

# VMware Horizon HTML Access Installations- und Einrichtungshandbuch

DEZ 2019

VMware Horizon HTML Access 5.3

VMware Horizon 7 7.10



vmware®

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

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://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](http://www.vmware.com/de)

Copyright © 2013-2019 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

# Inhalt

## VMware Horizon HTML Access Installations- und Einrichtungshandbuch 5

### 1 Konfiguration und Installation 6

- Systemanforderungen für HTML Access 7
- Vorbereiten von Verbindungsserver und Sicherheitsservern 9
  - Firewallregeln für Client-Webbrowser-Zugriff 11
- Konfigurieren von Horizon 7 zum Entfernen von Anmeldedaten aus dem Cache 12
- Vorbereiten von Desktops, Pools und Farmen 13
- Anforderungen für die Funktion „Session Collaboration“ 15
- Konfigurieren von HTML Access-Agents zur Verwendung von neuen TLS-Zertifikaten 16
  - Hinzufügen des Zertifikat-Snap-In zur MMC auf einem Remote-Desktop 17
  - Importieren eines Zertifikats für den HTML Access-Agent in den Windows-Zertifikatspeicher 17
  - Importieren von Stamm- und Zwischenzertifikaten für den HTML Access-Agent 18
  - Festlegen des Zertifikatfingerabdrucks in der Windows-Registrierung 19
- Konfiguration der HTML Access-Agents zur Verwendung spezifischer Verschlüsselungsansammlungen 20
- Konfigurieren von iOS zur Verwendung von durch Zertifizierungsstellen signierten Zertifikaten 21
- Verwenden eines von einer Zertifizierungsstelle signierten Zertifikats mit Unified Access Gateway 21
- Konfigurieren von Autoplay in Chrome und Safari 22
- Upgrade der HTML Access-Software 22
- Deinstallieren der HTML Access-Komponente vom Verbindungsserver 22
- Konfigurieren der Horizon Client-Datenfreigabe 23
  - Deaktivieren der Datenfreigabe für alle HTML Access-Benutzer 23
  - Von VMware erfasste Daten 24

### 2 Konfigurieren von HTML Access für Endbenutzer 26

- Konfigurieren der VMware Horizon-Webportalseite für Endbenutzer 26
- Verwenden von URIs zur Konfiguration von HTML Access-Webclients 30
  - Syntax für die Erstellung von URIs für HTML Access 30
  - Beispiele für URIs 33
- Gruppenrichtlinieneinstellungen für HTML Access 36

### 3 Verwalten der Remote-Desktop- und veröffentlichten Anwendungsverbindungen 37

- Verbindung zu einem Remote-Desktop oder einer veröffentlichten Anwendung herstellen 37
- Einstufen eines selbstsignierten Zertifikats als vertrauenswürdig 40
- Herstellen einer Verbindung mit einem Server im Workspace ONE-Modus 41
- Verwenden des nicht authentifizierten Zugriffs zur Verbindungsherstellung mit veröffentlichten Anwendungen 41

Festlegen der Zeitzone	42
Zulassen der H.264-Decodierung	43
Abmelden oder trennen	44

## **4 Verwenden eines Remote-Desktops oder einer veröffentlichten Anwendung 45**

Funktionsunterstützungs-Matrix	45
Verwenden der Sidebar	47
Monitore und Bildschirmauflösung	50
Verwenden mehrerer Monitore	50
Festlegen der Bildschirmauflösung für Remote-Desktops und veröffentlichte Anwendungen	51
Verwendung der DPI-Synchronisierung	52
Verwenden des Vollbildmodus	54
Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone	54
Freigeben von Remote-Desktop-Sitzungen	55
Einladen eines Benutzers zu einer Remote-Desktop-Sitzung	56
Verwalten einer freigegebenen Remote-Desktop-Sitzung	58
Betritt zu einer Remote-Desktop-Sitzung	59
Kopieren und Einfügen von Text	60
Verwenden des Fenster „Kopieren und Einfügen“	61
Übertragen von Dateien zwischen dem Client und einem Remote-Desktop oder einer veröffentlichten Anwendung	63
Herunterladen von Dateien von einem Remote-Desktop oder einer veröffentlichten Anwendung auf das Clientsystem	64
Hochladen von Dateien vom Clientsystem auf einen Remote-Desktop oder eine veröffentlichte Anwendung	65
Verwenden mehrerer Sitzungen einer veröffentlichten Anwendung von unterschiedlichen Clientgeräten aus	65
Sound	66
Tastenkombinationen	67
Internationalisierung	70
Internationale Tastaturen	71

## **5 Fehlerbehebung für Horizon Client 72**

Neustarten eines Remote-Desktops	72
Zurücksetzen von Remote-Desktops oder veröffentlichten Anwendungen	73

# VMware Horizon HTML Access Installations- und Einrichtungshandbuch

Das vorliegende Dokument *VMware Horizon HTML Access Installations- und Einrichtungshandbuch* beschreibt die Installation, Konfiguration und Verwendung der VMware Horizon® HTML Access™-Software für die Herstellung einer Verbindung zu virtuellen Desktops, ohne Software auf einem Clientsystem installieren zu müssen.

Die Informationen in diesem Dokument enthalten Systemanforderungen und Anleitungen zur Installation von HTML Access-Software auf einem VMware Horizon 7-Server und auf einer virtuellen Maschine des Remote-Desktops, damit Endbenutzer mit einem Webbrowser auf Remote-Desktops zugreifen können.

---

**Wichtig** Diese Informationen sind für Administratoren gedacht, die bereits Erfahrung mit der Verwendung von Horizon 7 und VMware vSphere haben. Wenn Sie ein neuer Benutzer von Horizon 7 sind, müssen Sie möglicherweise gelegentlich die schrittweisen Anleitungen für grundlegende Verfahren in der Dokumentation zur *Installation* von Horizon 7 und in der Dokumentation zu *Verwaltung der VMware Horizon Console* heranziehen.

---

# Konfiguration und Installation

# 1

Bei der Einrichtung einer Horizon 7-Bereitstellung für HTML Access müssen Sie HTML Access auf Horizon Connection Server installieren, die erforderlichen Ports öffnen und die HTML Access-Komponente auf der virtuellen Maschine des Remote-Desktops installieren.

Benutzer können dann auf ihre Remote-Desktops zugreifen, indem sie einen unterstützten Browser öffnen und die URL für Horizon Connection Server eingeben.

Dieses Kapitel enthält die folgenden Themen:

- [Systemanforderungen für HTML Access](#)
- [Vorbereiten von Verbindungsserver und Sicherheitsservern](#)
- [Konfigurieren von Horizon 7 zum Entfernen von Anmeldedaten aus dem Cache](#)
- [Vorbereiten von Desktops, Pools und Farmen](#)
- [Anforderungen für die Funktion „Session Collaboration“](#)
- [Konfigurieren von HTML Access-Agents zur Verwendung von neuen TLS-Zertifikaten](#)
- [Konfiguration der HTML Access-Agents zur Verwendung spezifischer Verschlüsselungsansammlungen](#)
- [Konfigurieren von iOS zur Verwendung von durch Zertifizierungsstellen signierten Zertifikaten](#)
- [Verwenden eines von einer Zertifizierungsstelle signierten Zertifikats mit Unified Access Gateway](#)
- [Konfigurieren von Autoplay in Chrome und Safari](#)
- [Upgrade der HTML Access-Software](#)
- [Deinstallieren der HTML Access-Komponente vom Verbindungsserver](#)
- [Konfigurieren der Horizon Client-Datenfreigabe](#)

# Systemanforderungen für HTML Access

Mit HTML Access wird für das Clientsystem keine weitere Software als ein unterstützter Browser benötigt. Die Horizon 7-Bereitstellung muss bestimmte Software-Anforderungen erfüllen.

## Browser auf Clientsystemen

Browser	Version
Chrome	75, 76
Internet Explorer	11
Safari	12
Firefox	67, 68
Microsoft Edge	42, 44
VMware Workspace ONE Web	Die neueste Version im Apple App Store (iOS-Geräte) oder im Google Play Store (Android-Geräte).

### Hinweis

- Folgende Elemente werden von Chrome auf einem Android-Gerät nicht unterstützt: die Windows-Taste, mehrere Monitore, das Kopieren und Einfügen in das System, die Dateiübertragung, das Drucken, die H.264-Decodierung, die Bereinigung von Anmeldedaten und eine externe Maus. Außerdem können die folgenden Tasten und Tastenkombinationen auf der Softwaretastatur nicht verwendet werden: ENTF, STRG+A, STRG+C, STRG+V, STRG+X, STRG+Y, STRG+Z.
- Folgende Elemente werden von Safari auf einem mobilen Gerät nicht unterstützt: eine externe Maus, die Windows-Taste, mehrere Monitore, das Kopieren und Einfügen in das System, die Dateiübertragung, das Drucken, die H.264-Decodierung und die Bereinigung von Anmeldedaten.

## Clientbetriebssysteme:

Betriebssystem	Version
Windows	7 SP1 (32 Bit und 64 Bit) 8.x (32 Bit und 64 Bit) 10 (32 Bit und 64 Bit)
Mac OS	10.14.x (Mojave) 10.13.x (High Sierra)
iOS	10 oder höher
Chrome OS	28.x oder höher
Android	7 oder höher

## Remote-Desktops

HTML Access erfordert Horizon Agent 7.0 oder höher und unterstützt alle Desktop-Betriebssysteme, die Horizon Agent 7.0 unterstützt. Weitere

Informationen finden Sie unter „Unterstützte Betriebssysteme für Horizon Agent“ in Version 7.0 oder höher im Dokument *Horizon 7-Installation*.

## Pool-Einstellungen

HTML Access erfordert die folgenden Pooleinstellungen.

- Die Option **Maximale Auflösung eines Monitors** muss auf **1920x1200** oder höher festgelegt sein, damit der Remote-Desktop über mindestens 17,63 MB an Video-RAM verfügt.

Wenn Sie 3D-Anwendungen verwenden, oder wenn die Endbenutzer mit einem MacBook mit Retina-Display oder mit einem Google Chromebook Pixel arbeiten, finden Sie weitere Informationen unter [Festlegen der Bildschirmauflösung für Remote-Desktops und veröffentlichte Anwendungen](#).

- Die Einstellung **HTML Access** muss aktiviert sein.

Konfigurationsanweisungen werden unter [Vorbereiten von Desktops, Pools und Farmen](#) bereitgestellt.

## Verbindungsserver

Der Verbindungsserver muss mit der Option HTML Access auf dem Server installiert sein.

Wenn Sie die HTML Access-Komponente installieren, wird die Regel **VMware Horizon View-Verbindungsserver (Blast-In)** für die Windows-Firewall konfiguriert, damit eingehender Datenverkehr auf dem TCP-Port 8443 zugelassen wird.

## Sicherheitsserver

Auf dem Sicherheitsserver muss die gleiche Version wie auf dem Verbindungsserver installiert sein.

Wenn Clientsysteme von außerhalb der firmeneigenen Firewall eine Verbindung herstellen, verwenden Sie einen Sicherheitsserver. Mit einem Sicherheitsserver benötigen die Clientsysteme keine VPN-Verbindung.

---

**Hinweis** Ein einzelner Sicherheitsserver kann bis zu 800 gleichzeitige Verbindungen mit Web Clients unterstützen.

---

## Firewalls von Drittanbietern

Fügen Sie Regeln hinzu, um den folgenden Datenverkehr zuzulassen:

- Server (einschließlich Sicherheitsserver, Verbindungsserver-Instanzen und Replikatserver): eingehender Datenverkehr auf TCP-Port 8443.
- Virtuelle Maschinen des Remote-Desktops: eingehender Datenverkehr (von Servern) auf TCP-Port 22443.

## Anzeigeprotokoll für Horizon

VMware Blast



Wenn Sie einen Webbrowser für den Zugriff auf einen Remote-Desktop verwenden, wird anstelle von PCoIP oder Microsoft RDP das VMware Blast-Protokoll verwendet. VMware Blast basiert auf HTTPS (HTTP über SSL/TLS).

## Vorbereiten von Verbindungsserver und Sicherheitsservern

Bevor Endbenutzer auf einen Remote-Desktop oder eine veröffentlichte Anwendung zugreifen können, muss ein Horizon-Administrator den Verbindungsserver sowie Sicherheitsserver installieren, falls diese verwendet werden.

Für sicheren externen Zugriff können Sie statt Sicherheitsservern Unified Access Gateway-Appliances verwenden. Weitere Informationen finden Sie im Dokument *Bereitstellen und Konfigurieren von Unified Access Gateway*.

Im Folgenden finden Sie eine Checkliste mit Aufgaben, die ein Horizon-Administrator durchführen muss, damit HTML Access verwendet werden kann.

- 1 Installieren Sie den Verbindungsserver. Hierfür muss auf dem Server bzw. den Servern einer replizierten Verbindungsserver-Gruppe die Einstellung **HTML Access installieren** ausgewählt sein. Wenn diese Einstellung ausgewählt ist, wird die HTML Access-Komponente installiert. Diese Einstellung ist im Installationsprogramm standardmäßig ausgewählt. Weitere Informationen finden Sie im Dokument *Horizon 7-Installation*.

Um sicherzustellen, dass die HTML Access-Komponente installiert ist, können Sie das Windows-Applet zum Deinstallieren von Programmen öffnen und in der Liste nach **VMware Horizon 7 HTML Access** suchen.

- 2 Wenn Sie Sicherheitsserver verwenden, installieren Sie Sicherheitsserver. Die Version des Sicherheitsservers muss mit der Version des Verbindungsservers übereinstimmen. Anweisungen zur Installation finden Sie im Dokument *Horizon 7-Installation*.
- 3 Vergewissern Sie sich, dass jede Verbindungsserver-Instanz oder jeder Sicherheitsserver ein TLS-Zertifikat besitzt, das unter Verwendung des Hostnamens, den Sie im Webbrowser eingeben, vollständig überprüft werden kann. Weitere Informationen finden Sie im Dokument *Horizon 7-Installation*.
- 4 Zum Verwenden der zweistufigen Authentifizierung, z. B. der RSA SecurID- oder RADIUS-Authentifizierung, muss diese Funktion auf dem Verbindungsserver aktiviert sein. Ab Horizon 7 Version 7.11 können Sie die Bezeichnungen auf der Anmeldeseite für die RADIUS-Authentifizierung anpassen. Weitere Informationen finden Sie in den Themen zur zweistufigen Authentifizierung im Dokument *Verwaltung der VMware Horizon Console*.
- 5 Um das Dropdown-Menü **Domäne** in Horizon Client auszublenden, aktivieren Sie die globale Einstellung **Domänenliste in der Kunden-Benutzeroberfläche ausblenden**. Diese Einstellung ist in Horizon 7, Version 7.1 und höher verfügbar. Ab Horizon 7, Version 7.8 ist sie standardmäßig aktiviert. Weitere Informationen finden Sie im Dokument *Verwaltung der VMware Horizon Console*.

- 6 Um die Domänenliste an Horizon Client zu senden, aktivieren Sie die globale Einstellung **Domänenliste senden**. 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 *Verwaltung der VMware Horizon Console*-Dokument für Horizon 7 Version 7.8 oder höher.
- 7 Wenn Sie eine Firewall eines Drittanbieters verwenden, konfigurieren Sie Regeln zum Zulassen von eingehendem Datenverkehr am TCP-Port 8443 für alle Sicherheitsserver- und Verbindungsserver-Hosts in einer replizierten Gruppe. Konfigurieren Sie außerdem eine Regel zum Zulassen von eingehendem Datenverkehr (von Servern) am TCP-Port 22443 auf virtuellen Maschinen von Remote-Desktops und RDS-Hosts im Datacenter. Weitere Informationen finden Sie unter [Firewallregeln für Client-Webbrowser-Zugriff](#).
- 8 Um einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen zu ermöglichen, aktivieren Sie diese Funktion im Verbindungsserver. Weitere Informationen finden Sie im Dokument *Verwaltung der VMware Horizon Console*.

