und drücken Sie Strg + C. Um die Datei auf einem Remote Desktop einzufügen, drücken Sie auf dem Remote Desktop Strg + V.

Diese Funktion erfordert Horizon Agent 2012 oder höher auf dem Agent-Computer.

Die Funktion der Clientlaufwerksumleitung muss auf dem Agentgerät installiert sein, um diese Funktion verwenden zu können. Weitere Informationen finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.

Sie können diese Funktion deaktivieren, indem Sie die Einstellungen **Dateien und Ordner aus eingehenden Zwischenablagedaten filtern** und **Dateien und Ordner aus ausgehenden Zwischenablagedaten filtern** in den Gruppenrichtlinieneinstellung **Formate für Zwischenablagenumleitung konfigurieren** für die Agentmaschine aktivieren. Informationen zu den Agent-Gruppenrichtlinieneinstellungen, die diese Funktion steuern, finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Für diese Funktion gelten die im Folgenden aufgeführten Einschränkungen.

- Sie funktioniert möglicherweise nicht für einige Sonderordner, z. B. den Ordner „Desktop“ oder einen kürzlich aufgerufenen Dateilistenordner, wenn Sie versuchen, mehrere Dateien zu kopieren und einzufügen, weil der Ordner möglicherweise Dateien und Ordner anzeigt, die sich nicht im selben übergeordneten Ordner befinden. Diese Funktion kann nur Dateien und Ordner kopieren und einfügen, die sich im selben übergeordneten Ordner befinden.
- Sie funktioniert möglicherweise nicht für bestimmte Anwendungen, z. B. WordPad und PowerPoint.

Protokollieren der Aktivität „Kopieren und Einfügen“

Wenn Sie die Funktion zur Überwachung der Zwischenablage aktivieren, zeichnet Horizon Agent Informationen zu Kopier- und Einfügeaktivitäten in einem Ereignisprotokoll auf dem Agent-Computer auf. Die Funktion zur Überwachung der Zwischenablage ist standardmäßig deaktiviert.

Diese Funktion gilt nur für das Kopieren und Einfügen von Text und Bildern. Sie gilt nicht für das Kopieren und Einfügen von Dateien und Ordnern.

Um die Funktion zur Überwachung der Zwischenablage nutzen zu können, müssen Sie die Gruppenrichtlinieneinstellung **Zwischenablagenüberwachung konfigurieren** konfigurieren.

Wenn Horizon Agent 7.6 auf dem Agent-Computer installiert ist, werden nur die Informationen zu Zwischenablagedaten, die vom Agent-Computer auf den Client Computer kopiert werden, im Ereignisprotokoll aufgezeichnet. Wenn Horizon Agent 7.7 oder höher auf dem Agent-Computer installiert ist, können Sie die Funktion zur Überwachung der Zwischenablage so konfigurieren, dass nur Informationen zu Daten, die vom Client Computer auf den Agent-Computer kopiert werden, nur zu Daten, die vom Agent-Computer auf den Client Computer kopiert werden, oder zu Daten, die in beide Richtungen kopiert werden, aufgezeichnet werden.

Sie können optional die Gruppenrichtlinieneinstellung **Gibt an, ob die Zwischenablagenumleitung zur Clientseite blockiert wird, wenn der Client die Überwachung nicht unterstützt** konfigurieren, um festzulegen, ob die Umleitung der Zwischenablage für Clients blockiert werden soll, die Funktion zur Überwachung der Zwischenablage nicht unterstützen.

Weitere Informationen zu den Gruppenrichtlinieneinstellungen für die Umleitung der Zwischenablage finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Das Ereignisprotokoll, in dem Informationen Kopier- und Einfügeaktivitäten aufgezeichnet wurden, heißt „VMware Horizon RX Audit“. Um das Ereignisprotokoll auf dem Agent-Computer anzuzeigen, können Sie die Windows-Ereignisanzeige verwenden. Um das Ereignisprotokoll über einen zentralisierten Speicherort anzuzeigen, können Sie VMware Log Insight oder die Windows-Ereignissammlung konfigurieren. Informationen zu Log Insight finden Sie unter https://docs.vmware.com/de/vRealize-Log-Insight/index.html. Informationen zur Windows-Ereignissammlung finden Sie in der Microsoft-Dokumentation.

Konfigurieren der Größe des Zwischenablagespeichers für den Client

Die Größe des Zwischenablagespeichers ist sowohl für den Server als auch für den Client konfigurierbar.

Diese Funktion gilt nur für das Kopieren und Einfügen von Text und Bildern. Sie gilt nicht für das Kopieren und Einfügen von Dateien und Ordnern.

Wenn eine PCoIP- oder VMware Blast-Sitzung eingerichtet wurde, sendet der Server die Größe seines Zwischenablagespeichers an den Client. Die effektive Größe des Zwischenablagespeichers entspricht dem kleineren Wert des Zwischenablagespeichers von Server und Client.

Ändern Sie zum Festlegen der Größe des Zwischenablagespeichers des Clients den Windows-Registrierungswert `HKLM\Software\VMware, Inc.\VMware VDPService\Plugins\MKSVchan \ClientClipboardSize`. Der Werttyp lautet REG_DWORD. Der Wert wird in KB angegeben. Wenn Sie 0 oder keinen Wert eingeben, gilt für den Client die Standardgröße des Zwischenablagespeichers von 8.192 KB (8 MB).

Ein hoher Wert für die Größe des Zwischenablagespeichers kann sich je nach verwendetem Netzwerk negativ auf die Leistung auswirken. VMware empfiehlt für die maximale Größe des Zwischenablagespeichers einen Wert von 16 MB.

Die maximale Größe des Zwischenablagespeichers für Kopier- und Einfügevorgänge beträgt 65.535 KB. Da dieser Grenzwert Metadaten und Formatierungsdaten umfasst, muss die tatsächliche Datengröße etwas weniger als 65.535 KB betragen. Verwenden Sie die Funktion der Clientlaufwerksumleitung, um größere Datenmengen zu übertragen.

Drag & Drop

Die Drag & Drop-Funktion funktioniert unterschiedlich in Abhängigkeit von der Horizon Agent-Version und der Konfiguration.

Mit Horizon Agent 7.9 und höher können Sie Dateien, Ordner, Text, Rich-Text und Bilder zwischen dem Clientsystem und Remote-Desktops sowie veröffentlichten Anwendungen per Drag & Drop verschieben. Mit Horizon Agent 7.7 und 7.8 können Sie nur Dateien und Ordner zwischen dem Clientsystem und Remote-Desktops sowie veröffentlichten Anwendungen per Drag & Drop verschieben. In früheren Versionen von Horizon Agent wird Drag & Drop nicht unterstützt.

Abhängig von der Horizon Agent-Version kann ein Horizon-Administrator bestimmte Gruppenrichtlinieneinstellungen oder intelligente Richtlinien verwenden, um das Drag & Drop-Verhalten zu konfigurieren. Vollständige Informationen zum Konfigurieren der Drag & Drop-Funktion finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon* für Ihre VMware Horizon-Version.

Ziehen von Text und Bildern

Mit Horizon Agent 7.9 und höher können Sie Text, Bilder und andere Datenformate aus dem Clientsystem in eine geöffnete Anwendung in einem Remote-Desktop oder einer veröffentlichten Anwendung ziehen. Beispielsweise können Sie Text aus einem Browser auf dem Clientsystem in

die WordPad-Anwendung auf einem Remote-Desktop ziehen und dort ablegen. Je nachdem, wie die Drag-and-Drop-Funktion konfiguriert ist, können Sie möglicherweise auch Text, Bilder und andere Datenformate von einer geöffneten Anwendung auf einen Remote-Desktop oder einer veröffentlichten Anwendung auf das Clientsystem ziehen.

Es werden die im Folgenden aufgeführten Datenformate unterstützt.

- HTML-Format
- Rich-Text-Format (RTF)
- CF_BITMAP
- CF_DIB
- CF_UNICODETEXT
- FileGroupDescriptorW
- FileGroupDescriptor
- FileContents

Ein Horizon-Administrator kann das Drag & Drop-Verhalten durch Konfigurieren der Gruppenrichtlinieneinstellungen steuern. Mit Horizon Agent 7.9 und Dynamic Environment Manager 9.8 und höher kann ein Horizon-Administrator auch intelligente Richtlinien verwenden, um das Drag-and-Drop-Verhalten zu konfigurieren. Dabei kann er auch die gesamte Drag-and-Drop-Funktion deaktivieren. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Ziehen von Dateien und Ordnern

Mit Horizon Agent 7.7 und höher können Sie Dateien und Ordner zwischen dem Windows-Clientsystem und Remote-Desktops sowie veröffentlichten Anwendungen ziehen und ablegen. Sie können mehrere Dateien und Ordner gleichzeitig per Drag & Drop verschieben. Ein Fortschrittsbalken zeigt den Status des Drag & Drop-Vorgangs.