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

Einstellung „Domänenliste senden“	Einstellung „Domänenliste in der Kunden-Benutzeroberfläche ausblenden“	Wie sich Benutzer anmelden
Deaktiviert (Standard)	Aktiviert	<p>Das Dropdown-Menü <b>Domäne</b> ist ausgeblendet. Benutzer müssen einen der folgenden Werte in das Textfeld <b>Benutzername</b> eingeben.</p> <ul style="list-style-type: none"> <li>■ Benutzername (nicht für mehrere Domänen zulässig)</li> <li>■ <b>Domäne\Benutzername</b></li> <li>■ <b>username@domain.com</b></li> </ul>
Deaktiviert (Standard)	Deaktiviert	<p>Wenn eine Standardldomäne auf dem Client konfiguriert ist, wird die Standardldomäne im Dropdown-Menü <b>Domäne</b> angezeigt. Wenn der Client keine Standardldomäne kennt, wird *DefaultDomain* im Dropdown-Menü <b>Domäne</b> angezeigt. Benutzer müssen einen der folgenden Werte in das Textfeld <b>Benutzername</b> eingeben.</p> <ul style="list-style-type: none"> <li>■ Benutzername (nicht für mehrere Domänen zulässig)</li> <li>■ <b>Domäne\Benutzername</b></li> <li>■ <b>username@domain.com</b></li> </ul>

Einstellung „Domänenliste senden“	Einstellung „Domänenliste in der Kunden- Benutzeroberfläche ausblenden“	Wie sich Benutzer anmelden
Aktiviert	Aktiviert	<p>Das Dropdown-Menü <b>Domäne</b> ist ausgeblendet. Benutzer müssen einen der folgenden Werte in das Textfeld <b>Benutzername</b> eingeben.</p> <ul style="list-style-type: none"> <li>■ Benutzername (nicht für mehrere Domänen zulässig)</li> <li>■ <i>Domäne\Benutzername</i></li> <li>■ <i>username@domain.com</i></li> </ul>
Aktiviert	Deaktiviert	<p>Benutzer können einen Benutzernamen in das Textfeld <b>Benutzername</b> eingeben und dann eine Domäne aus dem Dropdown-Menü <b>Domäne</b> auswählen. Alternativ können Benutzer auch einen der folgenden Werte in das Textfeld <b>Benutzername</b> eingeben.</p> <ul style="list-style-type: none"> <li>■ <i>Domäne\Benutzername</i></li> <li>■ <i>username@domain.com</i></li> </ul>

Nach der Installation der Server ist die Einstellung **Blast Secure Gateway** auf den betreffenden Verbindungsserver-Instanzen und Sicherheitsservern in Horizon Console aktiviert. Darüber hinaus ist für die Einstellung **Externe Blast-URL** die Verwendung von Blast Secure Gateway auf den betreffenden Verbindungsserver-Instanzen und Sicherheitsservern konfiguriert. Standardmäßig schließt die URL den FQDN der externen URL für den sicheren Tunnel sowie die standardmäßige Portnummer 8443 ein. Die URL muss den FQDN und die Portnummer enthalten, die ein Clientsystem zur Verbindungsherstellung mit diesem Verbindungsserver- oder Sicherheitsserver-Host verwenden kann. Weitere Informationen finden Sie unter „Festlegen der externen URLs für eine Verbindungsserver-Instanz“ im Dokument *Horizon 7-Installation*.

**Hinweis** Sie können HTML Access mit VMware Workspace ONE verwenden, damit Benutzer die Möglichkeit haben, über einen HTML5-Browser eine Verbindung zu ihren Desktops herzustellen. Informationen zur Installation von Workspace ONE und zur Konfiguration für die Verwendung mit dem Verbindungsserver finden Sie in der Workspace ONE-Dokumentation. Weitere Informationen zur Kopplung des Verbindungsservers mit einem SAML-Authentifizierungsserver finden Sie im Dokument *Verwaltung der VMware Horizon Console*.

## Firewallregeln für Client-Webbrowser-Zugriff

Um Client-Webbrowsern zu ermöglichen, eine Verbindung zu Sicherheitsservern, Verbindungsserver-Instanzen, Remote-Desktops und veröffentlichten Anwendungen herzustellen, müssen Ihre Firewalls eingehenden Datenverkehr auf bestimmten TCP-Ports erlauben.

HTML Access-Verbindungen müssen HTTPS verwenden. HTTP-Verbindungen sind nicht erlaubt.

Bei der Installation einer Verbindungsserver-Instanz oder eines Sicherheitsservers wird standardmäßig die Regel **VMware Horizon View-Verbindungsserver (Blast-In)** in der Windows-Firewall aktiviert, und die Firewall wird so konfiguriert, dass eingehender Datenverkehr auf dem TCP-Port 8443 zugelassen wird.

**Tabelle 1-1. Firewallregeln für Client-Browser-Zugriff**

Quelle	Standard quell- Port	Protokoll	Ziel	Standard ziel-Port	Hinweise
Client- Webbrowser	TCP beliebig	HTTPS	Sicherheitss erver oder Verbindungs server- Instanz	TCP 443	Um die erste Verbindung herzustellen, verbindet sich der Webbrowser auf einem Client-Gerät an TCP-Port 443 mit einem Sicherheitsserver oder einer Verbindungsserver-Instanz.
Client- Webbrowser	TCP beliebig	HTTPS	Blast Secure Gateway	TCP 8443	Nachdem die erste Verbindung hergestellt wurde, stellt der Webbrowser auf einem Clientgerät eine Verbindung mit dem Blast Secure Gateway über den TCP-Port 8443 her. Die zweite Verbindung kann nur hergestellt werden, wenn das Blast Secure Gateway auf einem Sicherheitsserver oder einer Verbindungsserver-Instanz aktiviert ist.
Blast Secure Gateway	TCP beliebig	HTTPS	HTML Access Agent	TCP 22443	Wenn, nachdem der Benutzer einen Remote-Desktop oder eine veröffentlichte Anwendung ausgewählt hat, das Blast Secure Gateway aktiviert ist, stellt das Blast Secure Gateway über den TCP-Port 22443 auf der virtuellen Maschine des Remote-Desktops oder auf dem RDS-Host eine Verbindung zum HTML Access-Agent her. Diese Agent-Komponente ist Bestandteil der Installation von Horizon Agent.
Client- Webbrowser	TCP beliebig	HTTPS	HTML Access- Agent	TCP 22443	Wenn, nachdem der Benutzer einen Remote-Desktop oder eine veröffentlichte Anwendung ausgewählt hat, das Blast Secure Gateway nicht aktiviert ist, stellt der Webbrowser auf einem Clientgerät direkt eine Verbindung über den TCP-Port 22443 auf der virtuellen Maschine des Remote-Desktops oder auf dem RDS-Host zum HTML Access-Agent her. Diese Agent-Komponente ist Bestandteil der Installation von Horizon Agent.

## Konfigurieren von Horizon 7 zum Entfernen von Anmeldedaten aus dem Cache

Sie können Horizon 7 so konfigurieren, dass die Anmeldeinformationen eines Benutzers aus dem Cache entfernt werden, wenn der Benutzer eine Registerkarte schließt, die mit einem Remote-Desktop oder einer veröffentlichten Anwendung bzw. mit dem Auswahlfenster für Desktops und Anwendungen verbunden ist.

Wenn diese Funktion deaktiviert ist (Standardeinstellung) verbleiben die Anmeldedaten im Cache.

**Hinweis** Ist diese Funktion aktiviert, werden die Anmeldedaten auch aus dem Cache gelöscht, wenn ein Benutzer die Seite für die Auswahl von Desktop und Anwendung oder die Seite für die Remote-Sitzung aktualisiert oder wenn er einen URI-Befehl auf der Registerkarte ausführt, die die Remote-Sitzung enthält. Wenn der Server ein selbstsigniertes Zertifikat bereitstellt, werden die Anmeldedaten aus dem Cache gelöscht, wenn ein Benutzer einen Remote-Desktop oder eine veröffentlichte Anwendung startet und das Zertifikat bei der Sicherheitswarnung akzeptiert.

## Voraussetzungen

Diese Funktion erfordert Horizon 7 Version 7.0.2 oder höher.

## Verfahren

- 1 Wählen Sie in Horizon Console **Einstellungen > Globale Einstellungen** aus, klicken Sie auf die Registerkarte **Allgemeine Einstellungen** und dann auf **Bearbeiten**.
- 2 Aktivieren Sie das Kontrollkästchen **Bereinigen von Anmeldeinformationen, wenn eine Registerkarte für HTML Access geschlossen wird**.
- 3 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ihre Änderungen werden sofort wirksam. Der Verbindungsserver muss nicht neu gestartet werden.

## Vorbereiten von Desktops, Pools und Farmen

Bevor Endbenutzer auf einen Remote-Desktop oder eine veröffentlichte Anwendung zugreifen können, muss ein Horizon-Administrator bestimmte Pool- und Farmeinstellungen konfigurieren und Horizon Agent auf virtuellen Desktop-Maschinen und RDS-Hosts im Datacenter installieren.

Der HTML Access-Client ist eine gute Alternative, wenn die Horizon Client-Software nicht auf dem Clientsystem installiert ist.

---

**Hinweis** Die Horizon Client-Software bietet mehr Funktionen und eine höhere Leistung als der HTML Access-Client. Beispielsweise funktionieren beim HTML Access-Client einige Tastenkombinationen auf dem Remote-Desktop nicht, sie funktionieren allerdings bei Horizon Client.

---

## Voraussetzungen

- Stellen Sie sicher, dass die Horizon-Komponenten die Systemanforderungen für HTML Access erfüllen. Siehe [Systemanforderungen für HTML Access](#).
- Vergewissern Sie sich, dass die HTML Access-Komponente zusammen mit dem Verbindungsserver auf dem Host bzw. den Hosts installiert ist und dass die Windows-Firewall auf den Verbindungsserver-Instanzen und allen Sicherheitsservern eingehenden Datenverkehr am TCP-Port 8443 zulassen. Siehe [Vorbereiten von Verbindungsserver und Sicherheitsservern](#).
- Wenn Sie eine Firewall eines Drittanbieters verwenden, konfigurieren Sie eine Regel, mit der eingehender Datenverkehr von Horizon Servern am TCP-Port 22443 für virtuelle Desktop-Maschinen und RDS-Hosts im Datacenter zugelassen wird. Siehe [Firewallregeln für Client-Webbrowser-Zugriff](#).
- Stellen Sie sicher, dass die virtuelle Maschine, die Sie als Desktop-Quelle verwenden möchten, oder der RDS-Host, der veröffentlichte Desktops und Anwendungen hostet, über ein unterstütztes Betriebssystem verfügt und dass VMware Tools installiert ist. Siehe [Systemanforderungen für HTML Access](#).

- Machen Sie sich mit den Verfahren für das Erstellen von Pools und Farmen sowie für das Zuweisen von Benutzerberechtigungen vertraut. Sehen Sie sich die Dokumente *Einrichten von virtuellen Desktops in Horizon 7* und *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7* an.
- Um sicherzustellen, dass der Remote-Desktop oder die veröffentlichte Anwendung für Endbenutzer zugänglich ist, installieren Sie Horizon Client für Windows auf einem Clientsystem. Sie können Horizon Client für Windows verwenden, um die Verbindung zu testen, bevor Sie versuchen, von einem Webbrowser eine Verbindung herzustellen. Anweisungen zur Installation finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*.
- Stellen Sie sicher, dass Sie einen der unterstützten Browser für den Zugriff auf einen Remote-Desktop oder eine veröffentlichte Anwendung verwenden. Siehe [Systemanforderungen für HTML Access](#).

## Verfahren

- 1 Erstellen oder bearbeiten Sie für veröffentlichte Desktops und Anwendungen die Farm mit Horizon Console und aktivieren Sie die Option **HTML Access für Desktops und Anwendungen in dieser Farm zulassen** in den Farmeinstellungen.
- 2 Bei virtuellen Desktop-Pools bearbeiten Sie den Desktop-Pool mit Horizon Console, damit der Pool mit HTML Access verwendet werden kann.
  - a Aktivieren Sie **HTML Access** in den Desktop-Pool-Einstellungen.
  - b Stellen Sie sicher, dass in den Pool-Einstellungen die **Maximale Auflösung für alle Monitore** auf **1920x1200** oder höher festgelegt ist.
- 3 Nachdem die Pools erstellt, neu zusammengestellt oder aktualisiert wurden, um Horizon Agent mit der Option **HTML Access für Desktops und Anwendungen in dieser Farm zulassen** oder **HTML Access** zu verwenden, verwenden Sie Horizon Client für Windows, um eine Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung herzustellen.

Mit diesem Schritt stellen Sie noch vor der Verwendung von HTML Access sicher, dass der Pool ordnungsgemäß arbeitet.

- 4 Öffnen Sie einen unterstützten Browser und geben Sie eine URL ein, die auf Ihre Verbindungsserver-Instanz verweist.

Beispiel:

```
https://horizon.mycompany.com
```

Die URL muss **https** enthalten.

- 5 Klicken Sie auf der angezeigten Webseite auf **VMware Horizon HTML Access** und melden Sie sich so wie bei Horizon Client für Windows an.
- 6 Klicken Sie auf der eingeblendeten Auswahlseite für Desktops und Anwendungen zur Herstellung der Verbindung auf ein Symbol.

Sie können jetzt von einem Webbrowser auf einen Remote-Desktop oder eine veröffentlichte Anwendung zugreifen.

### Nächste Schritte

Falls Ihre Sicherheitsrichtlinien für den HTML Access-Agent auf dem Remote-Desktop zur Erhöhung der Sicherheit die Verwendung eines TLS-Zertifikats von einer Zertifizierungsstelle vorsehen, finden Sie weitere Informationen unter [Konfigurieren von HTML Access-Agents zur Verwendung von neuen TLS-Zertifikaten](#).

## 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 4.7 oder höher für Windows, Mac oder Linux installiert sein oder HTML Access 4.7 oder höher verwendet werden.

### Windows-Remote-Desktops

- Horizon Agent 7.4 oder höher muss auf dem virtuellen Windows-Desktop oder auf dem RDS-Host für veröffentlichte Desktops installiert sein.
- 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 7*. Informationen zur Aktivierung der Funktion „Session Collaboration“ für eine Farm erhalten Sie im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

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 7*.

### Linux-Remote-Desktops

Informationen zu den Anforderungen für Linux-Remote-Desktops finden Sie im Dokument *Einrichten von Horizon 7 for Linux-Desktops*.

### 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.

# Konfigurieren von HTML Access-Agents zur Verwendung von neuen TLS-Zertifikaten

Um die Einhaltung von Branchen- oder Sicherheitsbestimmungen sicherzustellen, können Sie die standardmäßigen TLS-Zertifikate, die der HTML Access-Agent generiert, durch von einer Zertifizierungsstelle (CA, Certificate Authority) signierte Zertifikate ersetzen.

Wenn Sie den HTML Access-Agent auf Remote-Desktops installieren, erstellt der HTML Access-Agent-Dienst selbstsignierte Standardzertifikate. Der Dienst stellt die Standardzertifikate für Browser bereit, die HTML Access verwenden.

---

**Hinweis** Im Gastbetriebssystem auf der virtuellen Desktop-Maschine wird dieser Dienst VMware Blast-Dienst genannt.

---

Um die Standardzertifikate durch signierte Zertifikate zu ersetzen, die Sie von einer Zertifizierungsstelle erhalten haben, müssen Sie auf jedem Remote-Desktop ein Zertifikat in den lokalen Windows-Zertifikatspeicher des Computers importieren. Außerdem müssen Sie einen Registrierungswert festlegen, der es dem HTML Access-Agent ermöglicht, das neue Zertifikat zu verwenden.

Wenn Sie die standardmäßigen HTML Access-Agent-Zertifikate durch von einer Zertifizierungsstelle signierte Zertifikate ersetzen, konfigurieren Sie auf jedem Remote-Desktop ein eindeutiges Zertifikat. Konfigurieren Sie kein von einer Zertifizierungsstelle signiertes Zertifikat auf einer übergeordneten virtuellen Maschine oder Vorlage, die Sie für das Erstellen eines Desktop-Pools verwenden. Bei einem solchen Vorgehen entstehen Hunderte oder Tausende von Remote-Desktops, die identische Zertifikate haben.

## Verfahren

### 1 Hinzufügen des Zertifikat-Snap-In zur MMC auf einem Remote-Desktop

Bevor Sie Zertifikate im lokalen Windows-Zertifikatspeicher des Computers hinzufügen können, müssen Sie das Zertifikats-Snap-In der Microsoft Management Console (MMC) auf den Remote-Desktops hinzufügen, auf denen der HTML Access-Agent installiert ist.

### 2 Importieren eines Zertifikats für den HTML Access-Agent in den Windows-Zertifikatspeicher

Um ein standardmäßiges HTML Access-Agent-Zertifikat durch ein von einer Zertifizierungsstelle signiertes Zertifikat zu ersetzen, müssen Sie das von einer Zertifizierungsstelle signierte Zertifikat in den lokalen Windows-Zertifikatspeicher des Computers importieren. Führen Sie diesen Vorgang auf allen Remote-Desktops durch, auf denen der HTML Access-Agent installiert ist.

### 3 Importieren von Stamm- und Zwischenzertifikaten für den HTML Access-Agent

Wenn die Stamm- und Zwischenzertifikate in der Zertifikatskette nicht mit dem SSL-Zertifikat importiert werden, das Sie für den HTML Access-Agent importiert haben, müssen Sie diese Zertifikate in den lokalen Windows-Zertifikatsspeicher des Computers importieren.



#### 4 Festlegen des Zertifikatfingerabdrucks in der Windows-Registrierung

Um dem HTML Access-Agenten zu ermöglichen, ein durch eine Zertifizierungsstelle signiertes Zertifikat zu verwenden, das in den Windows-Zertifikatsspeicher importiert wurde, müssen Sie den Fingerabdruck des Zertifikats in einem Windows-Registrierungsschlüssel konfigurieren. Sie müssen diesen Schritt auf jedem Remote-Desktop vornehmen, auf dem Sie das Standardzertifikat durch ein durch eine Zertifizierungsstelle signiertes Zertifikat ersetzen.

## Hinzufügen des Zertifikat-Snap-In zur MMC auf einem Remote-Desktop

Bevor Sie Zertifikate im lokalen Windows-Zertifikatsspeicher des Computers hinzufügen können, müssen Sie das Zertifikats-Snap-In der Microsoft Management Console (MMC) auf den Remote-Desktops hinzufügen, auf denen der HTML Access-Agent installiert ist.

### Voraussetzungen

Stellen Sie sicher, dass die MMC und das Zertifikats-Snap-In in dem Windows-Gast-Betriebssystem verfügbar sind, in dem der HTML Access-Agent installiert wurde.

### Verfahren

- 1 Klicken Sie auf dem Remote-Desktop auf **Start** und geben Sie **mmc.exe** ein.
- 2 Gehen Sie im Fenster **MMC** auf **Datei > Snap-In hinzufügen/entfernen**.
- 3 Wählen Sie im Fenster **Snap-Ins hinzufügen oder entfernen** **Zertifikate** aus und klicken Sie auf **Hinzufügen**.
- 4 Wählen Sie im Fenster **Zertifikat-Snap-In** **Computerkonto**, klicken Sie auf **Weiter**, wählen Sie **Lokaler Computer** und klicken Sie auf **Fertig stellen**.
- 5 Klicken Sie im Fenster **Snap-In hinzufügen oder entfernen** auf **OK**.

### Nächste Schritte

Importieren Sie das SSL-Zertifikat in den Zertifikatsspeicher des lokalen Windows-Computers auf dem View Server-Host. Siehe [Importieren eines Zertifikats für den HTML Access-Agent in den Windows-Zertifikatsspeicher](#).

## Importieren eines Zertifikats für den HTML Access-Agent in den Windows-Zertifikatsspeicher

Um ein standardmäßiges HTML Access-Agent-Zertifikat durch ein von einer Zertifizierungsstelle signiertes Zertifikat zu ersetzen, müssen Sie das von einer Zertifizierungsstelle signierte Zertifikat in den lokalen Windows-Zertifikatsspeicher des Computers importieren. Führen Sie diesen Vorgang auf allen Remote-Desktops durch, auf denen der HTML Access-Agent installiert ist.

### Voraussetzungen

- Stellen Sie sicher, dass der HTML Access-Agent auf dem Remote-Desktop installiert ist.

- Stellen Sie sicher, dass das von einer Zertifizierungsstelle signierte Zertifikat auf den Remote-Desktop kopiert wurde.
- Überprüfen Sie, ob das Zertifikat-Snap-In der MMC hinzugefügt wurde. Siehe [Hinzufügen des Zertifikat-Snap-In zur MMC auf einem Remote-Desktop](#).

## Verfahren

- 1 Erweitern Sie im MMC-Fenster auf dem Remote-Desktop den Knoten **Zertifikate (Lokaler Computer)** und wählen Sie den Ordner **Persönlich** aus.
- 2 Wechseln Sie im Bereich „Aktionen“ zu **Weitere Aktionen > Alle Aufgaben > Importieren**.
- 3 Klicken Sie im **Zertifikatimport-Assistenten** auf **Weiter** und navigieren Sie zum Speicherort des Zertifikats.
- 4 Wählen Sie die Zertifikatdatei und klicken Sie auf **Öffnen**.

Um den Typ Ihrer Zertifikatdatei anzuzeigen, können Sie ihr Dateiformat im Dropdown-Menü **Dateiname** auswählen.

- 5 Geben Sie das Kennwort für den privaten Schlüssel in der Zertifikatdatei ein.
- 6 Wählen Sie **Schlüssel als exportierbar markieren**.
- 7 Wählen Sie **Alle erweiterbaren Eigenschaften mit einbeziehen** aus.
- 8 Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.

Das neue Zertifikat wird im Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** angezeigt.

- 9 Überprüfen Sie, ob das neue Zertifikat einen privaten Schlüssel enthält.
  - a Doppelklicken Sie im Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** auf das neue Zertifikat.
  - b Prüfen Sie, ob die folgende Meldung im Dialogfeld „Zertifikatinformationen“ auf der Registerkarte „Allgemein“ angezeigt wird: Sie besitzen einen privaten Schlüssel für dieses Zertifikat.

## Nächste Schritte

Falls erforderlich, importieren Sie das Stammzertifikat und Zwischenzertifikate in den Windows-Zertifikatspeicher. Siehe [Importieren von Stamm- und Zwischenzertifikaten für den HTML Access-Agent](#).

Konfigurieren Sie den entsprechenden Registrierungsschlüssel mit dem Zertifikatfingerabdruck. Siehe [Festlegen des Zertifikatfingerabdrucks in der Windows-Registrierung](#).

## Importieren von Stamm- und Zwischenzertifikaten für den HTML Access-Agent

Wenn die Stamm- und Zwischenzertifikate in der Zertifikatskette nicht mit dem SSL-Zertifikat importiert werden, das Sie für den HTML Access-Agent importiert haben, müssen Sie diese Zertifikate in den lokalen Windows-Zertifikatspeicher des Computers importieren.

## Verfahren

- 1 Auf der MMC-Konsole auf dem Remote-Desktop erweitern Sie den Knoten **Zertifikate (Lokaler Computer)** und gehen Sie zum Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
  - Wenn sich Ihr Stammzertifikat in diesem Ordner befindet und Ihre Zertifikatskette keine Zwischenzertifikate enthält, überspringen Sie diesen Vorgang.
  - Wenn Ihr Stammzertifikat sich nicht in diesem Ordner befindet, fahren Sie mit Schritt 2 fort.
- 2 Klicken Sie mit der rechten Maustaste auf den Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** und klicken Sie auf **Alle Aufgaben > Importieren**.
- 3 Klicken Sie im **Zertifikatsimport-Assistenten** auf **Weiter** und navigieren Sie zum Speicherort des Stamm-Zertifizierungsstellenzertifikats.
- 4 Wählen Sie die Datei mit dem Stamm-Zertifizierungsstellenzertifikat aus und klicken Sie auf **Öffnen**.
- 5 Klicken Sie auf **Weiter**, klicken Sie auf **Weiter** und klicken Sie auf **Fertig stellen**.
- 6 Wenn Ihr Serverzertifikat von einer Zwischenzertifizierungsstelle signiert wurde, importieren Sie alle Zwischenzertifikate in der Zertifikatskette in den lokalen Windows-Zertifikatsspeicher des Computers.
  - a Navigieren Sie zum Ordner **Zertifikate (Lokaler Computer) > Zwischenzertifizierungsstellen > Zertifikate**.
  - b Wiederholen Sie die Schritte 3 bis 6 für jedes zu importierende Zwischenzertifikat.

## Nächste Schritte

Konfigurieren Sie den entsprechenden Registrierungsschlüssel mit dem Zertifikatfingerabdruck. Siehe [Festlegen des Zertifikatfingerabdrucks in der Windows-Registrierung](#).

## Festlegen des Zertifikatfingerabdrucks in der Windows-Registrierung

Um dem HTML Access-Agenten zu ermöglichen, ein durch eine Zertifizierungsstelle signiertes Zertifikat zu verwenden, das in den Windows-Zertifikatsspeicher importiert wurde, müssen Sie den Fingerabdruck des Zertifikats in einem Windows-Registrierungsschlüssel konfigurieren. Sie müssen diesen Schritt auf jedem Remote-Desktop vornehmen, auf dem Sie das Standardzertifikat durch ein durch eine Zertifizierungsstelle signiertes Zertifikat ersetzen.

## Voraussetzungen

Stellen Sie sicher, dass das durch die Zertifizierungsstelle signierte Zertifikat in den Windows-Zertifikatsspeicher importiert wurde. Siehe [Importieren eines Zertifikats für den HTML Access-Agent in den Windows-Zertifikatsspeicher](#).

## Verfahren

- 1 Navigieren Sie im MMC-Fenster auf dem Remote-Desktop, auf dem der HTML Access-Agent installiert ist, zum Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate**.

- 2 Doppelklicken Sie auf das von Ihnen in den Windows-Zertifikatsspeicher importierte durch die Zertifizierungsstelle signierte Zertifikat.
- 3 Klicken Sie im Dialogfeld „Zertifikate“ auf die Registerkarte „Details“. Blättern Sie nach unten, und wählen Sie das Symbol **Fingerabdruck** aus.
- 4 Kopieren Sie den ausgewählten Fingerabdruck in eine Textdatei.

Zum Beispiel: 31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e

---

**Hinweis** Schließen Sie beim Kopieren des Fingerabdrucks das führende Leerzeichen nicht ein. Wenn Sie das führende Leerzeichen versehentlich zusammen mit dem Fingerabdruck in den Registrierungsschlüssel (in Schritt 7) einfügen, wird das Zertifikat möglicherweise nicht erfolgreich konfiguriert. Dieses Problem kann auftreten, auch wenn das führende Leerzeichen im Registrierungswert-Textfeld nicht angezeigt wird.

---

- 5 Starten Sie den Windows-Registrierungs-Editor auf dem Desktop, wo der HTML Access-Agent installiert ist.
- 6 Navigieren Sie zum Registrierungsschlüssel HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config.
- 7 Ändern Sie den Wert SslHash, und fügen Sie den Fingerabdruck des Zertifikats in das Textfeld ein.
- 8 Starten Sie Windows neu.

Wenn ein Benutzer über HTML Access eine Verbindung zu einem Remote-Desktop herstellt, präsentiert der HTML Access-Agent dem Browser des Benutzers das durch eine Zertifizierungsstelle signierte Zertifikat.

## Konfiguration der HTML Access-Agents zur Verwendung spezifischer Verschlüsselungsansammlungen

Sie können den HTML Access-Agent so konfigurieren, dass er anstelle der standardmäßigen Verschlüsselungen spezifische Verschlüsselungsansammlungen verwendet.

Der HTML Access-Agent erfordert standardmäßig eingehende SSL-Verbindungen, um Verschlüsselungen auf Basis bestimmter Verschlüsselungsverfahren, die umfassend gegen das Abhören und Fälschen von Netzwerken geschützt sind, verwenden zu können. Sie können eine alternative Liste mit Verschlüsselungsverfahren zur Verwendung durch den HTML Access-Agent konfigurieren. Der Satz mit akzeptablen Verschlüsselungsverfahren wird im OpenSSL-Format ausgedrückt, das unter <https://www.openssl.org/docs/manmaster/man1/ciphers.html> beschrieben ist.

### Verfahren

- 1 Starten Sie den Windows-Registrierungs-Editor auf dem Desktop, wo der HTML Access-Agent installiert ist.
- 2 Navigieren Sie zum Registrierungsschlüssel HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config.

- 3 Fügen Sie einen neuen Zeichenfolgenwert (REG\_SZ) hinzu, `SslCiphers`, und fügen Sie die Verschlüsselungsliste im OpenSSL-Format in das Textfeld ein.
- 4 Starten Sie den VMware Blast-Dienst neu, damit Ihre Änderungen wirksam werden.

Im Windows-Gast-Betriebssystem wird der Dienst für den HTML Access-Agent VMware Blast genannt.

Um zur Nutzung der standardmäßigen Verschlüsselungsliste zurückzukehren, löschen Sie den `SslCiphers`-Wert und starten Sie den VMware Blast-Dienst neu. Löschen Sie nicht einfach den Datenteil des Werts, sonst behandelt der HTML Access-Agent alle Verschlüsselungsverfahren entsprechend der Formatdefinition für die OpenSSL-Verschlüsselungsliste als inakzeptabel.

Wenn der HTML Access-Agent startet, schreibt er die Verschlüsselungsdefinition in die Protokolldatei des VMware Blast-Dienstes. Sie können die aktuelle standardmäßige Verschlüsselungsliste ermitteln, indem Sie die Protokolle beim Start des VMware Blast-Dienstes prüfen, der keinen `SslCiphers`-Wert in der Windows-Registrierung konfiguriert hat.

Die standardmäßige Verschlüsselungsdefinition des HTML Access-Agent kann sich von einer Version zur anderen unterscheiden, um einen verbesserten Schutz zu bieten.

## Konfigurieren von iOS zur Verwendung von durch Zertifizierungsstellen signierten Zertifikaten

Für die Verwendung von HTML Access auf iOS-Geräten müssen Sie SSL-Zertifikate installieren, die von einer Zertifizierungsstelle signiert wurden, anstelle von Standard-SSL-Zertifikaten, die durch Horizon Connection Server auf dem HTML Access Agent erstellt wurden.

Anweisungen dazu finden Sie unter „Konfigurieren von Horizon Client für iOS für vertrauenswürdige und Zwischenzertifikate“ im Dokument *Horizon 7-Installation*.

## Verwenden eines von einer Zertifizierungsstelle signierten Zertifikats mit Unified Access Gateway

Wenn Sie eine Unified Access Gateway-Appliance anstelle eines Verbindungsservers oder Sicherheitsservers verwenden, müssen Sie ein von einer Zertifizierungsstelle signiertes Zertifikat installieren, für das ein alternativer Antragstellernamen (Subject Alternative Name, SAN) konfiguriert ist.

Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat ohne konfigurierten SAN oder ein selbstsigniertes Zertifikat verwenden, erhalten Benutzer eine Fehlermeldung, dass ihre Verbindung nicht privat ist, und können keine Verbindung mit HTML Access herstellen.

---

**Hinweis** Wenn Sie eine Verbindungsserver-Instanz oder einen Sicherheitsserver verwenden, können Benutzer trotzdem eine Verbindung herstellen, indem sie auf den Link [Weiter zu IP-Adresse](#) (unsicher) klicken.

---

Informationen zum Installieren und Konfigurieren von Zertifikaten für Horizon 7 finden Sie im Dokument *Horizon 7-Installation*. Informationen zum Konfigurieren von HTML Access-Agents zur Verwendung von TLS-Zertifikaten finden Sie unter [Konfigurieren von HTML Access-Agents zur Verwendung von neuen TLS-Zertifikaten](#).

## Konfigurieren von Autoplay in Chrome und Safari

Wenn Sie HTML Access in Chrome 71 oder höher oder Safari 12 verwenden, wird Benutzern unter Umständen das Dialogfeld **Zum Aktivieren von Audio klicken** angezeigt, wenn sie einen Remote-Desktop oder eine veröffentlichte Anwendung zum ersten Mal starten oder den Browser während der Verwendung eines Remote-Desktops oder einer veröffentlichten Anwendung aktualisieren. Wenn Benutzer im Dialogfeld auf **OK** klicken, wird normalerweise Audio wiedergegeben.

Sie können durch Konfigurieren der Autoplay-Richtlinie im Browser verhindern, dass dieses Dialogfeld angezeigt wird.

- Geben Sie in Chrome **chrome://flags/#autoplay-policy** in die Navigationsleiste ein, scrollen Sie zu **Autoplay-Richtlinie** und wählen Sie **Keine Benutzeraktion erforderlich** aus dem Dropdown-Menü.
- Wählen Sie in Safari auf einem Mac **Safari > Einstellungen für diese Website**, halten Sie den Zeiger rechts von **Autoplay**, klicken Sie auf das Dropdown-Menü und wählen Sie **Autoplay immer zulassen**.

## Upgrade der HTML Access-Software

Für die meisten Versionen von HTML Access umfasst das Upgrade nur ein Upgrade von Horizon Connection Server und Horizon Agent.

Wenn Sie ein Upgrade für HTML Access durchführen, müssen Sie sicherstellen, dass die entsprechende Horizon Connection Server-Version auf allen Instanzen einer replizierten Gruppe installiert ist.

Beim Aktualisieren des Verbindungsservers wird HTML Access automatisch installiert oder aktualisiert.

---

**Hinweis** Um zu überprüfen, ob die HTML Access-Komponente installiert ist, können Sie im Windows-Betriebssystem das Applet zum Deinstallieren von Programmen öffnen und in der Liste nach HTML Access suchen.

---

## Deinstallieren der HTML Access-Komponente vom Verbindungsserver

Sie können die HTML Access-Komponente mit der gleichen Methode entfernen, mit der Sie andere Windows-Software entfernen.

### Verfahren

- 1 Öffnen Sie auf der Verbindungsserver-Instanz, auf der HTML Access installiert ist, das Applet zum Deinstallieren von Programmen, das in der Windows-Systemsteuerung zur Verfügung steht.

- 2 Wählen Sie **VMware Horizon 7 HTML Access** aus und klicken Sie auf **Deinstallieren**.
- 3 (Optional) Stellen Sie in der Windows-Firewall für den Host sicher, dass der TCP-Port 8443 keinen eingehenden Datenverkehr mehr erlaubt.

### Nächste Schritte

Verhindern Sie eingehenden Datenverkehr an TCP-Port 8443 auf der Windows-Firewall aller gepaarten Sicherheitsserver. Auf Firewalls von Drittanbietern ändern Sie gegebenenfalls die Regeln, um eingehenden Datenverkehr an TCP-Port 8443 für alle gepaarten Sicherheitsserver und die Verbindungsserver-Instanz zu verbieten.

## 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 *Verwaltung der VMware Horizon Console*.

Die Datenfreigabe ist in HTML Access standardmäßig aktiviert. Sie können die Einstellung zur Datenfreigabe nach der Herstellung einer Verbindung mit einem Server nicht mehr ändern.

Ein Horizon-Administrator kann die Datenfreigabe in HTML Access für alle Benutzer deaktivieren und verhindern, dass Benutzer die Einstellung für die Datenfreigabe in HTML Access ändern. Weitere Informationen finden Sie unter [Deaktivieren der Datenfreigabe für alle HTML Access-Benutzer](#).

### Verfahren

- 1 Starten Sie Horizon Client.
- 2 Klicken Sie auf der VMware Horizon-Anmeldeseite auf **Einstellungen** (Zahnradsymbol).
- 3 Aktivieren oder deaktivieren Sie die Option **Datenfreigabe zulassen**.

## Deaktivieren der Datenfreigabe für alle HTML Access-Benutzer

Ein Horizon-Administrator kann die Datenfreigabe für alle HTML Access-Benutzer deaktivieren und verhindern, dass Benutzer die Option **Datenfreigabe zulassen** in HTML Access ändern, indem er die folgende Einstellung der Datei C:\Programme\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\classes\portal-version.properties auf der Verbindungsserver-Instanz hinzufügt.

```
CEIP.disabled=true
```

Wenn diese Einstellung auf `true` festgelegt ist, wird die Option **Einstellungen** (Zahnradsymbol) auf der VMware Horizon-Anmeldeseite in HTML Access nicht angezeigt.

**Hinweis** Diese Einstellung hat keine Auswirkungen auf Benutzer, die Horizon Client zum Herstellen einer Verbindung mit der Verbindungsserver-Instanz verwenden. Informationen zum Deaktivieren der Datenfreigabe in Horizon Client finden Sie im Installations- und Einrichtungshandbuch für die entsprechende Horizon Client-Plattform.

## Von VMware erfasste Daten

Wenn Ihr Unternehmen am Programm zur Verbesserung der Benutzerfreundlichkeit von VMware (Customer Experience Improvement Program, CEIP) teilnimmt und die Datenfreigabe auf dem Client aktiviert ist, erfasst VMware Daten zum Clientsystem.

VMware sammelt die Daten auf den Clients zur Priorisierung der Hardware- und Softwarekompatibilität. Wenn sich ein Horizon-Administrator zur Teilnahme am CEIP entschieden hat, erfasst VMware anonyme Daten über Ihre Bereitstellung, um die Reaktion auf Kundenanforderungen verbessern zu können. Es werden jedoch keine Daten gesammelt, die Aufschluss über Ihr Unternehmen geben könnten. Die Clientinformationen werden erst an den Verbindungsserver und dann an VMware gesendet, zusammen mit den Daten der Server, Desktop-Pools und Remote-Desktops.

Zur Teilnahme am CEIP kann der Administrator, der die Installation des Verbindungsservers durchführt, bei der Ausführung des Installationsassistenten für den Verbindungsserver diese Option „abonnieren“ oder nach der Installation eine entsprechende Option in Horizon Console festlegen.

**Tabelle 1-2. Für das CEIP erfasste Clientdaten**

Beschreibung	Feldname	Wird dieses Feld anonymisiert?	Beispielswert
Unternehmen, das die Anwendung hergestellt hat	<client_vendor>	Nein	VMware
Produktname	<client_product>	Nein	VMware Horizon HTML Access
Client-Produktversion	<client_version>	Nein	5.3.0-build_number
Client-Binärarchitektur	<client_arch>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> <li>■ Browser</li> <li>■ arm</li> </ul>
Systemeigene Architektur des Browsers	<browser_arch>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> <li>■ Win32</li> <li>■ Win64</li> <li>■ MacIntel</li> <li>■ iPad</li> <li>■ Linux armv81 (zur Unterstützung von Android Chrome)</li> </ul>



**Tabelle 1-2. Für das CEIP erfasste Clientdaten (Fortsetzung)**

Beschreibung	Feldname	Wird dieses Feld anonymisiert ?	Beispielswert
Zeichenfolge zum Browserbenutzer-Agent	<browser_user_agent>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> <li>■ Mozilla/5.0 (Windows NT 6.1; WOW64)</li> <li>■ AppleWebKit/703.00 (KHTML, wie Gecko)</li> <li>■ Chrome/3.0.1750</li> <li>■ Safari/703.00</li> <li>■ Edge/13.10586</li> </ul>
Interne Versionszeichenfolge des Browsers	<browser_version>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> <li>■ 7.0.3 (für Safari),</li> <li>■ 44.0 (für Firefox)</li> <li>■ 13.10586 (für Edge)</li> </ul>
Core-Implementierung des Browsers	<browser_core>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> <li>■ Chrome</li> <li>■ Safari</li> <li>■ Firefox</li> <li>■ Internet Explorer</li> <li>■ Edge</li> </ul>
Angabe, ob der Browser auf einem Handheld-Gerät ausgeführt wird	<browser_is_handheld>	Nein	true

# Konfigurieren von HTML Access für Endbenutzer

## 2

Sie können das Aussehen der Webseite ändern, die Endbenutzer bei Eingabe der URL für HTML Access sehen. Sie können außerdem Gruppenrichtlinien festlegen, mit denen Bildqualität, verwendete Ports und weitere Einstellungen gesteuert werden.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren der VMware Horizon-Webportalseite für Endbenutzer](#)
- [Verwenden von URIs zur Konfiguration von HTML Access-Webclients](#)
- [Gruppenrichtlinieneinstellungen für HTML Access](#)

## Konfigurieren der VMware Horizon-Webportalseite für Endbenutzer

Sie können diese Webseite so konfigurieren, dass das Symbol zum Herunterladen von Horizon Client oder das Symbol für die Herstellung einer Verbindung mit einem Remote-Desktop über HTML Access angezeigt oder ausgeblendet wird. Sie können außerdem weitere Links auf dieser Seite konfigurieren.

Standardmäßig werden auf der Webportalseite ein Symbol für den Download und die Installation des nativen Horizon Client sowie ein Symbol für die Verbindungsherstellung über HTML Access angezeigt. Der verwendete Download-Link wird von den in der Datei `portal-links-html-access.properties` definierten Standardwerten bestimmt.

Es kann aber sein, dass die Links auf einen internen Webserver verweisen sollen oder dass Sie bestimmte Clientversionen auf Ihrem eigenen Server zur Verfügung stellen möchten. Sie können dann die Portalseite so konfigurieren, dass diese auf eine andere Download-URL verweist. Dazu müssen Sie den Inhalt der Datei `portal-links-html-access.properties` ändern. Wenn diese Datei nicht verfügbar oder leer ist und die Datei `oslinks.properties` vorhanden ist, wird der Link für die Installationsdatei aus der Datei `oslinks.properties` ermittelt.

Die Datei `oslinks.properties` wird im Ordner `<Installationsverzeichnis>\VMware\VMware View\Server\broker\webapps\portal\WEB-INF` installiert. Wenn diese Datei in der HTML Access-Sitzung nicht vorhanden ist, leitet der Download-Link die Benutzer standardmäßig zu `https://www.vmware.com/go/viewclients` weiter. Die Datei enthält die folgenden Standardwerte:

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win32=https://www.vmware.com/go/viewclients#win32
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux32=https://www.vmware.com/go/viewclients#linux32
link.linux64=https://www.vmware.com/go/viewclients#linux64
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.chromeos=https://chrome.google.com/webstore/detail/vmware-horizonclient/
pckbpdplfajmgaipljfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

Sie können Links zum Installationsprogramm für bestimmte Clientbetriebssysteme entweder in der Datei `portal-links-html-access.properties` oder in der Datei `oslinks.properties` erstellen. Wenn Sie beispielsweise die Portalseite auf einem Mac OS X-System öffnen, wird der Link für das native Mac OS X-Installationsprogramm angezeigt. Für Windows- oder Linux-Clients haben Sie die Möglichkeit, separate Links für die 32-Bit- und 64-Bit-Installationsprogramme zu erstellen.

## Verfahren

- 1 Öffnen Sie auf dem Verbindungsserver-Host die Datei `portal-links-html-access.properties` mit einem Texteditor.

Der Speicherort dieser Datei lautet `CommonAppDataFolder\VMware\VDM\portal\portal-links-html-access.properties`. Auf Windows Server 2008-Betriebssystemen entspricht das Verzeichnis `CommonAppDataFolder` dem Ordner `C:\ProgramData`. Zur Anzeige des Ordners `C:\ProgramData` in Windows Explorer müssen Sie im Dialogfeld mit den Ordneroptionen die Anzeige ausgeblendeter Ordner aktivieren.

Wenn die Datei `portal-links-html-access.properties` nicht vorhanden ist, jedoch die Datei `oslinks.properties`, öffnen Sie die Datei `<Installationsverzeichnis>\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\oslinks.properties` zur Änderung der URLs für das Herunterladen bestimmter Installationsdateien.

---

**Hinweis** Die Anpassungen für Horizon 7 5.x und frühere Versionen befanden sich in der Datei `portal-links.properties`, die sich im selben Verzeichnis `CommonAppDataFolder\VMware\VDM\portal\` befindet wie die Datei `portal-links-html-access.properties`.

---

## 2 Bearbeiten Sie die Konfigurationseigenschaften nach Bedarf.

Standardmäßig sind das Installationsprogramm-Symbol und das HTML Access-Symbol aktiviert und ein Link verweist auf die Client-Download-Seite auf der VMware-Website. Wenn Sie ein Symbol deaktivieren möchten, stellen Sie die Eigenschaft auf `false` ein. Dadurch wird das Symbol aus der Webseite entfernt.

**Hinweis** Die Datei `oslinks.properties` kann nur zur Konfiguration der Links zu bestimmten Installationsdateien verwendet werden. Sie unterstützt nicht die anderen unten aufgeführten Optionen.

Option	Eigenschafteneinstellung
<b>HTML Access deaktivieren</b>	<code>enable.webclient=false</code> Wenn für diese Option „false“ festgelegt ist, aber für die Option <code>enable.download</code> der Wert „true“ gesetzt ist, wird der Benutzer zu einer Webseite geleitet, von der das native Installationsprogramm für Horizon Client heruntergeladen werden kann. Wenn für beide Optionen der Wert „false“ festgelegt ist, wird dem Benutzer die folgende Nachricht angezeigt: „Wenden Sie sich an Ihren lokalen Administrator, um Anweisungen zum Zugriff auf diesen Verbindungsserver zu erhalten.“
<b>Herunterladen von Horizon Client deaktivieren</b>	<code>enable.download=false</code> Wenn für diese Option „false“ festgelegt ist, aber für die Option <code>enable.webclient</code> der Wert „true“ gesetzt ist, wird der Benutzer zur Anmeldeseite für HTML Access geleitet. Wenn für beide Optionen der Wert „false“ festgelegt ist, wird dem Benutzer die folgende Nachricht angezeigt: „Wenden Sie sich an Ihren lokalen Administrator, um Anweisungen zum Zugriff auf diesen Verbindungsserver zu erhalten.“
<b>Ändern der URL für die Webseite zum Herunterladen von Horizon Client</b>	<code>link.download=https://url-of-web-server</code> Verwenden Sie diese Eigenschaft, wenn Sie Ihre eigene Webseite erstellen möchten.