Wenn Sie Dateien oder Ordner zwischen dem Clientsystem und einem Remote-Desktop ziehen, wird die Datei oder der Ordner im Dateisystem auf dem Zielsystem angezeigt. Wenn Sie eine Datei per Drag & Drop in eine offene Anwendung wie Notepad verschieben, wird der Text in der Anwendung angezeigt. Wenn Sie eine Datei in eine neue E-Mail ziehen, wird die Datei zum Anhang.

Standardmäßig ist das Verschieben per Drag & Drop vom Clientsystem in Remote-Desktops und veröffentlichte Anwendungen aktiviert, von Remote-Desktops und veröffentlichten Anwendungen in das Clientsystem aber deaktiviert. Ein Horizon-Administrator kann die Drag & Drop-Richtung durch Konfigurieren der Gruppenrichtlinieneinstellungen steuern.

Das Ziehen und Ablegen von Dateien, Ordnern und Dateiinhalten erfordert, dass die Funktion der Clientlaufwerksumleitung in Horizon Agent installiert ist. Die Funktion der Clientlaufwerksumleitung wird standardmäßig installiert. Vollständige Informationen zum Konfigurieren der Drag & Drop-Funktion, einschließlich der Funktionsanforderungen, finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon* für Ihre VMware Horizon-Version.

Tipps für die Verwendung der Drag & Drop-Funktion

Wenn Sie die Drag & Drop-Funktion verwenden, befolgen Sie diese Tipps.

Hinweis Je nach Horizon Agent-Version gelten einige Tipps möglicherweise nicht für Ihre Umgebung.

- Sie müssen das VMware Blast- oder PCoIP-Anzeigeprotokoll verwenden.
- Wenn die Funktion der relativen Mausbewegung aktiviert ist (**Optionen > Relative Maus aktivieren**), können Sie nur vom Clientsystem zu einem virtueller Desktop per Drag & Drop verschieben.
- Wenn ein Drag & Drop-Vorgang durchgeführt wird, können Sie keinen neuen starten, bis der erste abgeschlossen wurde.
- Sie können die Drag & Drop-Funktion im geschachtelten Modus nicht verwenden.
- Für den Drag & Drop-Vorgang müssen Sie die primäre Maustaste (standardmäßig die linke) verwenden. Verwenden der sekundären Maustaste (standardmäßig die rechte) und Drücken von Strg + Umschalt + Alt + primäre Maustaste werden nicht unterstützt.
- Sie können zwischen Remote-Desktops nicht per Drag & Drop verschieben.
- Sie können nicht zwischen veröffentlichten Anwendungen aus unterschiedlichen Farmen ziehen und ablegen.
- Wenn Sie Dateien oder Ordner zwischen dem Clientsystem und einem Remote-Desktop per Drag & Drop verschieben, wird die Datei oder der Ordner im Dateisystem auf dem Zielsystem angezeigt. Wenn Sie eine Datei per Drag & Drop in eine offene Anwendung wie Notepad verschieben, wird der Text in der Anwendung angezeigt. Wenn Sie eine Datei in eine neue E-Mail ziehen, wird die Datei zum Anhang.
- Sie können mehrere Dateien und Ordner gleichzeitig per Drag & Drop verschieben. Ein Fortschrittsbalken zeigt den Status des Drag & Drop-Vorgangs.
- Standardmäßig ist das Verschieben per Drag & Drop vom Clientsystem in Remote-Desktops und veröffentlichte Anwendungen aktiviert, von Remote-Desktops und veröffentlichten Anwendungen in das Clientsystem aber deaktiviert.
- Wenn Sie formatierten Text ziehen, handelt es sich bei den Daten teilweise um Text und teilweise um Formatierungsinformationen. Wenn Sie eine große Menge an formatiertem Text

oder Text und ein Bild ziehen, kann es beim Ablegen dazu kommen, dass Sie den einfachen Text ganz oder teilweise sehen, nicht aber die Formatierung oder das Bild. Dieses Problem tritt auf, weil die drei Datentypen manchmal getrennt gespeichert werden. Je nach Art des Dokuments können Bilder möglicherweise als Bilder oder als RTF-Daten gespeichert werden.

- Wenn Sie sowohl reinen Text als auch RTF-Daten ziehen und die Gesamtdatengröße kleiner als der Schwellenwert für die Drag & Drop-Größe ist, wird der formatierte Text kopiert. Da RTF-Daten nicht abgeschnitten werden können, werden die RTF-Daten verworfen und nur der reine Text (oder ein Teil des reinen Texts) wird kopiert, wenn die Gesamtdatengröße der Daten größer als der Schwellenwert für die Drag & Drop-Größe ist.
- Sollten Sie nicht in der Lage sein, den gesamten formatierten Text und die Bilder auf einmal an den gewünschten Ort zu ziehen, versuchen Sie in mehreren Vorgängen jeweils einen Teil des Materials zu übertragen.
- Wenn Sie eine Datei vom Clientsystem per Drag & Drop in eine veröffentlichte Anwendung verschieben, können Sie nicht auf **Speichern unter** klicken, um die Datei zurück in eine andere Datei auf dem Clientsystem zu kopieren. Klicken Sie auf **Speichern**, um die Datei wieder in dieselbe Datei auf dem Clientsystem zu kopieren.
- Wenn Sie eine Datei aus dem Clientsystem in eine Anwendung auf einem Remote-Desktop ziehen, wird die Datei auf dem Remote-Desktop kopiert, und Sie können nur die Kopie der Datei bearbeiten.
- Wenn Sie eine Datei in einer 64-Bit-Windows-Maschine nicht von Horizon Client in eine lokale 64-Bit-Anwendung ziehen können, versuchen Sie, die 32-Bit-Version der lokalen Anwendung zu verwenden.
- Wenn die lokale Zielanwendung das gezogene Objekt nicht akzeptiert, ziehen Sie das Objekt in das lokale Dateisystem und ziehen Sie es dann aus dem lokalen Dateisystem in die lokale Zielanwendung.
- Für Fault Tolerance ist ein integrierter Zeitüberschreitungsmechanismus vorhanden.

Tipps für die Verwendung von veröffentlichten Anwendungen

Veröffentlichte Anwendungen ähneln Anwendungen, die auf dem lokalen Clientsystem installiert sind. Befolgen Sie diese Tipps bei der Verwendung von veröffentlichten Anwendungen.

- Sie können eine veröffentlichte Anwendung über die veröffentlichte Anwendung minimieren und maximieren. Wenn eine veröffentlichte Anwendung minimiert wird, wird sie in der Taskleiste des Clientsystems angezeigt. Sie können die veröffentlichte Anwendung auch minimieren und maximieren, indem Sie auf ihr Symbol in der Taskleiste klicken.
- Sie können eine veröffentlichte Anwendung über die veröffentlichte Anwendung oder dadurch beenden, dass Sie mit der rechten Maustaste auf ihr Symbol in der Taskleiste klicken.
- Sie können Alt+Tabulator drücken, um zwischen geöffneten veröffentlichten Anwendungen zu wechseln.

- Wenn eine veröffentlichte Anwendung ein Element in der Windows-Taskleiste erstellt, erscheint dieses Element auch in der Taskleiste des Clientsystems. Standardmäßig erscheinen die Taskleistensymbole nur, um Benachrichtigungen anzuzeigen. Sie können dieses Verhalten auf dieselbe Weise anpassen, wie Sie nativ installierte Anwendungen anpassen.

  Hinweis Wenn Sie die Systemsteuerung öffnen, um die Symbole im Infobereich anzupassen, werden die Namen der Symbole für veröffentlichte Anwendungen als VMware Horizon Client – *Name der Anwendung* – aufgeführt.

Erneute Verbindungsherstellung zu veröffentlichten Anwendungen nach dem Trennen der Verbindung

Aktive veröffentlichte Anwendungen können geöffnet bleiben, nachdem Sie die Verbindung für einen Server in Horizon Clienttrennen. Durch eine entsprechende Konfiguration können Sie festlegen, wie sich aktive veröffentlichte Anwendungen verhalten, wenn Sie erneut eine Verbindung mit dem Server in Horizon Client herstellen.

Sie können die Einstellungen für das Wiederverbindungsverhalten von veröffentlichten Anwendungen in Horizon Client von der Befehlszeile aus oder durch Konfigurieren einer Gruppenrichtlinieneinstellung deaktivieren. Die Gruppenrichtlinieneinstellung hat Vorrang gegenüber der Befehlszeileneinstellung. Weitere Informationen finden Sie unter der Option `–appSessionReconnectionBehavior` in Horizon Client-Befehlsverwendung oder unter der Gruppenrichtlinieneinstellung **Disconnected application session resumption behavior** (Wiederaufnahmeverhalten von getrennten Anwendungssitzungen) in Einstellungen für die Skriptdefinition für Client-GPOs.

Verfahren

1. Klicken Sie mit der rechten Maustaste im Fenster für die Desktop- und Anwendungsauswahl von Horizon Client auf eine veröffentlichte Anwendung und wählen Sie **Einstellungen** aus.
2. Wählen Sie im Bereich für Remoteanwendungen eine Einstellung für das Wiederverbindungsverhalten von Anwendungen aus.

Option	Beschreibung
Vor Neuverbindung zum Öffnen von veröffentlichten Anwendungen fragen	Wenn Sie erneut eine Verbindung mit dem Server herstellen, werden Sie von Horizon Client darüber informiert, dass eine oder mehrere veröffentlichte Anwendungen ausgeführt werden. Durch Klicken auf **Mit Anwendungen neu verbinden** können Sie die Fenster der veröffentlichten Anwendungen erneut öffnen. Durch Klicken auf **Nicht jetzt** werden die Fenster nicht erneut geöffnet.
Neuverbindung zum Öffnen von veröffentlichten Anwendungen automatisch herstellen	Fenster für aktive veröffentlichte Anwendungen werden automatisch wieder geöffnet, wenn Sie erneut eine Verbindung mit dem Server herstellen.
Vor Neuverbindung nicht fragen und nicht automatisch neu verbinden	Horizon Client fordert Sie nicht dazu auf, aktive veröffentlichte Anwendungen wieder zu öffnen, und Fenster von aktiven veröffentlichten Anwendungen werden nicht wieder geöffnet, wenn Sie erneut eine Verbindung mit dem Server herstellen.

3 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ergebnisse

Die Einstellung wird wirksam, wenn Horizon Client das nächste Mal eine Verbindung mit dem Server herstellt.

Verwenden mehrerer Sitzungen einer veröffentlichten Anwendung von unterschiedlichen Clientgeräten aus

Wenn der Mehrfachsitzungsmodus für eine veröffentlichte Anwendung aktiviert ist, können Sie mehrere Sitzungen derselben veröffentlichten Anwendung verwenden, wenn Sie sich auf dem Server von unterschiedlichen Clientgeräten aus anmelden.

Wenn Sie beispielsweise eine veröffentlichte Anwendung im Mehrfachsitzungsmodus auf Client A öffnen und dann dieselbe veröffentlichte Anwendung auf Client B öffnen, bleibt die veröffentlichte Anwendung auf Client A geöffnet und eine neue Sitzung der veröffentlichten Anwendung wird auf Client B geöffnet. Wenn der Mehrfachsitzungsmodus hingegen deaktiviert ist (Einzelsitzungsmodus), wird die Sitzung der veröffentlichten Anwendung auf Client A unterbrochen und auf Client B wiederhergestellt.

Für die Funktion „Mehrfachsitzungsmodus“ gelten die im Folgenden aufgeführten Einschränkungen.

- Der Mehrfachsitzungsmodus funktioniert nicht bei Anwendungen, die nicht mehrere Instanzen unterstützen, beispielsweise Skype for Business.
- Wenn die Anwendungssitzung unterbrochen wird, während Sie eine veröffentlichte Anwendung im Mehrfachsitzungsmodus verwenden, werden Sie automatisch abgemeldet, und alle nicht gespeicherten Daten gehen verloren.

Voraussetzungen

Ein Horizon Administrator muss den Mehrfachsitzungsmodus für den Anwendungspool aktivieren. Benutzer können den Mehrfachsitzungsmodus für eine veröffentlichte Anwendung nur dann ändern, wenn ein Horizon Administrator es zulässt. Siehe *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*. Diese Funktion erfordert Horizon 7 Version 7.7 oder höher.

Verfahren

1 Stellen Sie eine Verbindung mit einem Server her.

2 Öffnen Sie das Dialogfeld „Einstellungen“ und wählen Sie im linken Bereich **Mehrfachstart** aus.

   - Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Zahnradsymbol **Einstellungen**.

- Klicken Sie mit der rechten Maustaste auf einen Remote-Desktop oder eine veröffentlichte Anwendung im Fenster für die Desktop- und Anwendungsauswahl und wählen Sie **Einstellungen** aus.

Wenn keine veröffentlichten Anwendungen zur Verwendung im Mehrfachsitzungsmodus verfügbar sind, wird die Einstellung **Mehrfachstart** nicht angezeigt.

3 Wählen Sie die veröffentlichten Anwendungen aus, die Sie im Mehrfachsitzungsmodus verwenden möchten, und klicken Sie auf **OK**.

Wenn ein Horizon Administrator den Mehrfachsitzungsmodus für eine veröffentlichte Anwendung erzwungen hat, können Sie diese Einstellung nicht ändern.

Verwenden eines lokalen IMEs mit veröffentlichten Anwendungen

Wenn Sie nicht englische Tastaturen und Gebietsschemata verwenden, können Sie einen auf dem lokalen Clientsystem installierten IME (Eingabemethoden-Editor) dazu nutzen, nicht englische Zeichen an eine veröffentlichte Anwendung zu senden.

Sie können mit Abkürzungstasten und Symbolen im Infobereich (Taskleiste) des lokalen Systems zu einem anderen IME wechseln. Sie müssen keinen IME auf dem Server installieren, der die veröffentlichte Anwendung hostet.

Bei Aktivierung dieser Funktion wird der lokale IME verwendet. Sofern auf dem Server, der die veröffentlichte Anwendung hostet, ein IME installiert und konfiguriert ist, wird dieser Remote-IME ignoriert.

Diese Funktion ist standardmäßig deaktiviert. Wenn Sie diese Funktion aktivieren oder deaktivieren, müssen Sie die Verbindung mit dem Server trennen und sich erneut anmelden. Erst dann wird die Änderung wirksam.

Voraussetzungen

- Stellen Sie sicher, dass einer oder mehrere IMEs auf dem Clientsystem installiert sind.
- Vergewissern Sie sich, dass die Eingabesprache auf dem lokalen Clientsystem der in vom IME verwendeten Sprache entspricht.

Verfahren

1 Klicken Sie mit der rechten Maustaste im Fenster für die Desktop- und Anwendungsauswahl von Horizon Client auf eine veröffentlichte Anwendung und wählen Sie **Einstellungen** aus.

2 Aktivieren Sie im Bereich „Remoteanwendungen“ das Kontrollkästchen **Lokalen IME in gehosteten Anwendungen erweitern** und klicken Sie auf **OK**.

3 Starten Sie die Sitzung neu.

Option	Aktion
Vom Server abmelden	Trennen Sie die Verbindung mit dem Server, melden Sie sich erneut an und stellen Sie wieder eine Verbindung mit der veröffentlichten Anwendung her. Sie können die Arbeit mit den veröffentlichten Anwendungen fortsetzen, die getrennt, doch nicht geschlossen waren. Sie können auch die Arbeit mit allen Remote Desktops fortsetzen.
Anwendungen zurücksetzen	Klicken Sie mit der rechten Maustaste auf das Symbol einer veröffentlichten Anwendung, wählen Sie **Einstellungen** aus und klicken Sie auf **Zurücksetzen**. Wenn Sie diese Option verwenden, werden alle geöffneten Remote Desktops nicht getrennt, aber alle veröffentlichten Anwendungen werden geschlossen und müssen neu gestartet werden.

Die Einstellung wird erst nach dem Neustart der Sitzung wirksam. Sie gilt für alle veröffentlichten Anwendungen auf dem Server.

4 Verwenden Sie den lokalen IME wie bei lokal installierten Anwendungen.

Ergebnisse

Die Sprachbezeichnung und ein Symbol für den IME werden im Infobereich (bzw. in der Taskleiste) des lokalen Clientsystems angezeigt. Sie können Abkürzungstasten verwenden, um zu einer anderen Sprache oder einem anderen IME zu wechseln. Tastenkombinationen zur Durchführung bestimmter Aktionen, wie z. B. Strg+X für das Ausschneiden von Text sowie Alt +Rechtspfeil für das Verschieben zu einer anderen Registerkarte, funktionieren ordnungsgemäß.

Hinweis Auf Windows 7- und Windows 8.x-Systemen können Sie Abkürzungstasten für IMEs im Dialogfeld **Textdienste und Eingabesprachen** festlegen. (Das Dialogfeld ist über **Systemsteuerung > Region und Sprache > Registerkarte „Tastaturen und Sprachen“ > Schaltfläche „Tastaturen ändern“ > Textdienste und Eingabesprachen > Registerkarte „Erweiterte Tastatureinstellungen“** erreichbar.)

Drucken auf einem Remote-Desktop oder in einer veröffentlichten Anwendung

Mit der Funktion „VMware Integrated Printing“ können Sie von einem Remote-Desktop oder einer veröffentlichten Anwendung aus auf einem Netzwerkdrucker oder einem lokal angeschlossenen Drucker drucken.

Informationen zum Installieren der VMware Integrated Printing-Funktion finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.

Informationen zum Konfigurieren der VMware Integrated Printing-Funktion finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Informationen zu den Typen von Remote-Desktops, die die VMware Integrated Printing-Funktion unterstützen, finden Sie unter Funktionsunterstützung für Windows-Clients.