Option	Eigenschafteneinstellung
<b>Create links for specific installers (Links für bestimmte Installationsprogramme erstellen)</b>	<p>Die folgenden Beispiele enthalten vollständige URLs; Sie können jedoch auch relative URLs verwenden, wenn Sie, wie im nächsten Schritt beschrieben, die Installationsdateien in dem Verzeichnis „downloads“ ablegen, das sich im Verzeichnis C:\Programme\VMware\VMware View\Server\broker\webapps\ auf dem Verbindungsserver befindet.</p> <ul style="list-style-type: none"> <li>■ Allgemeiner Link zum Herunterladen des Installationsprogramms: <pre>link.download=https://server/downloads</pre> </li> <li>■ 32-Bit-Windows-Installationsprogramm: <pre>link.win32=https://Server/downloads/VMware-Horizon-Client-x86-Build-Nr..exe</pre> </li> <li>■ 64-Bit-Windows-Installationsprogramm: <pre>link.win64=https://Server/downloads/VMware-Horizon-Client-x86_64-Build-Nr..exe</pre> </li> <li>■ Windows Phone-Installationsprogramm: <pre>link.winmobile=https://Server/downloads/VMware-Horizon-Client-Build-Nr..appx</pre> </li> <li>■ 32-Bit-Linux-Installationsprogramm: <pre>link.linux32=https://Server/downloads/VMware-Horizon-Client-Build-Nr..x86.bundle</pre> </li> <li>■ 64-Bit-Linux-Installationsprogramm: <pre>link.linux64=https://Server/downloads/VMware-Horizon-Client-Build-Nr..x64.bundle</pre> </li> <li>■ Mac OS X-Installationsprogramm: <pre>link.mac=https://Server/downloads/VMware-Horizon-Client-Build-Nr..dmg</pre> </li> <li>■ iOS-Installationsprogramm: <pre>link.ios=https://Server/downloads/VMware-Horizon-Client-iPhoneOS-Build-Nr..ipa</pre> </li> <li>■ Android-Installationsprogramm: <pre>link.android=https://Server/downloads/VMware-Horizon-Client-AndroidOS-Build-Nr..apk</pre> </li> <li>■ Chrome OS-Installationsprogramm: <pre>link.chromeos=https://Server/downloads/VMware-Horizon-Client-ChromeOS-Build-Nr..apk</pre> </li> </ul>
<b>Ändern der URL für den Hilfe-Link auf der Anmeldeseite</b>	<pre>link.help</pre> <p>Dieser Link verweist standardmäßig auf ein Hilfesystem, das auf der VMware-Website verwaltet wird. Der Hilfe-Link wird auf der Anmeldeseite unten angezeigt.</p>

- 3 Damit Benutzer die Installationsprogramme von einem anderen Speicherort als der VMware-Website herunterladen, legen Sie die Installationsdateien auf dem HTTP-Server ab, auf dem sich auch die Installationsdateien befinden.

Dieser Speicherort muss mit den URLs übereinstimmen, die Sie in der Datei `portal-links-html-access.properties` oder `oslinks.properties` im vorherigen Schritt angegeben haben. Um die Dateien beispielsweise in einem Verzeichnis „downloads“ auf dem Verbindungsserver-Host zu speichern, verwenden Sie den folgenden Pfad:

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

Die Links zu den Installationsdateien können dann relative URLs mit dem Format `/downloads/client-installationsdateiname` verwenden.

- 4 Starten Sie den Horizon-Webkomponentendienst neu.

## Verwenden von URIs zur Konfiguration von HTML Access-Webclients

Mithilfe so genannter Uniform Resource Identifiers (URIs) können Sie eine Webseite oder E-Mail mit verschiedenen Verknüpfungen erstellen, auf die die Endbenutzer zum Start von HTML Access Web client, zur Verbindung mit Horizon Connection Server oder zum Start eines bestimmten Desktops oder einer bestimmten Anwendung mit bestimmten Konfigurationsoptionen klicken.

Sie können die Verbindungsherstellung mit einem Remote-Desktop oder einer Anwendung durch Erstellen von Web- oder E-Mail-Verknüpfungen für die Endbenutzer deutlich vereinfachen. Diese Verknüpfungen werden durch die Generierung von URIs erstellt, die einige oder alle der folgenden Informationen bereitstellen, sodass die Endbenutzer diese nicht angeben müssen:

- Horizon Connection Server-Adresse
- Portnummer für Horizon Connection Server
- Active Directory-Benutzername
- RADIUS- oder RSA SecurID-Benutzername, falls dieser nicht mit dem Active Directory-Benutzernamen identisch ist
- Domänenname
- Desktop- oder Anwendungsanzeigename
- Aktionen, darunter „Durchsuchen“, „Zurücksetzen“, „Abmelden“ und „Sitzung starten“

## Syntax für die Erstellung von URIs für HTML Access

Die Syntax umfasst eine Pfadkomponente zur Angabe des Servers sowie optional eine Abfrage zur Angabe eines Benutzers, des Remote-Desktops oder der veröffentlichten Anwendung sowie Aktionen oder Konfigurationsoptionen.

## URI-Spezifikation

Verwenden Sie zum Generieren von URIs für den Start von HTML Access die folgende Syntax:

```
https://authority-part[/?query-part]
```

### ***authority-part***

Gibt die Serveradresse und optional eine nicht standardmäßige Portnummer an. Die Servernamen müssen der DNS-Syntax entsprechen.

Verwenden Sie zur Angabe einer Portnummer die folgende Syntax:

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

### ***query-part***

Gibt die zu verwendenden Konfigurationsoptionen oder die durchzuführenden Aktionen an. 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. Sollten die Abfragen miteinander in Konflikt stehen, wird die letzte Abfrage in der Liste verwendet. Verwenden Sie die folgende Syntax:

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

Beachten Sie beim Erstellen der Abfragekomponente (query-part) die folgenden Richtlinien:

- Wenn Sie nicht mindestens eine der unterstützten Abfragen verwenden, wird die standardmäßige VMware Horizon-Webportalseite angezeigt.
- Für die Abfragekomponente werden einige Sonderzeichen nicht unterstützt; es muss deshalb für diese das URL-Codierungsformat wie folgt angewendet werden: Für das Hashzeichen (#, Doppelkreuz) verwenden Sie **%23**, für das Prozentzeichen (%) **%25**, für das Kaufmännische Und (&) den Platzhalter **%26**, für das At-Zeichen (@) **%40** und für den Rückschrägstrich (\) verwenden Sie **%5C**.

Weitere Informationen zur URL-Codierung finden Sie unter [http://www.w3schools.com/tags/ref\\_urlencode.asp](http://www.w3schools.com/tags/ref_urlencode.asp).

- Für die Abfragekomponente 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/>.

## Unterstützte Abfragen

In diesem Abschnitt werden die Abfragen aufgeführt, die für HTML Access unterstützt werden. Wenn Sie URIs für mehrere Clienttypen generieren, so zum Beispiel für Desktop-Clients oder mobile Clients, finden Sie im Installations- und Einrichtungsdokument für jede Art von Clientsystem weitere Informationen.

### action

**Tabelle 2-1. 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	Startet 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.
reset	Führt den angegebenen Remote-Desktop herunter und startet ihn neu. Nicht gespeicherte Daten gehen verloren. Das Zurücksetzen eines Remote-Desktops entspricht dem Betätigen der Reset-Taste auf einem physischen PC. Diese Aktion ist für eine veröffentlichte Anwendung ungültig.
logout	Meldet den Benutzer vom Gastbetriebssystem auf dem Remote-Desktop ab. Diese Aktion ist für eine veröffentlichte Anwendung ungültig.
restart	Führt den primären Remote-Desktop herunter und startet diesen neu, wenn der Benutzer die Anforderung für den Neustart bestätigt. Diese Aktion ist für eine veröffentlichte Anwendung ungültig.

### applicationId

Der Anzeigename der veröffentlichten Anwendung. Dieser Anzeigename ist der Name, der in Horizon Console beim Erstellen des Anwendungspools angegeben wurde. Weist der Anzeigename ein Leerzeichen auf, verwendet der Browser %20 zur Darstellung des Leerzeichens.

### args

Gibt Befehlszeilenargumente zum Hinzufügen an, wenn eine 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.

### desktopId

Der Anzeigename des Remote-Desktops. Der Anzeigename ist der Name, der in Horizon Console beim Erstellen des Desktop-Pools angegeben



wurde. Weist der Anzeigename ein Leerzeichen auf, verwendet der Browser **%20** zur Darstellung des Leerzeichens.

<b>domainName</b>	Der NETBIOS-Domänenname, 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.
<b>tokenUserName</b>	Der RSA- oder RADIUS-Benutzername. 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, wird der Windows-Benutzername verwendet.
<b>userName</b>	<p>Der Active Directory-Benutzer, der eine Verbindung zum Remote-Desktop oder zur veröffentlichten Anwendung herstellt. Für den Benutzernamen sind folgende Formate zulässig:</p> <ul style="list-style-type: none"> <li>■ <i>Benutzername</i></li> <li>■ <i>Domänenname%5CBenutzername</i></li> <li>■ Benutzerprinzipalname (User Principal Name, UPN) in der Form <i>Benutzername@Domänenname</i></li> </ul>
<b>unauthenticatedAccess Enabled</b>	Wenn für diese Option <b>True</b> festgelegt ist, ist die Funktion für den nicht authentifizierten Zugriff standardmäßig aktiviert. HTML Access wird gestartet, und ein Benutzerkonto für anonyme Benutzer wird angezeigt. Ein Beispiel für die Syntax ist etwa <b>unauthenticatedAccessEnabled=true</b> .
<b>unauthenticatedAccess Account</b>	Damit wird das Konto festgelegt, das verwendet werden soll, wenn die Funktion für den nicht authentifizierten Zugriff aktiviert ist. Wenn der nicht authentifizierte Zugriff deaktiviert ist, wird diese Abfrage ignoriert. Die entsprechende Syntax lautet beispielsweise bei Verwendung des Benutzerkontos <b>anonymous1</b> dann <b>unauthenticatedAccessAccount=anonymous1</b> .

## Beispiele für URIs

Sie können Hypertext-Links oder Schaltflächen mit einem URI erstellen und diese Links in E-Mails oder auf einer Webseite einbinden. Ihre Endbenutzer können dann auf diese Links klicken, um beispielsweise einen bestimmten Remote-Desktop oder eine bestimmte Remoteanwendung mit den von Ihnen angegebenen Startoptionen zu öffnen.

## URI-Syntaxbeispiele

Nach jedem URI-Beispiel finden Sie eine Beschreibung, was der Endbenutzer nach Anklicken des URI-Links sieht. Für die Abfragen muss die Groß- und Kleinschreibung nicht beachtet werden. Sie können beispielsweise **domainName** oder **domainname** verwenden.

1 `https://horizon.mycompany.com/?domainName=finance&userName=fred`

HTML Access Web client wird gestartet und stellt eine Verbindung mit dem Server `horizon.mycompany.com` her. Im Anmeldefeld wird das Textfeld **Benutzername** mit dem Namen **fred** und das Textfeld **Domäne** mit **finance** gefüllt. Der Benutzer muss das Kennwort eingeben.

2 `https://horizon.mycompany.com/?userName=finance%5Cfred`

HTML Access Web client wird gestartet und stellt eine Verbindung mit dem Server `horizon.mycompany.com` her. Im Anmeldefeld ist im Textfeld **Benutzername** der Name **financefred** enthalten. Der Benutzer muss das Kennwort eingeben.

3 `https://horizon.mycompany.com/?userName=fred@finance`

HTML Access Web client wird gestartet und stellt eine Verbindung mit dem Server `horizon.mycompany.com` her. Im Anmeldefeld ist im Textfeld **Benutzername** der Name **fred@finance** enthalten. Der Benutzer muss das Kennwort eingeben.

4 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=start-session`

HTML Access Web client wird gestartet und stellt eine Verbindung mit dem Server `horizon.mycompany.com` her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domännennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigenamen als **Primary Desktop** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet.

5 `https://horizon.mycompany.com/?applicationId=Notepad&action=start-session`

HTML Access Web client wird gestartet und stellt eine Verbindung mit dem Server `horizon.mycompany.com` her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domännennamen und Kennwort auf. Nach der erfolgreichen Anmeldung wird der Editor gestartet.

6 `https://horizon.mycompany.com:7555/?desktopId=Primary%20Desktop`

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

7 `https://horizon.mycompany.com/?applicationId=Primary%20Application&desktopId=Primary%20Desktop`

Dieser URI gibt eine Anwendung und einen Desktop an. Wenn Sie eine Anwendung und einen Desktop angeben, wird nur der Desktop gestartet.

8 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=reset`

Der HTML Access Web Client wird gestartet und stellt eine Verbindung mit dem Server `horizon.mycompany.com` her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domännennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung zeigt der Client ein Dialogfeld an, in dem der Benutzer aufgefordert wird, das Zurücksetzen für „Primary Desktop“ zu bestätigen.

**Hinweis** Diese Aktion ist nur verfügbar, wenn der Horizon-Administrator den Endbenutzern das Zurücksetzen ihrer Maschinen erlaubt hat.

9 `https://horizon.mycompany.com/?My%20Notepad++?args=%22My%20new%20file.txt%22`

Öffnet My Notepad++ auf dem Server `horizon.mycompany.com` und übergibt das Argument `my_new_file.txt` an den Befehl zum Start der Anwendung. Der Dateiname ist in doppelte Anführungszeichen gesetzt, da er Leerzeichen enthält.

10 `https://horizon.mycompany.com/?Notepad++%2012?args=a.txt%20b.txt`

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

**Hinweis** 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`.

11 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=restart`

HTML Access Web client wird gestartet und stellt eine Verbindung mit dem Server `horizon.mycompany.com` her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domännennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung zeigt der Client ein Dialogfeld an, in dem der Benutzer aufgefordert wird, den Neustart für „Primary Desktop“ zu bestätigen.

**Hinweis** Diese Aktion ist nur verfügbar, wenn der Horizon-Administrator den Endbenutzern den Neustart ihrer Maschinen erlaubt hat.

12 `https://horizon.mycompany.com/?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_user1`

HTML Access Web client wird gestartet und stellt eine Verbindung mit dem Server `horizon.mycompany.com` mithilfe des Kontos **anonymous\_user1** her.

## 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** besagt und eine Schaltfläche mit dem Text **TestButton** zu codieren.

```
<html>
<body>

<a href="https://horizon.mycompany.com/?domainName=finance&userName=fred">Test Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'https://horizon.mycompany.com/?domainName=finance&userName=fred'"></form> <br>

</body>
</html>
```

## Gruppenrichtlinieneinstellungen für HTML Access

HTML Access verwendet das VMware Blast-Protokoll. Sie konfigurieren Gruppenrichtlinien für HTML Access, indem Sie Gruppenrichtlinien für das VMware Blast-Protokoll konfigurieren.

Weitere Informationen finden Sie unter „Konfigurieren von Richtlinien für Desktop- und Anwendungspools“ und „VMware Blast – Richtlinieneinstellungen“ im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

# Verwalten der Remote-Desktop- und veröffentlichten Anwendungsverbindungen

## 3

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 zurücksetzen.

Dieses Kapitel enthält die folgenden Themen:

- [Verbindung zu einem Remote-Desktop oder einer veröffentlichten Anwendung herstellen](#)
- [Einstufen eines selbstsignierten Zertifikats als vertrauenswürdig](#)
- [Herstellen einer Verbindung mit einem Server im Workspace ONE-Modus](#)
- [Verwenden des nicht authentifizierten Zugriffs zur Verbindungsherstellung mit veröffentlichten Anwendungen](#)
- [Festlegen der Zeitzone](#)
- [Zulassen der H.264-Decodierung](#)
- [Abmelden oder trennen](#)

## Verbindung zu einem Remote-Desktop oder einer veröffentlichten Anwendung herstellen

Verwenden Sie Ihre Active Directory-Anmeldedaten zum Herstellen einer Verbindung mit den Remote-Desktops und veröffentlichten Anwendungen, für deren Verwendung Sie autorisiert sind.