Festlegen von Druckeinstellungen für die Funktion „VMware Integrated Printing“

Sie können auf einem Remote-Desktop für die Funktion „VMware Integrated Printing“ Druckeinstellungen festlegen. Mit der Funktion „VMware Integrated Printing“ können Sie lokale oder Netzwerkdrucker von einem Remote-Desktop verwenden, ohne auf dem Windows-Remote-Desktop zusätzliche Druckertreiber installieren zu müssen. Für jeden Drucker, der über diese Funktion zur Verfügung steht, können Sie Voreinstellungen für Datenkomprimierung, Druckqualität, doppelseitigen Druck, Farbe und andere Einstellungen festlegen.

Auf dem Einzelbenutzer-Desktop einer virtuellen Maschine wird jeder virtuelle Drucker standardmäßig als *<printer_name>*(*vdi*) angezeigt. In einem veröffentlichten Desktop oder einer veröffentlichten Anwendung wird jeder virtuelle Drucker standardmäßig als *<printer_name>*(v*<session_ID>*) angezeigt.

Beginnend mit Horizon Agent 7.12 können Sie die Gruppenrichtlinie verwenden, um die Druckernamenskonvention für Clientdrucker zu ändern, die umgeleitet werden. Informationen hierzu finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon* für Ihre Horizon Agent-Version.

Voraussetzungen

Zur Anwendung der Funktion „VMware Integrated Printing“ muss ein Horizon-Administrator diese auf dem Remote-Desktop installieren. Diese Aufgabe beinhaltet die Aktivierung der Option **VMware Integrated Printing** im Horizon Agent-Installationsprogramm. Informationen zum Installieren von Horizon Agent finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*. Informationen zum Konfigurieren der VMware Integrated Printing-Funktion finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Um zu bestimmen, ob die Funktion „VMware Integrated Printing“ auf einem Remote-Desktop installiert ist, stellen Sie sicher, dass die Dateien `C:\Programme\Common Files\VMware\Remote Experience\x64\vmware-print-redir-server.exe` und `C:\Programme\Common Files\VMware\Remote Experience\x64\vmware-print-redir-service.exe` im Remote-Desktop-Dateisystem vorhanden sind.

Diese Funktion erfordert Horizon Agent 7.7 oder höher.

Verfahren

1. Navigieren Sie auf dem Windows-Remote-Desktop zu **Systemsteuerung > Hardware und Sound > Geräte und Drucker**.
2. Klicken Sie im Fenster **Geräte und Drucker** mit der rechten Maustaste auf den virtuellen Drucker und wählen Sie aus dem Kontextmenü **Druckereigenschaften** aus.
3. Klicken Sie auf der Registerkarte **Allgemein** auf **Einstellungen**.
4. Klicken Sie im Dialogfeld mit den Druckeinstellungen auf die verschiedenen Registerkarten und geben Sie an, welche Einstellungen verwendet werden sollen.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Drucken von einem Remote-Desktop auf einem lokalen USB-Drucker

Ein USB-Drucker ist ein Drucker, der an einen USB-Port auf dem lokalen Clientsystem angeschlossen ist. Sie können Druckaufträge an einen USB-Drucker, der an das lokale Clientsystem angeschlossen ist, von einem Remote-Desktop aus senden.

Sie können die Funktion für die USB-Umleitung oder „VMware Integrated Printing“ nutzen, um von einem Remote-Desktop auf einem USB-Drucker zu drucken. Umgeleitete USB-Drucker und virtuelle Drucker können ohne Konflikt zusammenarbeiten.

Verwenden der Funktion zur USB-Umleitung

Um die Funktion zur USB-Umleitung zu nutzen, um einen USB-Drucker an einen virtuellen USB-Port auf einem Remote-Desktop anzuschließen, müssen die erforderlichen Druckertreiber sowohl auf dem Remote-Desktop als auch auf dem Clientsystem installiert sein.

Wenn Sie die USB-Umleitungsfunktion verwenden, um einen USB-Drucker umzuleiten, ist der USB-Drucker nicht länger logisch an den physischen USB-Anschluss am lokalen Clientsystem angeschlossen und wird auf dem lokalen Clientsystem nicht in der Liste der lokalen Drucker angezeigt. Sie können vom Remote-Desktop auf dem USB-Drucker drucken. Sie können aber nicht mehr vom lokalen Clientcomputer auf dem USB-Drucker drucken.

Auf einem Remote-Desktop werden umgeleitete USB-Drucker als *<drucker_name>* angezeigt.

Weitere Informationen finden Sie unter Verwenden von USB-Geräten.

Verwenden der VMware Integrated Printing-Funktion

Wenn Sie die Funktion „VMware Integrated Printing“ nutzen, um Druckaufträge an einen USB-Drucker zu senden, können Sie sowohl vom Remote Desktop als auch vom lokalen Clientsystem auf dem USB-Drucker drucken und müssen im Remote Desktop keine Druckertreiber installieren.

Um die Funktion „VMware Integrated Printing“ verwenden zu können, muss die Funktion bei der Installation von Horizon Agent aktiviert sein. Weitere Informationen finden Sie in den Dokumenten *Einrichten von virtuellen Desktops in Horizon* und *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.

Weitere Informationen finden Sie unter Festlegen von Druckeinstellungen für die Funktion „VMware Integrated Printing“.

Verwenden der Funktion der URL-Inhaltsumleitung

Ein Horizon Administrator kann URL-Links so konfigurieren, dass diese durch Klicken in einem Remote Desktop oder in einer veröffentlichten Anwendung im Standard-Browser auf dem lokalen Clientsystem geöffnet werden. Der URL-Link kann zu einer Webseite, einer Telefonnummer, einer E-Mail-Adresse oder zu einer anderen Art von Link führen. Diese Funktion wird als URL-Inhaltsumleitung bezeichnet.

Ein Horizon Administrator kann außerdem URL-Links konfigurieren, die in einem Remote Desktop oder einer veröffentlichten Anwendung geöffnet werden, wenn Sie auf dem lokalen Clientsystem in einem Browser oder einer Anwendung darauf klicken. Wenn Horizon Client noch nicht geöffnet ist und Sie auf den URL-Link klicken, wird das Programm gestartet und Sie werden aufgefordert, sich anzumelden.

Ein Horizon-Administrator kann die URL-Inhaltsumleitung aus Sicherheitsgründen einrichten. Wenn Sie z. B. bei der Arbeit sind und auf einen Link klicken, der auf eine URL verweist, die sich außerhalb des Unternehmensnetzwerks befindet, ist es möglicherweise sicherer, wenn der Link in einer veröffentlichten Anwendung geöffnet wird. Ein Administrator kann konfigurieren, welche veröffentlichte Anwendung den Link öffnet.

Verwenden der URL-Inhaltsumleitung mit Chrome

Bei der ersten Umleitung einer URL aus dem Chrome-Browser des Clients werden Sie aufgefordert, die URL in Horizon Client zu öffnen. Wenn Sie das Kontrollkästchen **Auswahl für URL:VMware Horizon Client-Protokoll-Links speichern** (empfohlen) aktivieren und anschließend auf **VMware Horizon Client öffnen** klicken, wird diese Aufforderung nicht mehr angezeigt.

Verbessern der Mausleistung in einem Remote-Desktop

Wenn Sie das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll bei 3D-Anwendungen in einem Remote-Desktop verwenden, können Sie die Mausleistung durch Aktivierung der Funktion für die relative Mausbewegung verbessern.

In den meisten Fällen überträgt Horizon Client bei Verwendung von Anwendungen, die kein 3D-Rendering erfordern, Informationen über Mauszeigerbewegungen mithilfe von absoluten Koordinaten. Bei der Verwendung von absoluten Koordinaten rendert der Client die Mausbewegungen lokal, wodurch die Leistung insbesondere dann verbessert wird, wenn Sie sich außerhalb des Firmennetzwerks befinden.

Bei der Arbeit mit grafikintensiven Anwendungen wie AutoCAD oder bei 3D-Videospielen können Sie die Mausleistung verbessern, indem Sie die Funktion für die relative Mausbewegung aktivieren. Diese Funktion verwendet relative statt absoluter Koordinaten.

Wenn die Funktion der relativen Mausbewegung aktiviert ist, kann die Performance langsam sein, wenn Sie sich außerhalb des Firmennetzwerks in einem WAN befinden.

Voraussetzungen

Ein Horizon-Administrator muss die 3D-Wiedergabe für den Desktop-Pool aktivieren. Informationen zu den Pooleinstellungen und zu den Optionen für ein 3D-Rendering finden Sie in den Dokumenten *Einrichten von virtuellen Desktops in Horizon* und *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.

Verfahren

1 Starten Sie Horizon Client und melden Sie sich beim Server an.

2 Klicken Sie mit der rechten Maustaste auf den Remote-Desktop und wählen Sie **VMware Blast** oder **PCoIP** aus.

3 Stellen Sie eine Verbindung mit dem Remote-Desktop her.

4 Wählen Sie **Optionen > Relative Maus aktivieren** in der Horizon Client-Menüleiste aus.

   Die Option ist eine Umschaltoption. Um die relative Mausbewegung zu deaktivieren, wählen Sie erneut **Optionen > Relative Maus aktivieren** aus.

   Hinweis Wenn Sie Horizon Client im Fenstermodus und nicht im Vollbildmodus verwenden und die Funktion der relativen Mausbewegung aktiviert ist, können Sie möglicherweise den Mauszeiger nicht auf die Horizon Client-Menüoptionen oder aus dem Horizon Client-Fenster hinaus bewegen. Um diese Situation zu beheben, drücken Sie Strg+Alt.

Verwenden von Scannern

Mit der Funktion der Scannerumleitung können Sie unter Verwendung von Scannern, die mit dem lokalen Clientsystem verbunden sind, Informationen in Remote-Desktops und veröffentlichte Anwendungen einscannen. Diese Funktion leitet Scandaten mit deutlich weniger Bandbreite um, als mit der USB-Umleitung erreicht werden kann.

Scannerumleitung unterstützt Standard-Scangeräte, die zu den TWAIN- und WIA (Windows Image Acquisition)-Formaten kompatibel sind. Sie müssen die Scanner-Gerätetreiber auf dem lokalen Clientsystem installiert haben. Sie müssen die Scanner-Gerätetreiber nicht auf einem Remote-Desktop installieren.

Sofern ein Horizon-Administrator die Scannerumleitungsfunktion konfiguriert hat und Sie das PCoIP-Anzeigeprotokoll oder das VMware Blast-Anzeigeprotokoll verwenden, kann ein mit Ihrem lokalen Clientsystem verbundener Scanner auf einem Remote-Desktop oder in einer veröffentlichten Anwendung genutzt werden.

Wichtig Verbinden Sie keinen Scanner aus dem Menü **USB-Gerät verbinden** in Horizon Client. Die Leistung ist dann nicht mehr ausreichend.

Wenn Scandaten zu einem Remote-Desktop oder einer veröffentlichten Anwendung umgeleitet werden, können Sie auf dem lokalen Clientcomputer nicht auf den Scanner zugreifen. Umgekehrt können Sie über den Remote-Desktop oder die veröffentlichte Anwendung nicht auf den Scanner zugreifen, wenn dieser gerade vom lokalen Clientcomputer genutzt wird.

Ein Horizon-Administrator kann Gruppenrichtlinieneinstellungen konfigurieren, um die im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ verfügbaren Optionen zu steuern. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Hinweis Wenn ein Horizon-Administrator die Scannerumleitung für die Verwendung eines bestimmten Scanners konfiguriert und dieser Scanner nicht verfügbar ist, funktioniert die Scannerumleitung nicht.

Tipps zur Verwendung der Scannerumleitungsfunktion

- Um die Einstellungen für die Scannerumleitung zu ändern, klicken Sie auf das Scannersymbol () in der Taskleiste oder im Infobereich des Remote-Desktops. In einer veröffentlichten Anwendung wird das Taskleistensymbol zum lokalen Clientcomputer umgeleitet.

  Hinweis Es besteht keine Notwendigkeit, das Menü zu verwenden, das angezeigt wird, wenn Sie auf das Scannersymbol klicken. Die Scannerumleitung funktioniert ohne weitere Konfiguration. Wenn das Menü keine Scanner auflistet, ist ein nicht kompatibler Scanner mit dem lokalen Clientsystem verbunden. Wenn das Scannersymbol nicht angezeigt wird, ist die Scannerumleitungsfunktion entweder deaktiviert oder nicht auf dem Remote-Desktop installiert. Das Scannersymbol wird auch nicht auf den lokalen Clientsystemen angezeigt, die diese Funktion nicht unterstützen.

- Wenn das Dialogfeld „TWAIN-Scanner-Eigenschaften" angezeigt werden soll, auch wenn eine Scananwendung das Dialogfeld „Scannen“ nicht anzeigt, klicken Sie im Menü des Scannersymbols auf die Option **Einstellungen** und aktivieren Sie das Kontrollkästchen **Dialogfeld „TWAIN-Scanner-Eigenschaften“ erzwingen**.
- Um die tatsächlichen Scanner-Namen anstelle von „Virtueller VMware-*nnn*-Scanner“ anzuzeigen, klicken Sie im Menü des Scannersymbols auf die Option **Einstellungen** und aktivieren Sie das Kontrollkästchen **Anbieterdefinierte Namen für TWAIN-Scanner verwenden**.
- Um Optionen zur Steuerung der Bildkomprimierung auszuwählen oder festzulegen, wie der Standard-Scanner ausgewählt werden soll, klicken Sie im Menü des Scannersymbols auf die Option **Einstellungen** und wählen Sie die Registerkarte **Komprimierung** oder **Standard** aus.
- Wenn Sie beabsichtigen, die Funktion „Echtzeit-Audio/Video“ für die Umleitung von Webcams wie von VMware empfohlen zu verwenden, klicken Sie im Menü des Scannersymbols auf die Option **Einstellungen** und aktivieren Sie das Kontrollkästchen **Bildverarbeitungsgeräte vom Typ Webcam ausblenden**.
- Die meisten TWAIN-Scanner zeigen standardmäßig ein Dialogfeld mit Scannereinstellungen an. Dies gilt jedoch nicht für alle von ihnen. Für die Scanner, die keine Einstellungsoptionen anzeigen, können Sie die Option **Einstellungen** im Menü des Scannersymbols verwenden und die Option **Dialogfeld „TWAIN-Scanner-Eigenschaften“ erzwingen** auswählen.
- Um das Dialogfeld „TWAIN-Scanner-Eigenschaften“ auf dem Remote-Desktop anzuzeigen, klicken Sie im Menü des Scannersymbols auf die Option **Einstellungen** und aktivieren Sie das

Kontrollkästchen **Agent (Dialogfeld „VMware-Scanner-Eigenschaften“)**. Um das Dialogfeld „TWAIN-Scanner-Eigenschaften“ auf dem lokalen Clientsystem anzuzeigen, aktivieren Sie das Kontrollkästchen **Client (Dialogfeld „Systemeigene Scanner-Eigenschaften“, falls unterstützt)**.

Hinweis Im Dialogfeld „TWAIN-Scanner-Eigenschaften“ des Agenten sind möglicherweise einige weniger häufig verwendete Optionen nicht enthalten. Um diese weniger allgemeinen Optionen zu verwenden, aktivieren Sie das Kontrollkästchen **Client (Dialogfeld „Systemeigene Scanner-Eigenschaften“, falls unterstützt)**.

- Wenn ein zu scannendes Bild zu groß ist oder mit zu hoher Auflösung gescannt wird, funktioniert das Scannen möglicherweise nicht. In diesem Fall kann es vorkommen, dass die Fortschrittsanzeige für den Scanvorgang einzufrieren scheint oder die Scanneranwendung unerwartet schließt. Wenn Sie den Remote-Desktop minimieren, wird möglicherweise eine Fehlermeldung auf dem lokalen Clientsystem angezeigt, die darauf hinweist, dass die Auflösung zu hoch eingestellt ist. Zur Behebung dieses Problems verringern Sie die Auflösung oder beschränken den zu scannenden Bereich auf einen Bildausschnitt und wiederholen den Scanvorgang.

Umleiten serieller Ports

Mithilfe der Funktion zum Umleitung serieller Ports können Sie lokal verbundene serielle Ports (COM-Ports) wie integrierte RS232-Ports und USB-Seriell-Adapter umleiten. Geräte wie Drucker, Barcodeleser und andere serielle Geräte können mit diesen Ports verbunden und in Remote-Desktops verwendet werden.

Wenn ein Horizon-Administrator die Funktion zur Umleitung serieller Ports konfiguriert hat und Sie das VMware Blast- oder PCoIP-Anzeigeprotokoll verwenden, kann die Umleitung serieller Ports ohne weitere Konfiguration auf dem Remote-Desktop angewendet werden. Beispielsweise lässt sich ein COM1-Port auf dem lokalen Clientsystem als COM1-Port auf den Remote-Desktop umleiten. COM2 wird dabei als COM2 umgeleitet. Wird der COM-Port bereits verwendet, wird er zugeordnet, um Konflikte zu vermeiden. Wenn beispielsweise der COM1- und der COM2-Port bereits auf dem Remote-Desktop vorhanden sind, wird der COM1-Port auf dem Clientsystem standardmäßig dem COM3-Port zugeordnet.

Sie müssen alle erforderlichen Gerätetreiber auf dem lokalen Clientsystem installiert haben, aber Sie müssen diese nicht auf dem Remote-Desktop installieren. Wenn Sie beispielsweise einen USB-Seriell-Adapter verwenden, der für Ihr lokales Clientsystem bestimmte Gerätetreiber benötigt, müssen Sie diese Gerätetreiber nur auf dem Clientsystem installieren.