### Voraussetzungen

- Besorgen Sie sich die Anmeldedaten, etwa einen Active Directory-Benutzernamen und das zugehörige Kennwort, den RSA SecurID-Benutzernamen und -Passcode oder die RADIUS-Authentifizierungsdaten.
- Besorgen Sie sich den NETBIOS-Domännennamen für die Anmeldung. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.

## Verfahren

- 1 Öffnen Sie einen Browser und geben Sie die URL für die Verbindungsserver-Instanz ein.

Für die URL geben Sie **https** und den vollqualifizierten Domännennamen ein, z. B. `https://horizon.company.com`.

Verbindungen zum Verbindungsserver verwenden immer SSL. Der Standardport für SSL-Verbindungen ist 443. Wenn der Verbindungsserver nicht zur Verwendung des Standardports konfiguriert ist, muss folgendes beispielhaft dargestellte Format verwendet werden:

**horizon.company.com:1443.**

Das Webportal von VMware Horizon erscheint. Standardmäßig werden auf dieser Seite ein Symbol für den Download und für die Installation des nativen Horizon Client sowie ein Symbol für die Verbindungsherstellung über HTML Access angezeigt.

- 2 (Optional) Aktivieren Sie das Kontrollkästchen **Klicken Sie auf diese Option, damit dieser Bildschirm übergangen und immer HTML Access verwendet wird.**

Ihre Auswahl wird im lokalen Speicher für den aktuell verwendeten Browser gespeichert. Wenn Sie das nächste Mal die URL für die Verbindungsserver-Instanz mithilfe des gleichen Browsertyps und mit demselben Clientcomputer eingeben, werden Sie direkt zum Anmeldebildschirm geleitet. Wenn Sie einen anderen Browsertyp auf demselben Clientcomputer oder den gleichen Browsertyp auf einem anderen Clientcomputer verwenden, wird das VMware Horizon-Webportal angezeigt. Löschen Sie Ihren Browsercache, wenn das VMware Horizon-Webportal angezeigt werden soll.

- 3 Klicken Sie auf das Symbol **VMware Horizon HTML Access**.

- 4 Wenn Sie im Anmeldedialogfeld zur Eingabe von RSA SecurID-Anmeldedaten oder RADIUS-Authentifizierungsinformationen aufgefordert werden, geben Sie den Benutzernamen sowie den Passcode ein und klicken Sie auf **Anmelden**.

Der Passcode kann möglicherweise sowohl aus einer PIN als auch aus einer auf dem Token generierten Nummer bestehen.

- 5 Wenn Sie erneut aufgefordert werden, RSA SecurID-Anmeldedaten oder RADIUS-Authentifizierungs-Anmeldedaten einzugeben, geben Sie die nächste zum Token generierte Nummer ein.

Geben Sie nicht Ihre PIN oder dieselbe, zuvor eingegebene generierte Nummer ein. Warten Sie, falls nötig, bis eine neue Nummer generiert wurde.

Wenn dieser Schritt erforderlich ist, dann nur, wenn Sie den ersten Passcode falsch eingegeben haben oder wenn die Konfigurationseinstellungen im RSA-Server geändert werden.

**6** Geben Sie im Anmeldedialogfeld Ihre Anmeldedaten ein.

- a Geben Sie in das Textfeld „Benutzername“ Ihren gültigen Active Directory-Benutzernamen entweder im Format *Benutzername*, *Domäne\Benutzername* oder im Format *Benutzername@Domäne* ein.

Wenn das Textfeld „Domäne“ deaktiviert ist, müssen Sie entweder das Format *Domäne\Benutzername* oder das Format *Benutzername@Domäne* verwenden.

- b Geben Sie Ihr Kennwort ein.
- c (Optional) Wenn das Textfeld „Domäne“ aktiviert ist, wählen Sie einen Domänennamen aus, wenn dieser noch nicht korrekt aufgeführt ist.

---

**Hinweis** Wenn Sie den Anmeldevorgang vorzeitig abbrechen möchten, klicken Sie auf **Abbrechen**.

---

- 7 (Optional) Wenn Sie die Zeitzone manuell festlegen müssen, die im Remote-Desktop oder in der veröffentlichten Anwendung verwendet wird, klicken Sie auf die Schaltfläche **Einstellungen** der Symbolleiste rechts oben im Auswahlfenster für Desktops und Anwendungen. Deaktivieren Sie die Option **Zeitzone automatisch festlegen** und wählen Sie eine Zeitzone aus dem Dropdown-Menü aus. Siehe [Festlegen der Zeitzone](#).

- 8 (Optional) Bevor Sie das Element für den Zugriff auswählen, klicken Sie im Auswahlbildschirm für Desktops und Anwendungen zur Kennzeichnung eines Remote-Desktops oder einer veröffentlichten Anwendung als Favorit auf den grauen Stern im Symbol des Desktops oder der veröffentlichten Anwendung.

Das Sternsymbol erscheint dann nicht mehr grau, sondern gelb. Nach der nächsten Anmeldung klicken Sie, wenn Sie nur Favoriten darstellen möchten, dieses Sternsymbol oben rechts im Browserfenster an.

- 9 Klicken Sie auf das Symbol des Remote-Desktops oder der veröffentlichten Anwendung, auf den oder die Sie zugreifen möchten.

Der Remote-Desktop oder die veröffentlichte Anwendung wird in Ihrem Browser angezeigt. Es ist auch eine Navigations-Sidebar verfügbar. Um die Sidebar einzublenden, klicken Sie auf die Registerkarte links im Browserfenster. Mit der Sidebar können Sie auf andere Remote-Desktops oder veröffentlichte Anwendungen zugreifen, das Fenster „Einstellungen“ aufrufen, Text kopieren und einfügen und vieles mehr.

**Nächste Schritte**

Unmittelbar nach der Verbindungsherstellung mit einem Desktop oder einer veröffentlichten Anwendung wird die Verbindung getrennt und eine Aufforderung angezeigt, auf einen Link zur Bestätigung des Sicherheitszertifikats zu klicken, wenn Sie dem Zertifikat vertrauen. Siehe [Einstufen eines selbstsignierten Zertifikats als vertrauenswürdig](#).

## Einstufen eines selbstsignierten Zertifikats als vertrauenswürdig

In einigen Fällen werden Sie bei der erstmaligen Herstellung einer Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung vom Browser möglicherweise aufgefordert, das vom Remotecomputer verwendete selbstsignierte Zertifikat zu akzeptieren. Sie müssen das Zertifikat als vertrauenswürdig einstufen, bevor Sie eine Verbindung mit dem Remote-Desktop oder der veröffentlichten Anwendung herstellen können.

Die meisten Browser bieten die Möglichkeit, das selbstsignierte Zertifikat dauerhaft als vertrauenswürdig einzustufen. Wenn Sie das Zertifikat dauerhaft als vertrauenswürdig einstufen, müssen Sie das Zertifikat bei jedem Neustart des Browsers überprüfen. Bei einem Safari-Browser muss das Sicherheitszertifikat dauerhaft als vertrauenswürdig eingestuft werden, damit eine Verbindung hergestellt werden kann.

### Verfahren

- 1 Wenn im Browser eine Warnmeldung zu einem nicht vertrauenswürdigen Zertifikat oder zum nicht privaten Status Ihrer Verbindung angezeigt wird, müssen Sie das Zertifikat überprüfen, um sicherzustellen, dass es dem Zertifikat entspricht, das Ihr Unternehmen verwendet.

Wenden Sie sich gegebenenfalls an Ihren Systemadministrator, der Ihnen weiterhelfen kann. In Chrome können Sie beispielsweise wie nachfolgend dargestellt vorgehen.

- a Klicken Sie auf das Schlosssymbol in der Adressleiste.
- b Klicken Sie auf den Link **Zertifikatsinformationen**.
- c Stellen Sie sicher, dass das Zertifikat dem Zertifikat entspricht, das Ihr Unternehmen verwendet.

Wenden Sie sich gegebenenfalls an Ihren Systemadministrator, der Ihnen weiterhelfen kann.

- 2 Akzeptieren Sie das Sicherheitszertifikat.

Jeder Browser verfügt über eigene Meldungen und Eingabeaufforderungen für das Akzeptieren oder dauerhafte Einstufen eines Zertifikats als vertrauenswürdig. In einem Chrome-Browser können Sie beispielsweise auf den Link **Erweitert** auf der Browserseite klicken und dann auf **Weiter zu Servername (unsicher)**.

Gehen Sie in einem Safari-Browser für die dauerhafte Einstufung eines Zertifikats als vertrauenswürdig wie nachfolgend dargestellt vor.

- a Klicken Sie auf die Schaltfläche **Zertifikat einblenden** im Dialogfeld „Zertifikat nicht vertrauenswürdig“.
- b Aktivieren Sie das Kontrollkästchen **Immer vertrauen** und klicken Sie auf **Fortfahren**.
- c Wenn Sie dazu aufgefordert werden, geben Sie Ihr Kennwort ein und klicken Sie auf **Einstellungen aktualisieren**.

Der Remote-Desktop oder die veröffentlichte Anwendung wird gestartet.



## Herstellen einer Verbindung mit einem Server im Workspace ONE-Modus

Ab Horizon 7 Version 7.2 hat ein Horizon-Administrator die Möglichkeit, den Workspace ONE-Modus auf einer Verbindungsserver-Instanz zu aktivieren.

Wenn der Workspace ONE-Modus aktiviert ist, können Sie eine Verbindung mit dem Server nur über das Workspace ONE-Webportal herstellen. Sie werden zum Workspace ONE-Webportal weitergeleitet, wenn Sie versuchen, eine Verbindung mit dem Server über HTML Access herzustellen. Nach der Verbindungsherstellung mit dem Server über das Workspace ONE-Webportal können Sie Remote-Desktops und veröffentlichte Anwendungen nur über das Workspace ONE-Webportal starten.

In der Sidebar werden nicht alle Berechtigungen angezeigt, wenn der Workspace ONE-Modus aktiviert ist. Es werden nur die aktuell ausgeführten Desktops und veröffentlichten Anwendungen angezeigt.

Die im Folgenden aufgeführten Probleme können auftreten, wenn der Workspace ONE-Modus aktiviert ist.

- Sie können über HTML Access keine Verbindung mit dem Server herstellen. Sie können möglicherweise nicht auf den Server zugreifen, oder es wird eventuell eine Meldung angezeigt, dass der Server den Empfang Ihrer Anmeldeinformationen von einer anderen Anwendung oder von einem anderen Server erwartet.
- Nach dem Start eines Remote-Desktops oder einer veröffentlichten Anwendung über das Workspace ONE-Webportal können Ihre Remote-Desktops oder veröffentlichten Anwendungen nicht in HTML Access angezeigt oder gestartet werden.

## 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.

### Voraussetzungen

- Führen Sie die unter [Vorbereiten von Verbindungsserver und Sicherheitsservern](#) 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 *Verwaltung der VMware Horizon Console*.

## Verfahren

- 1 Um eine Verbindung mit dem Server herzustellen, auf dem Sie über einen nicht authentifizierten Zugriff verfügen, öffnen Sie einen Browser und geben Sie einen Uniform Resource Identifier (URI) ein.

Verwenden Sie eine der folgenden URI-Syntaxen.

- `https://authority-part?unauthenticatedAccessEnabled=true`
- `https://authority-part?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_account`

*authority-part* ist die Serveradresse und optional eine nicht standardmäßige Portnummer. Wenn Sie eine Portnummer angeben müssen, geben Sie *server-address:port-number* ein.

*anonymous\_account* ist das Benutzerkonto für einen nicht authentifizierten Zugriff.

Verbindungen verwenden immer TLS. Der Standardport für TLS-Verbindungen ist 443. Wenn der Server nicht zur Verwendung des Standardports konfiguriert ist, muss folgendes beispielhaft dargestellte Format verwendet werden: **horizon.company.com:1443**.

- 2 (Optional) Wenn Sie im URI kein Benutzerkonto für einen nicht authentifizierten Zugriff angegeben haben, wählen Sie ein Benutzerkonto für einen nicht authentifizierten Zugriff aus dem Dropdown-Menü **Benutzerkonto** aus, falls erforderlich, und klicken Sie auf **Absenden**.

Wenn nur ein Benutzerkonto für den nicht authentifizierten Zugriff verfügbar ist, wird dieses Benutzerkonto standardmäßig ausgewählt.

Das Auswahlfenster für Anwendungen wird angezeigt.

- 3 Klicken Sie auf das Symbol der veröffentlichten Anwendung, auf die Sie zugreifen möchten.

Die veröffentlichte Anwendung wird in Ihrem Browser angezeigt. Es ist auch eine Navigations-Sidebar verfügbar. Um die Sidebar anzuzeigen, klicken Sie auf die Registerkarte links im Browser. Mit der Sidebar können Sie auf andere veröffentlichte Anwendungen zugreifen, das Fenster **Einstellungen** anzeigen, Text kopieren und einfügen und vieles mehr.

---

**Hinweis** Sie können mit nicht authentifizierten Anwendungssitzungen keine erneuten Verbindungen herstellen. Wenn Sie die Verbindung mit dem Client trennen, werden Sie automatisch von der lokalen Benutzersitzung abgemeldet.

---

## Festlegen der Zeitzone

Für Remote-Desktops oder veröffentlichte Anwendungen wird automatisch die Zeitzone Ihres lokalen Systems festgelegt.

Wenn Sie den HTML Access-Client verwenden und die Zeitzone aufgrund bestimmter Richtlinien für die Sommerzeit nicht ermittelt werden kann, müssen Sie die Zeitzone manuell festlegen.

Um die korrekte Zeitzone vor der Herstellung einer Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung manuell festzulegen, klicken Sie auf die Schaltfläche **Einstellungen** in der Symbolleiste rechts oben im Auswahlfenster für Desktops und Anwendungen. Deaktivieren Sie die Option **Zeitzone automatisch festlegen** im Fenster **Einstellungen** und wählen Sie eine Zeitzone aus dem Dropdown-Menü aus.

Der ausgewählte Wert wird als Ihre bevorzugte Zeitzone gespeichert, die bei der Herstellung einer Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung verwendet werden soll.

Wenn Sie bereits mit einem Remote-Desktop oder einer veröffentlichten Anwendung verbunden sind, kehren Sie zum Auswahlfenster für Desktops und Anwendungen zurück und ändern Sie die aktuelle Einstellung für die Zeitzone.

Die Option **Zeitzone automatisch festlegen** ist nicht im Fenster **Einstellungen**, das von der Sidebar aus aufgerufen werden kann, verfügbar.

---

**Hinweis** Wenn Sie den Chrome-Browser auf einem Android-Gerät verwenden, die Option **Zeitzone automatisch festlegen** auf **true** gesetzt ist und Sie die Zeitzone des Android-Systems ändern, wird die neue Zeitzone nicht automatisch mit dem Remote-Desktop synchronisiert. Bei diesem Problem handelt es sich um eine Beschränkung von Chrome auf dem Android-System. Um die ausgewählte Zeitzone zu synchronisieren, müssen Sie das Android-Gerät und den Chrome-Browser neu starten.

---

## Zulassen der H.264-Decodierung

Wenn Sie den Chrome-Browser verwenden, können Sie im Client eine H.264-Decodierung für Sitzungen von Remote-Desktops und veröffentlichten Anwendungen 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 Sie die H.264-Decodierung zulassen, verwendet der HTML Access-Client diese auch, sofern der Agent die H.264-Codierung unterstützt. Wenn der Agent keine H.264-Codierung unterstützt, verwendet der HTML Access-Client die JPEG/PNG-Decodierung.