Wichtig Wenn Sie ein Gerät in einem USB-Seriell-Adapter verwenden, verbinden Sie dieses nicht über das Menü **USB-Gerät verbinden** in Horizon Client. Dies würde dazu führen, dass das Gerät über die USB-Umleitung umgeleitet und die Umleitung serieller Ports umgangen wird.

Tipps zur Verwendung der Umleitung serieller Ports

- Um die zugeordneten COM-Ports zu verbinden, deren Verbindung zu trennen oder anzupassen, klicken Sie auf das Symbol des seriellen Ports des Remote-Desktops (📹) in der Taskleiste oder im Infobereich des Remote-Desktops.

  Wenn Sie auf das Symbol des seriellen Ports klicken, erscheint das Kontextmenü **Umleitung serieller COM-Ports für VMware Horizon**. Wenn ein Administrator die Konfiguration gesperrt hat, werden die Elemente im Kontextmenü abgeblendet dargestellt. Das Symbol erscheint nur, wenn ein Horizon Administrator die Funktion zur Umleitung serieller Ports konfiguriert hat und alle Anforderungen erfüllt sind. Weitere Informationen finden Sie unter Systemanforderungen für die Umleitung serieller Ports.

- Im Kontextmenü werden die Portelemente als ***Port* zugeordnet zu *Port*** aufgelistet, z. B. **COM1 zugeordnet zu COM3**. Der erste Port (in diesem Beispiel COM1) ist der physische Port oder der USB-Seriell-Adapter auf dem lokalen Clientsystem. Der zweite Port (in diesem Beispiel COM3) ist der Port, der auf dem Remote-Desktop verwendet wird.

- Um den Befehl **Porteigenschaften** auszuwählen, klicken Sie mit der rechten Maustaste auf einen COM-Port.

  Im Dialogfeld „Porteigenschaften“ können Sie einen Port für die automatische Herstellung einer Verbindung beim Beginn einer Remote-Desktop-Sitzung konfigurieren. Außerdem können Sie festlegen, dass das DSR-Signal (Data Set Ready) ignoriert wird, das für einige Modems oder andere Geräte erforderlich ist.

  Sie können auch die Portnummer ändern, die der Remote-Desktop verwendet. Wenn z. B. der COM1-Port auf dem Clientsystem dem COM3-Port auf dem Remote-Desktop zugeordnet ist, die verwendete Anwendung aber COM1 benötigt, können Sie die Portnummer in COM1 ändern. Wenn COM1 auf dem Remote-Desktop vorhanden ist, wird möglicherweise **COM1 (Überlappend)** angezeigt. Dieser überlappende Port lässt sich weiterhin verwenden. Der Remote-Desktop kann serielle Daten vom Server oder vom Clientsystem über den Port empfangen.

- Stellen Sie eine Verbindung zu einem zugeordneten COM-Port her, bevor Sie eine Anwendung starten, die Zugriff auf diesen Port erfordert. Klicken Sie z. B. mit der rechten Maustaste auf einen COM-Port und wählen Sie im eingeblendeten Kontextmenü die Option **Verbinden**, um den Port auf dem Remote-Desktop zu verwenden. Beim Start der Anwendung wird der serielle Port geöffnet.

  Wenn ein umgeleiteter COM-Port auf einem Remote-Desktop geöffnet und verwendet wird, können Sie auf diesen Port auf dem lokalen Computer nicht zugreifen. Umgekehrt können Sie auf den COM-Port auf dem Remote-Desktop nicht zugreifen, wenn dieser Port auf dem lokalen Computer verwendet wird.

- Auf dem Remote-Desktop haben Sie die Möglichkeit, mithilfe der Registerkarte **Porteinstellungen** im Windows-Geräte-Manager die Standard-Baudrate für einen bestimmten COM-Port festzulegen. Verwenden Sie die gleichen Einstellungen im Windows-Gerätemanager auf dem Clientsystem. Die Einstellungen auf dieser Registerkarte werden nur verwendet, wenn die Anwendung keine Porteinstellungen angibt.
- Bevor Sie die Verbindung mit dem COM-Port trennen können, muss der Port in der Anwendung oder die Anwendung selbst geschlossen werden. Sie können dann mit der Option **Verbindung trennen** die Verbindung trennen und den physischen COM-Port für die Verwendung auf dem Clientcomputer zur Verfügung stellen.
- Wenn Sie einen seriellen Port für eine automatische Verbindung konfigurieren, eine Anwendung starten, die den seriellen Port öffnet, und dann die Remote-Desktop-Sitzung trennen und erneut verbinden, ist die Funktion zur automatischen Verbindung nicht wirksam. Sie können dann auch mit dem Taskleistensymbol des seriellen Ports keine Verbindung herstellen. In den meisten Fällen kann die Anwendung den seriellen Port nicht mehr verwenden. Sie müssen die Anwendung beenden, die Remote-Desktop-Sitzung trennen und sie dann wiederherstellen, um das Problem zu beheben.

Tastenkombinationen

Sie können Tastenkombinationen für Menübefehle und häufig auszuführende Aktionen verwenden.

Häufig verwendete Tastenkombinationen

Diese Tastenkombinationen funktionieren in Horizon Client wie in allen Anwendungen.

Tabelle 5-1. Häufig verwendete Tastenkombinationen

Aktion	Taste oder Tastenkombination
Klicken auf die markierte Schaltfläche in einem Dialogfeld	Drücken Enter.
Öffnen des Kontextmenüs	Drücken Sie Umschalt+F10.
Klicken auf die Schaltfläche **Abbrechen** in einem Dialogfeld.	Drücken Sie die Esc-Taste.
Navigieren zwischen Elementen im Serverauswahlfenster oder im Fenster für die Desktop- und Anwendungsauswahl	Verwenden Sie eine Pfeiltaste für die Bewegung in Richtung des Pfeils. Für die Bewegung nach rechts drücken Sie die Tabulatortaste. Für die Bewegung nach links drücken Sie Umschalt+Tabulatortaste.
Löschen eines Elements im Serverauswahlfenster oder im Fenster für die Desktop- und Anwendungsauswahl	Drücken Sie die „Entf“-Taste.
Navigieren zwischen dem **Start**- und dem Remote-Desktop-Fenster in Windows 8.x	Drücken Sie die Windows-Taste.

Tastenkombinationen für das Serverauswahlfenster

Diese Tastenkombinationen können Sie im Serverauswahlfenster von Horizon Client verwenden.

Tabelle 5-2. Tastenkombinationen für die Serverauswahl

Menübefehl oder Aktion	Tastenkombination
Öffnen der Onlinehilfe in einem Browserfenster	Alt+O+H, Strg+H
Befehl **Neuer Server**	Alt+N
Öffnen des Fensters **Supportinformationen**	Alt+O+S
Öffnen des Fenster **Info über Horizon Client**	Alt+O+V
Befehl **SSL konfigurieren**	Alt+O+O
Befehl **Selektor nach Start eines Elements ausblenden**	Alt+O+A

Tastenkombinationen für die Desktop- und Anwendungsauswahl

Diese Tastenkombinationen können für die Auswahl von Remote-Desktops und veröffentlichten Anwendungen in Horizon Client verwendet werden.

Tabelle 5-3. Tastenkombinationen für die Desktop- und Anwendungsauswahl

Menübefehl oder Aktion	Tastenkombination
Öffnen der Onlinehilfe in einem Browserfenster	Alt+O+H, Strg+H
Öffnen des Menüs **Optionen**	Alt+O
Öffnen des Fensters **Supportinformationen**	Alt+O+S
Öffnen des Fenster **Info über Horizon Client**	Alt+O+V
Abmelden vom Remote-Desktop	Shift+F10+B
Trennen der Verbindung zum Server und Abmelden vom Server	Alt+D
Wechseln zwischen **Favoriten anzeigen** und **Alle anzeigen**	Alt+F
Beim Anzeigen von Favoriten: Wechseln zum nächsten Element im Suchergebnis, nachdem die ersten Zeichen des Namens der veröffentlichten Anwendung oder des Remote-Desktops eingegeben wurden	F4
Beim Anzeigen von Favoriten: Wechseln zum vorherigen Element im Suchergebnis	Shift+F4
Markieren als Favorit oder Entfernen der Kennzeichnung als Favorit	Shift+F10+F
Öffnen des Menüs **Einstellungen**	Alt+S oder Shift+F10+E
Starten des ausgewählten Elements	Enter oder Shift+F10+S
Anheften einer Verknüpfung für den Remote-Desktop oder eine veröffentlichte Anwendung an das Start-Menü (für Windows 7 und früher) oder das Start-Fenster (für Windows 8.x und höher) auf dem Clientsystem	Shift+F10+Z
Öffnen des Kontextmenüs **Anzeigeeinstellungen** für den ausgewählten Remote-Desktop	Shift+F10+A
Verwenden des PCoIP-Anzeigeprotokolls zum Herstellen einer Verbindung mit dem ausgewählten Remote-Desktop	Shift+F10+P

Tabelle 5-3. Tastenkombinationen für die Desktop- und Anwendungsauswahl (Fortsetzung)

Menübefehl oder Aktion	Tastenkombination
Verwenden des RDP-Anzeigeprotokolls zum Herstellen einer Verbindung mit dem ausgewählten Remote-Desktop	Shift+F10+M
Erstellen einer Remote-Desktop-Verknüpfung für das ausgewählte Element	Shift+F10+V
Hinzufügen des ausgewählten Elements zum Startmenü oder Startfenster	Shift+F10+Z
Zurücksetzen des ausgewählten Remote-Desktops (falls der Administrator das Zurücksetzen erlaubt)	Shift+F10+D
Aktualisieren der Liste mit Remote-Desktops und veröffentlichten Anwendungen	F5

Tastenkombinationen für das Desktop-Fenster

Für die Verwendung dieser Tastenkombinationen müssen Sie Strg+Alt drücken oder auf die Horizon Client-Menüleiste klicken, anstatt innerhalb des Remote-Desktops zu klicken, bevor Sie die Tasten verwenden. Diese Tastenkombinationen funktionieren nur mit dem VMware Blast-Anzeigeprotokoll oder mit dem PCoIP-Anzeigeprotokoll.

Tabelle 5-4. Tastenkombinationen für das Remote-Desktop-Fenster

Menübefehl oder Aktion	Tastenkombination
Freigeben des Mauszeigers, sodass er sich nicht mehr im Remote-Desktop befindet	Strg+Alt
Öffnen des Menüs **Optionen**	Alt+O
Öffnen des Fensters **Supportinformationen**	Alt+O+S
Öffnen des Fenster **Info über Horizon Client**	Alt+O+V
Öffnen des Dialogfelds „Einstellungen der Ordnerfreigabe“	Alt+O+F
Umschalten von **Anzeigeskalierung aktivieren**	Alt+O+N
Befehl **Zu einem anderen Desktop wechseln**	Alt+O+S
Befehl **Verbindung mit diesem Desktop automatisch herstellen**	Alt+O+B
Befehl **Relative Maus aktivieren**	Alt+O+R
Befehl **Strg+Alt+Entf senden**	Alt+O+C
Befehl **Trennen**	Alt+O+E
Befehl **Trennen und abmelden**	Alt+O+A
Befehl **USB-Gerät verbinden**	Alt+V

Tastenkombinationen für Eingabefokus

Sie können die Gruppenrichtlinieneinstellungen **Tastenkombination zum Erfassen des Eingabefokus** und **Tastenkombination zum Freigeben des Eingabefokus** verwenden, um Tastenkombinationen für den Eingabefokus zu konfigurieren. Sie können die Gruppenrichtlinieneinstellung **Automatischer Eingabefokus in einem virtuellen Desktopfenster** verwenden, um automatisch Eingaben an den Remote-Desktop zu senden, wenn ein Benutzer den Remote-Desktop in den Vordergrund bringt. Diese Funktionen sind nützlich für Benutzer, die keine Mausklicks verwenden können, um einen Remote-Desktop zu erfassen und freizugeben. Weitere Informationen finden Sie unter Allgemeine Einstellungen für Client-GPOs

Synchronisierung der als Eingabequelle für die Tastatur festgelegten Sprache

Wenn Sie eine Verbindung mit einem Remote-Desktop herstellen, wird die auf dem Clientsystem als Eingabequelle für die Tastatur festgelegte Sprache auf dem Remote-Desktop synchronisiert.

Diese Funktion unterstützt die nachfolgenden auf dem Clientsystem als Eingabequelle für die Tastatur festgelegten Sprachen.

- Japanisch
- Englisch
- Chinesisch
- Koreanisch
- Französisch
- Deutsch
- Spanisch

Es wird nicht synchronisiert, wenn die als Eingabequelle für die Tastatur festgelegte Sprache nicht unterstützt wird.

Die Synchronisierung der Quellsprache der Tastatureingabe wird von der Agenten-seitigen Gruppenrichtlinieneinstellung **Synchronisierung des Tastaturgebietsschemas** gesteuert. Weitere Informationen finden Sie unter „VMware Blast – Gruppenrichtlinieneinstellungen“ im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon*.

Konfigurieren der Synchronisierung von Sperrtasten

Sie können Horizon Client so konfigurieren, dass der Umschaltstatus der Tasten Num, Rollen und Feststellen vom Clientsystem auf einen Remote-Desktop synchronisiert wird, indem Sie eine Einstellung in Horizon Client aktivieren. Diese Einstellung ist standardmäßig deaktiviert.

Sie können auch die Horizon Client-Gruppenrichtlinieneinstellung **Tastatur, Scroll- und Feststelltaste automatisch synchronisieren** verwenden, um die Synchronisierung der Sperrtasten zu konfigurieren. Wenn diese Gruppenrichtlinieneinstellung aktiviert oder deaktiviert ist, können Benutzer die Einstellung für die Synchronisierung der Sperrtasten auf der Horizon Client-Benutzeroberfläche nicht ändern. Weitere Informationen finden Sie unter Allgemeine Einstellungen für Client-GPOs.

Wenn die Gruppenrichtlinieneinstellung **Tastatur, Scroll- und Feststelltaste automatisch synchronisieren** entweder deaktiviert oder nicht konfiguriert ist oder wenn die Einstellung für die Synchronisierung für Horizon Client-Sperrtasten nicht aktiviert ist (Standardeinstellung), wird der Umschaltzustand der Sperrtasten standardmäßig vom Remote-Desktop zum Clientsystem synchronisiert.

Verfahren

1. Starten Sie Horizon Client und stellen Sie eine Verbindung mit einem Server her.
2. Öffnen Sie das Dialogfeld „Einstellungen“ für den Remote-Desktop.
   - Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Symbol für **Einstellungen** (Zahnrad) und wählen Sie im linken Bereich den Remote-Desktop aus.
   - Klicken Sie im Fenster für die Desktop- und Anwendungsauswahl mit der rechten Maustaste auf den Remote-Desktop und wählen Sie **Einstellungen** aus.
3. Um die Funktion zur Synchronisierung von Sperrtasten zu aktivieren, aktivieren Sie das Kontrollkästchen **Tastatur, Scroll- und Feststelltaste automatisch synchronisieren** und klicken Sie auf **OK**.

Fehlerbehebung für Horizon Client 6

Sie können die meisten Probleme mit Horizon Client beheben, indem Sie Remote Desktops oder veröffentlichte Anwendungen neu starten oder zurücksetzen oder Horizon Client neu installieren.

Dieses Kapitel enthält die folgenden Themen:

Neustarten eines Remote-Desktops

Wenn das Remote Desktop-Betriebssystem nicht mehr reagiert, kann es erforderlich sein, einen Remote Desktop neu zu starten. Der Neustart eines Remote Desktops entspricht dem Neustart des Windows-Betriebssystems. In der Regel werden Sie dabei vom Remote-Desktop-Betriebssystem aufgefordert, alle nicht gespeicherten Daten zu speichern, bevor der Neustart erfolgt.

Sie können einen Remote Desktop nur dann neu starten, wenn ein Horizon Administrator die Funktion zum Neustart des Remote Desktops aktiviert hat.

Informationen zur Aktivierung der Funktion zum Neustart eines Desktops finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.

Verfahren

- Verwenden Sie die Option **Desktop neu starten**.

Option	Aktion
Von innerhalb des Remote-Desktops	Wählen Sie **Optionen > Desktop neu starten** aus der Menüleiste aus.
Im Desktop-Auswahlfenster	Klicken Sie mit der rechten Maustaste auf das Symbol des Remote Desktops und wählen Sie **Desktop neu starten** aus.

  Horizon Client fordert Sie zur Bestätigung des Neustarts auf.

Ergebnisse

Das Betriebssystem im Remote Desktop wird neu gestartet, der Client wird getrennt und vom Remote Desktop abgemeldet.

Nächste Schritte

Warten Sie eine Weile, bis das System neu gestartet wurde, und versuchen Sie anschließend, erneut eine Verbindung zum Remote Desktop herzustellen.

Wenn das Problem durch den Neustart des Remote-Desktops nicht behoben werden kann, müssen Sie den Remote-Desktop eventuell zurücksetzen. Siehe Zurücksetzen von Remote-Desktops oder veröffentlichten Anwendungen.

Zurücksetzen von Remote-Desktops oder veröffentlichten Anwendungen

Sie müssen einen Remote-Desktop eventuell zurücksetzen, wenn das Betriebssystem nicht mehr reagiert und der Neustart des Remote-Desktops das Problem nicht löst.

Das Zurücksetzen eines Remote Desktops entspricht dem Betätigen der Reset-Taste auf einem physischen Computer, mit der der Neustart des Computers erzwungen wird. Alle Dateien, die auf dem Remote-Desktop geöffnet sind, werden geschlossen und nicht gespeichert.