Wenn Sie mit einem Remote-Desktop oder einer veröffentlichten Anwendung verbunden sind, können Sie die H.264-Decodierung zulassen, indem Sie im Fenster **Einstellungen** die Option **H.264-Decodierung zulassen** aktivieren, die in der Sidebar verfügbar ist. Sie müssen die Verbindung zum Remote-Desktop oder zur veröffentlichten Anwendung trennen und wiederherstellen, damit die neue Einstellung wirksam wird.

Wenn Sie nicht mit einem Remote-Desktop oder einer veröffentlichten Anwendung verbunden sind, können Sie rechts oben im Auswahlfenster für Desktops und Anwendungen auf die Symbolleistenschaltfläche **Einstellungen** klicken und im Fenster **Einstellungen** die Option **H.264-Decodierung zulassen** aktivieren. Die neue Einstellung wird für alle Sitzungen wirksam, die nach der Einstellungsänderung verbunden sind.

## 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.

### Verfahren

- ◆ Melden Sie sich vom Server ab und trennen Sie die Verbindung mit dem Remote-Desktop (ohne sich abzumelden) oder beenden Sie die veröffentlichte Anwendung.

Option	Aktion
Im Fenster für die Desktop- und Anwendungsauswahl vor der Herstellung einer Verbindung mit einem Remote Desktop oder einer veröffentlichten Anwendung	Klicken Sie in der rechten oberen Ecke des Fensters auf die Schaltfläche <b>Abmelden</b> der Symbolleiste.
In der Sidebar nach hergestellter Verbindung mit einem Remote Desktop oder einer veröffentlichten Anwendung	Klicken Sie oben auf der Seitenleiste auf die Symbolleistenschaltfläche <b>Abmelden</b> .

- ◆ Schließen Sie eine veröffentlichte Anwendung.

Option	Aktion
Von der veröffentlichten Anwendung	Beenden Sie die veröffentlichte Anwendung auf die übliche Weise. Klicken Sie beispielsweise in der Ecke des Fensters der veröffentlichten Anwendung auf die Schaltfläche <b>X</b> (Schließen).
In der Sidebar	Klicken Sie auf das <b>X</b> neben dem Namen der veröffentlichten Anwendung in der Liste <b>Wird ausgeführt</b> der Sidebar.

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

Option	Aktion
Von innerhalb des Remote-Desktops	Melden Sie sich über das Windows- <b>Start</b> -Menü ab.
In der Sidebar	<p>Um sich abzumelden und die Verbindung zu trennen, klicken Sie auf die Schaltfläche <b>Menü öffnen</b> neben dem Namen des Remote Desktops in der Liste <b>Wird ausgeführt</b> der Sidebar und wählen Sie <b>Abmelden</b> aus. Dateien, die auf dem Remote Desktop geöffnet sind, werden ohne vorheriges Speichern geschlossen.</p> <p>Um die Verbindung zu trennen, ohne sich abzumelden, klicken Sie auf die Schaltfläche <b>Menü öffnen</b> neben dem Namen des Remote Desktops in der Liste <b>Wird ausgeführt</b> und wählen Sie <b>Schließen</b> aus.</p> <p><b>Hinweis</b> Ein Horizon Administrator kann den Remote Desktop so konfigurieren, dass Sie beim Trennen der Verbindung automatisch abgemeldet werden. In diesem Fall werden alle geöffneten Anwendungen auf dem Remote Desktop geschlossen.</p>

# Verwenden eines Remote-Desktops oder einer veröffentlichten Anwendung

## 4

Der Client bietet eine Navigations-Sidebar mit Schaltflächen in einer Symbolleiste, mit denen Sie auf einfache Weise die Verbindung mit einem Remote-Desktop oder mit einer veröffentlichten Anwendung trennen können. Oder Sie senden das Pendant der Tastenkombination Strg+Alt+Entf durch Klicken auf eine Schaltfläche.

Dieses Kapitel enthält die folgenden Themen:

- [Funktionsunterstützungs-Matrix](#)
- [Verwenden der Sidebar](#)
- [Monitore und Bildschirmauflösung](#)
- [Verwenden des Vollbildmodus](#)
- [Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone](#)
- [Freigeben von Remote-Desktop-Sitzungen](#)
- [Kopieren und Einfügen von Text](#)
- [Übertragen von Dateien zwischen dem Client und einem Remote-Desktop oder einer veröffentlichten Anwendung](#)
- [Verwenden mehrerer Sitzungen einer veröffentlichten Anwendung von unterschiedlichen Clientgeräten aus](#)
- [Sound](#)
- [Tastenkombinationen](#)
- [Internationalisierung](#)
- [Internationale Tastaturen](#)

## Funktionsunterstützungs-Matrix

Wenn Sie über einen browserbasierten HTML Access-Client auf einen Remote-Desktop oder eine Remoteanwendung zugreifen, stehen einige Funktionen nicht zur Verfügung.

## Funktionsunterstützung für Desktops virtueller Einzelbenutzer-Maschinen

Tabelle 4-1. Über HTML Access unterstützte Funktionen

Funktion	Windows 7-Desktop	Windows 8.x-Desktop	Windows 10-Desktop	Windows Server 2008 R2-Desktop	Windows Server 2012 R2-Desktop	Windows Server 2016- oder Windows Server 2019-Desktop
RSA SecurID oder RADIUS	X	X	X	X	X	X
Einmaliges Anmelden	X	X	X	X	X	X
RDP-Anzeigeprotokoll						
PCoIP-Anzeigeprotokoll						
VMware Blast-Anzeigeprotokoll	X	X	X	X	X	X
USB-Umleitung						
Echtzeit-Audio/Video (RTAV)	X	X	X	X	X	X
Windows Media MMR						
Virtueller Druck						
Standortbasiertes Drucken	X	X	X	X	X	X
Smartcards						
Mehrere Monitore	X	X	X	X	X	X

Weitere Erläuterungen für diese Funktionen und deren Einschränkungen finden Sie im Dokument *Planung der Horizon 7-Architektur*.

## Funktionsunterstützung für sitzungsbasierte Desktops und gehostete Anwendungen auf RDS-Hosts

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

**Hinweis** Die nachfolgend dargestellte Tabelle enthält Zeilen nur für die von RDS-Hosts verfügbaren Funktionen, wenn Sie HTML Access verwenden. Weitere Funktionen sind verfügbar, wenn Sie Horizon Client nativ installiert, wie Horizon Client für Windows verwenden.

**Tabelle 4-2. Unterstützte Funktionen für HTML Access auf RDS-Hosts**

<b>Funktion</b>	<b>Windows Server 2008 R2 RDS-Host</b>	<b>Windows Server 2012 oder 2012 R2 RDS-Host</b>	<b>Windows Server 2016</b>	<b>Windows Server 2019</b>
RSA SecurID oder RADIUS	X	X	Horizon Agent 7.0.2 und höher	Horizon Agent 7.7 und höher
Einmaliges Anmelden	X	X	Horizon Agent 7.0.2 und höher	Horizon Agent 7.7 und höher
VMware Blast-Anzeigeprotokoll	X	X	Horizon Agent 7.0.2 und höher	Horizon Agent 7.7 und höher
Standortbasiertes Drucken	X (nur virtuelle Maschine)	X (nur virtuelle Maschine)	Horizon Agent 7.0.2 und höher (nur virtuelle Maschine)	Horizon Agent 7.7 und höher
Echtzeit-Audio/Video (RTAV)	Horizon Agent 7.0.2 und höher	Horizon Agent 7.0.2 und höher	Horizon Agent 7.0.3 und höher	Horizon Agent 7.7 und höher
Mehrere Monitore (nur für sitzungsbasierte Desktops)	X	X	X	X

Informationen dazu, welche Versionen jedes Gastbetriebssystems oder welche Service Packs unterstützt werden, finden Sie unter „Unterstützte Betriebssysteme für Horizon Agent“ im Dokument *Horizon 7-Installation*.

## Verwenden der Sidebar

Nachdem Sie eine Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung hergestellt haben, können Sie mit der Sidebar andere Remote-Desktops und veröffentlichte Anwendungen starten, zwischen ausgeführten Remote-Desktops und veröffentlichten Anwendungen wechseln und weitere Aktionen durchführen.

Die Sidebar wird auf der linken Seite des Fensters des Remote-Desktops oder der veröffentlichten Anwendung angezeigt. Klicken Sie auf die Registerkarte der Sidebar, um die Sidebar ein- oder auszublenden. Sie können die Registerkarte auch nach oben oder unten verschieben.

Um eine Liste mit Dokumenten anzuzeigen, die in einer ausgeführten veröffentlichten Anwendung geöffnet sind, klicken Sie in der Liste **Wird ausgeführt** auf den Erweiterungspfeil neben der veröffentlichten Anwendung.

**Hinweis** Wenn zwei Dokumente in identischen, aber separaten und auf zwei unterschiedlichen Servern gehosteten veröffentlichten Anwendungen geöffnet sind, wird die entsprechende veröffentlichte Anwendung in der Sidebar zweimal in der Liste **Wird ausgeführt** angezeigt.

Mit der Sidebar können Sie viele Aktionen durchführen.

**Tabelle 4-3. Sidebar-Aktionen**

Aktion	Prozedur
Anzeigen der Sidebar	Wenn eine veröffentlichte Anwendung oder ein Remote-Desktop geöffnet ist, klicken Sie auf die Registerkarte der Sidebar. Bei geöffneter Sidebar können Sie im Fenster der veröffentlichten Anwendung oder des Remote-Desktops weiterhin Aktionen ausführen.
Ausblenden der Sidebar	Klicken Sie auf die Registerkarte der Sidebar.
Starten einer veröffentlichten Anwendung oder eines Remote-Desktops	Klicken Sie in der Liste <b>Verfügbar</b> der Sidebar auf den Namen einer veröffentlichten Anwendung oder eines Remote-Desktops. Remote-Desktops werden zuerst aufgeführt.
Suchen nach einer veröffentlichten Anwendung oder einem Remote-Desktop	<ul style="list-style-type: none"> <li>■ Klicken Sie auf das Feld <b>Suche</b> und beginnen Sie mit der Eingabe des Namens der veröffentlichten Anwendung oder des Remote-Desktops.</li> <li>■ Um eine veröffentlichte Anwendung oder einen Remote-Desktop zu starten, klicken Sie in den Suchergebnissen auf den entsprechenden Namen.</li> <li>■ Um zur Startansicht der Sidebar zurückzukehren, tippen Sie im Suchfeld auf <b>X</b>.</li> </ul>
Erstellen einer Liste der beliebtesten veröffentlichten Anwendungen und Remote-Desktops	Klicken Sie auf den grauen Stern neben dem Namen des Remote-Desktops oder der veröffentlichten Anwendung in der Liste <b>Verfügbar</b> der Sidebar. Sie können dann mit der Schaltfläche <b>Favoriten anzeigen</b> in der Symbolleiste (Sternsymbol) neben <b>Verfügbar</b> eine Liste mit den festgelegten Favoriten aufrufen.
Wechseln zwischen veröffentlichten Anwendungen oder Remote-Desktops	Klicken Sie auf den Namen der veröffentlichten Anwendung oder des Remote-Desktops in der Liste <b>Wird ausgeführt</b> der Sidebar.
Aktivieren des Mehrfach Sitzungsmodus für veröffentlichte Anwendungen	Klicken Sie auf die Schaltfläche <b>Menü öffnen</b> in der Sidebar, dann auf <b>Einstellungen</b> und scrollen Sie nach unten zur Einstellung <b>Mehrfachstart</b> . Weitere Informationen finden Sie unter <a href="#">Verwenden mehrerer Sitzungen einer veröffentlichten Anwendung von unterschiedlichen Clientgeräten aus</a> .
Öffnen des Fensters zum Kopieren und Einfügen	Klicken Sie auf die Schaltfläche <b>Kopieren und Einfügen</b> oben auf der Sidebar. Mit dieser Schaltfläche können Sie Text in Ihre Anwendungen aus Ihrem lokalen Clientsystem und aus Ihren Anwendungen auf Ihr lokales Clientsystem kopieren. Weitere Informationen finden Sie unter <a href="#">Kopieren und Einfügen von Text</a> . In iOS Safari ist diese Schaltfläche nicht verfügbar, da die Funktion zum Kopieren und Einfügen nicht unterstützt wird.
Öffnen des Fensters „Dateiübertragung“	Klicken Sie oben in der Sidebar auf die Schaltfläche <b>Dateiübertragung</b> , um Dateien vom Remote-Desktop herunterzuladen oder zu diesem hochzuladen. Weitere Informationen dazu finden Sie unter <a href="#">Herunterladen von Dateien von einem Remote-Desktop oder einer veröffentlichten Anwendung auf das Clientsystem</a> und <a href="#">Hochladen von Dateien vom Clientsystem auf einen Remote-Desktop oder eine veröffentlichte Anwendung</a> .
Aktivieren von ⌘-A, ⌘-C, ⌘-V und ⌘-X	Diese Option wird im Fenster <b>Einstellungen</b> nur bei Verwendung eines Mac angezeigt. Klicken Sie auf die Schaltfläche <b>Menü öffnen</b> in der Symbolleiste oben auf der Sidebar und klicken Sie dann auf <b>Einstellungen</b> . Nach Aktivierung dieser Funktion wird die ⌘-Taste auf dem Mac der Strg-Taste auf dem Windows-Remote-Desktop bzw. in der Windows-Remoteanwendung zugeordnet. Beispielsweise entspricht dann das Drücken der Tastenkombination ⌘-A auf dem Mac dem Drücken von Strg+A auf dem Windows-Remote-Desktop bzw. in der Remoteanwendung.