Durch das Zurücksetzen von veröffentlichten Anwendungen werden alle geöffneten Anwendungen beendet.

Sie können einen Remote Desktop nur dann zurücksetzen, wenn ein Horizon Administrator die Funktion zum Zurücksetzen des Remote Desktops aktiviert hat.

Informationen zur Aktivierung der Funktion zum Zurücksetzen eines Desktops finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon*.

Verfahren

1 Verwenden Sie zum Zurücksetzen eines Remote-Desktops den Befehl **Desktop zurücksetzen**.

Option	Aktion
Von innerhalb des Remote-Desktops	Wählen Sie **Optionen > Desktop zurücksetzen** aus der Menüleiste aus.
Im Fenster für die Desktop- und Anwendungsauswahl	Klicken Sie mit der rechten Maustaste auf das Symbol des Remote Desktops und wählen Sie **Desktop zurücksetzen** aus.

2 Verwenden Sie zum Zurücksetzen von veröffentlichten Anwendungen die Schaltfläche **Zurücksetzen** im Fenster für die Desktop- und Anwendungsauswahl.

   a Klicken Sie in der Menüleiste auf die Schaltfläche **Einstellungen** (Zahnradsymbol).

   b Wählen Sie im linken Fensterbereich **Anwendungen** aus, klicken Sie im rechten Fensterbereich auf die Schaltfläche **Zurücksetzen** und klicken Sie auf **OK**.

Ergebnisse

Wenn Sie einen Remote Desktop zurücksetzen, wird das Betriebssystem im Remote Desktop neu gestartet, der Client wird getrennt und vom Remote Desktop abgemeldet. Wenn Sie veröffentlichte Anwendungen zurücksetzen, werden diese beendet.

Nächste Schritte

Warten Sie eine Weile, bis das System neu gestartet wurde, und versuchen Sie anschließend erneut, eine Verbindung mit dem Remote Desktop oder der veröffentlichten Anwendung herzustellen.

Reparieren von Horizon Client für Windows

Manchmal können Sie Probleme mit Horizon Client beheben, indem Sie Horizon Client reparieren.

Voraussetzungen

- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Stellen Sie sicher, dass Sie über das Horizon Client-Installationsprogramm verfügen. Sie können Horizon Client nicht reparieren, wenn Sie nicht über das Installationsprogramm verfügen.

Verfahren

- Führen Sie eine der folgenden Aufgaben aus, um Horizon Client interaktiv zu reparieren.
  - Doppelklicken Sie auf das Horizon Client-Installationsprogramm und klicken Sie auf **Reparieren**.
  - Führen Sie das Horizon Client-Installationsprogramm über die Befehlszeile aus und geben Sie den Befehl `/repair` ein.

Geben Sie z. B. bei der Eingabeaufforderung den folgenden Befehl ein:

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /repair
```

y.y.y steht für die Versionsnummer und *xxxxxx* für die Build-Nummer.

- Um Horizon Client automatisch zu reparieren, führen Sie das Horizon Client-Installationsprogramm über die Befehlszeile aus und geben Sie die Installationsbefehle `/silent` und `/repair` ein.

  Geben Sie z. B. in der Befehlszeile den folgenden Befehl ein:

  ```
  VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /repair
  ```

  y.y.y steht für die Versionsnummer und *xxxxxx* für die Build-Nummer.

Deinstallieren von Horizon Client für Windows

Wenn das Problem durch Reparieren von Horizon Client nicht behoben wird, müssen Sie Horizon Client möglicherweise deinstallieren und neu installieren.

Die nachfolgend dargestellten Schritte zeigen, wie Sie Horizon Client mit dem Horizon Client-Installationsprogramm deinstallieren.

Wenn Sie nicht über das Horizon Client-Installationsprogramm verfügen, können Sie Horizon Client auf dieselbe Weise wie andere Anwendungen auf Ihrem Windows-System deinstallieren. Beispielsweise können Sie auf einem Windows 10-System die Deinstallation des Windows-Betriebssystems verwenden oder eine Programmfunktion ändern (**Systemsteuerung > Programme und Funktionen > Programm deinstallieren oder ändern**).

Voraussetzungen

Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.

Verfahren

- Um Horizon Client interaktiv zu deinstallieren, führen Sie eine der folgenden Aufgaben aus.
  - Doppelklicken Sie auf das Horizon Client -Installationsprogramm und klicken Sie auf **Entfernen**.
  - Führen Sie das Horizon Client-Installationsprogramm über die Befehlszeile aus und geben Sie den Befehl `/uninstall` ein.

    Geben Sie z. B. bei der Eingabeaufforderung den folgenden Befehl ein:

    ```
    VMware-Horizon-Client-y.y.y-xxxxxx.exe /uninstall
    ```

    y.y.y steht für die Versionsnummer und *xxxxxx* für die Build-Nummer.

- Um Horizon Client automatisch zu deinstallieren, führen Sie das Horizon Client-Installationsprogramm über die Befehlszeile aus und geben Sie die Installationsbefehle `/silent` und `/uninstall` ein.

  Geben Sie z. B. bei der Eingabeaufforderung den folgenden Befehl ein:

  ```
  VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /uninstall
  ```

  y.y.y steht für die Versionsnummer und *xxxxxx* für die Build-Nummer.

Nächste Schritte

Installieren Sie Horizon Client erneut. Siehe Kapitel 2 Installation von Horizon Client für Windows.

Probleme bei der Tastatureingabe

Wenn Sie Zeichen in einen Remote-Desktop oder eine veröffentlichte Anwendung eingeben, scheint keine der Tastatureingaben zu funktionieren.

Problem

Bei einer Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung werden während der Eingabe keine Zeichen auf dem Bildschirm angezeigt. Ein anderes mögliches Phänomen ist die mehrmalige Wiederholung einer Taste.

Ursache

Einige Sicherheitsprogramme, wie z. B. Norton 360 Total Security, verfügen über eine Funktion zur Ermittlung von Keylogger-Software, die die Tastatureingabe sperrt. Mit dieser Sicherheitsfunktion soll das System vor Spyware geschützt werden, mit der z. B. Kennwörter oder Kreditkartennummern gestohlen werden. Diese Sicherheitssoftware kann allerdings verhindern, dass Horizon Client Tastatureingaben an den Remote-Desktop oder die veröffentlichte Anwendung sendet.

Lösung

- Deaktivieren Sie auf dem Clientsystem die Funktion zur Erkennung von Keyloggern Ihrer Antivirus- oder Sicherheitssoftware.

Vorgehensweise, wenn Horizon Client unerwartet beendet wird

Horizon Client wird beendet, selbst wenn Sie die Anwendung nicht schließen.

Problem

Horizon Client wird unerwartet beendet. Abhängig von der Serverkonfiguration wird möglicherweise eine Meldung wie die Folgende angezeigt: `Es besteht keine sichere Verbindung mit dem View-Verbindungsserver`. Manchmal wird keine Meldung angezeigt.

Ursache

Dieses Problem tritt auf, wenn die Verbindung zum Server getrennt wird.

Lösung

- Starten Sie Horizon Client neu. Sie können sich erfolgreich verbinden, wenn der Server wieder ausgeführt wird. Sollten weiterhin Probleme mit der Verbindung bestehen, wenden Sie sich an den Systemadministrator oder den VMware Support.

Herstellen einer Verbindung mit einem Server im Workspace ONE-Modus

Sie können eine Verbindung mit einem Server nicht direkt über Horizon Client herstellen, da sonst die Berechtigungen für Ihre Remote Desktops und veröffentlichten Anwendungen in Horizon Client nicht angezeigt werden.

Problem

- Wenn Sie versuchen, eine direkte Verbindung mit dem Server über Horizon Client herzustellen, werden Sie von Horizon Client zum Workspace ONE-Portal umgeleitet.
- Wenn Sie einen Remote Desktop oder eine veröffentlichte Anwendung über einen URI oder eine Verknüpfung öffnen oder wenn Sie eine lokale Datei über die Dateiverknüpfung öffnen, leitet die Anforderung Sie zum Workspace ONE-Portal zur Authentifizierung weiter.
- Nach dem Öffnen eines Remote Desktops oder einer veröffentlichten Anwendung über Workspace ONE und dem Start von Horizon Client werden andere berechtigte Remote Desktops oder veröffentlichte Anwendungen in Horizon Client nicht angezeigt oder können nicht geöffnet werden.

Ursache

Ein Horizon Administrator kann Workspace ONE auf einer Verbindungsserverinstanz aktivieren. Dies ist das Standardverhalten, wenn der Workspace ONE-Modus auf einer Verbindungsserverinstanz aktiviert ist.

Lösung

Verwenden Sie Workspace ONE, um eine Verbindung mit einem Workspace ONE-aktivierten Server herzustellen und um auf Ihre Remote Desktops und veröffentlichten Anwendungen zuzugreifen.