**Tabelle 4-3. Sidebar-Aktionen (Fortsetzung)**

Aktion	Prozedur
Schließen eines ausgeführten Remote-Desktops	<p>Klicken Sie auf die Schaltfläche <b>Menü öffnen</b> neben dem Namen des Remote-Desktops in der Liste <b>Wird ausgeführt</b> der Sidebar und wählen Sie eine Aktion aus.</p> <ul style="list-style-type: none"> <li>■ Wählen Sie <b>Schließen</b> aus, um die Verbindung mit dem Remote-Desktop ohne Abmeldung von dessen Betriebssystem zu trennen. Ein Horizon-Administrator kann den Remote-Desktop so konfigurieren, dass Sie beim Trennen der Verbindung automatisch abgemeldet werden. In diesem Fall gehen nicht gespeicherte Änderungen in geöffneten Anwendungen verloren.</li> <li>■ Wählen Sie <b>Abmelden</b> aus, um sich vom Betriebssystem abzumelden und die Verbindung mit dem Remote-Desktop zu trennen. Alle nicht gespeicherten Änderungen in geöffneten Anwendungen gehen verloren.</li> </ul>
Schließen einer laufenden veröffentlichten Anwendung	<p>Klicken Sie auf das <b>X</b> neben dem Dateinamen unter dem Namen der veröffentlichten Anwendung in der Liste <b>Wird ausgeführt</b> der Sidebar. Klicken Sie auf das <b>X</b> neben dem Namen der veröffentlichten Anwendung, um die veröffentlichte Anwendung zu beenden und alle geöffneten Dateien dieser veröffentlichten Anwendung zu schließen.</p> <p>Sie werden gegebenenfalls dazu aufgefordert, die durchgeführten Änderungen in den Dateien zu speichern.</p>
Zurücksetzen eines Remote-Desktops	<p>Klicken Sie auf die Schaltfläche <b>Menü öffnen</b> neben dem Namen des Remote-Desktops in der Liste <b>Wird ausgeführt</b> der Sidebar und wählen Sie <b>Zurücksetzen</b> aus. Alle Dateien, die auf dem Remote-Desktop geöffnet sind, werden ohne vorheriges Speichern geschlossen. Sie können einen Remote-Desktop nur zurücksetzen, wenn ein Horizon-Administrator diese Funktion aktiviert hat.</p>
Neustarten eines Remote-Desktops	<p>Klicken Sie auf die Schaltfläche <b>Menü öffnen</b> neben dem Namen des Remote-Desktops in der Liste <b>Wird ausgeführt</b> der Sidebar und wählen Sie <b>Neustarten</b> aus. 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 neu starten, wenn ein Horizon-Administrator diese Funktion aktiviert hat.</p>
Zurücksetzen aller ausgeführten veröffentlichten Anwendungen	<p>Klicken Sie oben in der Sidebar auf die Symbolleistenschaltfläche <b>Menü öffnen</b>, dann auf <b>Einstellungen</b> und schließlich auf <b>Alle ausgeführten Anwendungen zurücksetzen</b>. Alle nicht gespeicherten Änderungen gehen dann verloren.</p>
Verwenden von Tastenkombinationen mit der Windows-Taste	<p>Klicken Sie auf die Schaltfläche <b>Menü öffnen</b> in der Symbolleiste oben auf der Sidebar, klicken Sie dann auf <b>Einstellungen</b> und aktivieren Sie <b>Windows-Tasten für Desktops aktivieren</b>. Weitere Informationen finden Sie unter <a href="#">Tastenkombinationen</a>.</p>
Senden von Strg+Alt+Entf zum aktuellen Arbeitsbereich	<p>Klicken Sie auf die Schaltfläche <b>Strg+Alt+Entf senden</b> in der Symbolleiste oben auf der Sidebar.</p>
Trennen einer Serververbindung	<p>Klicken Sie oben in der Sidebar auf die Symbolleistenschaltfläche <b>Menü öffnen</b> und dann auf <b>Abmelden</b>.</p>
Verwenden des Modus mit hoher Auflösung auf Computern mit einer hochauflösenden Anzeige wie Retina Macbook Pro	<p>Klicken Sie auf die Schaltfläche <b>Menü öffnen</b> in der Symbolleiste oben auf der Sidebar, klicken Sie dann auf <b>Einstellungen</b> und aktivieren Sie <b>Modus mit hoher Auflösung</b>.</p>
H.264-Decodierung zulassen	<p>(Nur Chrome) Klicken Sie oben in der Sidebar auf die Symbolleistenschaltfläche <b>Menü öffnen</b>, dann auf <b>Einstellungen</b> und aktivieren Sie <b>H.264-Decodierung zulassen</b>. Weitere Informationen finden Sie unter <a href="#">Zulassen der H.264-Decodierung</a>.</p>
Verwenden mehrerer Monitore	<p>(Nur Chrome Version 55 oder höher) Klicken Sie auf die Schaltfläche <b>Menü öffnen</b> in der Symbolleiste oben auf der Sidebar und wählen Sie <b>Anzeigeeinstellungen</b> aus. Weitere Informationen finden Sie unter <a href="#">Verwenden mehrerer Monitore</a>.</p>

**Tabelle 4-3. Sidebar-Aktionen (Fortsetzung)**

Aktion	Prozedur
Aktivieren oder Schließen der Bildschirmtastatur	(Nur für iOS Safari) Klicken Sie auf das Tastatursymbol oben auf der Sidebar. Sie können die Bildschirmtastatur auch durch Tippen auf den Bildschirm mit drei Fingern aktivieren bzw. deaktivieren.
Anzeigen der Hilfethemen	Klicken Sie oben in der Sidebar auf die Symbolleistschaltfläche <b>Menü öffnen</b> , klicken Sie auf <b>Einstellungen</b> und dann auf <b>Hilfe</b> . Sie können auch auf das Horizon-Logo oben in der Sidebar und dann auf <b>Hilfe</b> klicken.
Anzeigen des Dialogfelds „Info über VMware Horizon Client“	Klicken Sie auf die Symbolleistschaltfläche <b>Menü öffnen</b> oder auf das Horizon-Logo oben in der Sidebar und dann auf <b>Info</b> . Sie können auch auf das Horizon-Logo oben in der Sidebar klicken.
Anzeigen eines Remote-Desktops oder einer veröffentlichte Anwendung im Vollbildmodus	Klicken Sie oben in der Sidebar auf die Symbolleistschaltfläche <b>Menü öffnen</b> und dann auf <b>Vollbild</b> .
Beenden des Vollbildmodus	Klicken Sie oben in der Sidebar auf die Symbolleistschaltfläche <b>Menü öffnen</b> und dann auf <b>Vollbildmodus beenden</b> .
Senden von Esc an einen Remote-Desktop oder eine veröffentlichte Anwendung im Vollbildmodus	Klicken Sie oben in der Sidebar auf die Symbolleistschaltfläche <b>Menü öffnen</b> und dann auf <b>Esc senden</b> .

## 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.

### Verwenden mehrerer Monitore

Mithilfe eines Chrome-Browsers (Version 55 oder höher) können Sie in HTML Access mehrere Monitore für die Anzeige eines Remote-Desktop-Fensters verwenden.

Sie können Ihrem primären Monitor einen zusätzlichen Monitor hinzufügen und darin das aktuelle Remote-Desktop-Fenster anzeigen, mit dem Sie verbunden sind. Wenn Sie beispielsweise über drei Monitore verfügen, können Sie festlegen, dass das Fenster des Remote-Desktops nur auf zwei dieser drei Monitore angezeigt wird. Für die Einrichtung mehrerer Monitore müssen benachbarte Monitore ausgewählt werden. Die Monitore lassen sich nebeneinander oder übereinander anordnen.

#### Verfahren

- 1 Starten Sie HTML Access und melden Sie sich bei einem Server an.
- 2 Klicken Sie im Auswahlfenster für Desktops und Anwendungen auf das Symbol für den Remote-Desktop, auf den Sie zugreifen möchten.
- 3 Um die Sidebar anzuzeigen, klicken Sie auf die Registerkarte der Sidebar.
- 4 Klicken Sie auf die Schaltfläche **Menü öffnen** in der Symbolleiste oben auf der Sidebar und wählen Sie **Mehrere Monitore** aus.

- 5 Klicken Sie im Fenster „Mehrere Monitore“ auf **Display hinzufügen**.

---

**Hinweis** Wenn das Browserfenster „Display-Selektor“ nicht angezeigt wird, fügen Sie die FQDN-Adresse des Servers im Abschnitt „Pop-ups/Ausnahmen verwalten“ im Fenster **Inhaltseinstellungen** des Browsers hinzu.

---

- 6 Ziehen Sie das Browserfenster **Display-Selektor** in die andere Monitoranzeige (Display), die Sie verwenden möchten.

Die Meldung im Browserfenster **Display-Selektor** wird geändert und ein graues rechteckiges Symbol hinzugefügt.

- 7 Klicken Sie im Browserfenster **Display-Selektor** auf das Monitorsymbol **+**, um die Verwendung der aktuellen Monitoranzeige zu bestätigen.

In der aktuellen Monitoranzeige wird die Meldung **Auf andere Displays warten** eingeblendet und das graue Monitorsymbol im Fenster **Mehrere Monitore** Ihrer primären Anzeige grün dargestellt.

- 8 Klicken Sie im Fenster **Mehrere Monitore** auf **OK**, wenn Sie die Monitoranzeigen für die Sitzung hinzugefügt haben.

Das Fenster **Mehrere Monitore** wird geschlossen, die Meldung **Auf andere Displays warten** in der nicht primären Monitoranzeige wird ausgeblendet und das Remote-Desktop-Fenster wird angezeigt.

- 9 Um den Modus für mehrere Anzeigen zu beenden, drücken Sie auf „Esc“ und klicken Sie im Dialogfeld **Modus für mehrere Displays beenden** zur Bestätigung auf **Ja**.

---

**Hinweis** Wenn Sie die Esc-Taste im Remote-Desktop verwenden müssen, öffnen Sie die Sidebar-Registerkarte, klicken Sie auf die Schaltfläche **Menü öffnen** in der Symbolleiste oben auf der Sidebar und wählen Sie **ESC senden** aus.

---

## Festlegen der Bildschirmauflösung für Remote-Desktops und veröffentlichte Anwendungen

Wenn ein Remote-Desktop von einem Horizon-Administrator mit ausreichend Video-RAM konfiguriert wird, kann HTML Access die Größe des Remote-Desktops an die Größe des Browserfensters anpassen. Standardmäßig sind 36 MB an Video-RAM (VRAM) konfiguriert. Dies liegt über der Mindestanforderung von 16 MB, wenn Sie keine 3D-Anwendungen verwenden.

Wenn Sie einen Browser oder ein Chrome-Gerät mit einer hohen Pixeldichte-Auflösung verwenden, z. B. ein MacBook mit Retina-Display oder ein Google Chromebook Pixel, können Sie den Remote-Desktop oder die veröffentlichte Anwendung auf diese Auflösung festlegen. Aktivieren Sie die Option **Modus mit hoher Auflösung** im Fenster **Einstellungen**, das in der Sidebar verfügbar ist. Diese Option wird im Fenster **Einstellungen** nur angezeigt, wenn Sie eine hochauflösende oder normale Anzeige verwenden, die eine Skalierung größer als 100 % aufweist.

Mit der Funktion „Modus mit hoher Auflösung“ kann die Auflösung einer aktiven Remotesitzung nicht geändert werden. Sie müssen sich abmelden und erneut anmelden, damit die Funktion wirksam wird.

Um die 3D-Renderfunktion zu verwenden, müssen Sie ausreichend VRAM für jeden Remote-Desktop zuteilen.

- Die softwarebeschleunigte Grafikfunktion, die ab vSphere 5.0 oder höher zur Verfügung steht, ermöglicht es Ihnen, 3D-Anwendungen wie Windows Aero-Themen oder Google Earth zu verwenden. Für diese Funktion sind zwischen 64 MB und 128 MB VRAM erforderlich.
- Die hardwarebeschleunigte Grafikfunktion (vSGA), die mit vSphere 5.1 oder höher verfügbar ist, ermöglicht die Verwendung von 3D-Anwendungen für Entwurf, Modellierung und Multimedia. Für diese Funktion sind zwischen 64 MB und 512 MB VRAM erforderlich. Der Standardwert ist 96 MB.
- Die dedizierte vDGA-Funktion (Virtual Dedicated Graphics Acceleration, virtuelle hardwarebeschleunigte Grafikfunktion), die ab vSphere 5.5 oder höher verfügbar ist, weist eine einzige physische GPU (Graphical Processing Unit, Grafikverarbeitungseinheit) auf einem ESXi-Host einer einzelnen virtuellen Maschine zu. Verwenden Sie diese Funktion, wenn Sie hochwertige, hardwarebeschleunigte Workstation-Grafiken benötigen. Für diese Funktion sind zwischen 64 MB und 512 MB VRAM erforderlich. Der Standardwert ist 96 MB.

Wenn die 3D-Wiedergabe aktiviert ist, beträgt die Höchstzahl der Monitore 1 und die maximale Auflösung beträgt 3840 x 2160.

In gleicher Weise müssen Sie, wenn Sie einen Browser oder ein Gerät mit einer hohen Pixeldichte-Auflösung verwenden, z. B. ein MacBook mit Retina-Display oder ein Google Chromebook Pixel, jedem Remote-Desktop ausreichend VRAM zuteilen.

---

**Wichtig** Die Schätzung der für das VMware Blast-Anzeigeprotokoll benötigten Menge an VRAM ähnelt der Schätzung des benötigten VRAM für das PCoIP-Anzeigeprotokoll. Richtlinien finden Sie im Dokument *Planung der Horizon 7-Architektur* unter „Bestimmen der Speicheranforderungen für virtuelle Desktops“.

---

## 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.

Wenn die DPI-Synchronisierung deaktiviert ist, wird die Anzeigeskalierung verwendet. Die Anzeigeskalierungsfunktion skaliert den Remote-Desktop oder die veröffentlichte Anwendung entsprechend.

Wenn Sie die Auflösung manuell festlegen möchten, können Sie möglicherweise die Einstellung **Modus mit hoher Auflösung** aktivieren. Weitere Informationen hierzu finden Sie unter [Festlegen der Bildschirmauflösung für Remote-Desktops und veröffentlichte Anwendungen](#).

Die Gruppenrichtlinieneinstellung **DPI-Synchronisierung** des Agenten bestimmt, ob die DPI-Synchronisierungsfunktion aktiviert ist. Die Funktion ist standardmäßig aktiviert. Bei der DPI-Synchronisierung wird der DPI-Wert in der Remotesitzung so geändert, dass er dem DPI-Wert des Clientcomputers entspricht, wenn Sie eine Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung herstellen. Für die DPI-Synchronisierungsfunktion ist Horizon Agent 7.0.2 oder höher erforderlich.

Falls die Gruppenrichtlinieneinstellung **DPI-Synchronisierung pro Verbindung** des Agenten zusätzlich zur Gruppenrichtlinieneinstellung **DPI-Synchronisierung** aktiviert ist, wird die DPI-Synchronisierung unterstützt, wenn Sie erneut eine Verbindung mit einem Remote-Desktop herstellen. Diese Funktion ist standardmäßig deaktiviert. Für die Funktion „DPI-Synchronisierung pro Verbindung“ ist Horizon Agent 7.8 oder höher erforderlich.

Weitere Informationen zu den Gruppenrichtlinieneinstellungen **DPI-Synchronisierung** und **DPI-Synchronisierung pro Verbindung** finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

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

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

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

Für virtuelle Desktops wird die Funktion „DPI-Synchronisierung pro Verbindung“ auf folgenden Gastbetriebssystemen unterstützt:

- Windows 10, Version 1607 und höher
- Windows Server 2016 und höher, als Desktop konfiguriert

Die Funktion „DPI-Synchronisierung pro Verbindung“ wird für veröffentlichte Desktops oder veröffentlichte Anwendungen nicht unterstützt.

Im Folgenden finden Sie Tipps zur Verwendung der DPI-Synchronisierungsfunktion.

- Wenn Sie die DPI-Einstellung auf dem Clientsystem ändern, aber die DPI-Einstellung auf dem Remote-Desktop nicht geändert wird, müssen Sie sich eventuell ab- und erneut anmelden, damit Horizon Client die neue DPI-Einstellung auf dem Clientsystem erkennen kann.

- Wenn Sie eine Remotesitzung auf einem Clientsystem starten, dessen DPI-Einstellung auf einen Wert über 100 Prozent festgelegt ist, und dann die gleiche Sitzung auf einem anderen Clientsystem verwenden, dessen DPI-Einstellung auf einen anderen Wert über 100 Prozent festgelegt ist, müssen Sie sich auf dem zweiten Clientsystem eventuell von der Sitzung ab- und erneut anmelden, damit die DPI-Synchronisierung auf dem zweiten Clientsystem funktioniert.
- Obwohl Windows 10- und Windows 8.x-Systeme unterschiedliche DPI-Einstellungen auf unterschiedlichen Monitoren unterstützen, verwendet die DPI-Synchronisierungsfunktion den DPI-Wert, der auf dem Monitor des Clientsystems festgelegt wurde, in dem sich der Webbrowser befindet, mit dem die HTML Access-Clientsitzung gestartet wird. HTML Access unterstützt keine unterschiedlichen DPI-Einstellungen für verschiedene Monitore.
- Wenn Sie eine Synchronisierung mit einem anderen Monitor mit einer anderen DPI-Einstellung durchführen möchten, müssen Sie sich vom Remote-Desktop oder von der veröffentlichten Anwendung abmelden, den Webbrowser, in dem Sie die HTML Access-Clientsitzung starten, zu diesem Monitor ziehen und sich erneut beim Remote-Desktop oder bei der veröffentlichten Anwendung anmelden, um die DPI-Einstellungen zwischen dem Clientsystem und dem Remote-Desktop bzw. der veröffentlichten Anwendung aneinander anzupassen.

## Verwenden des Vollbildmodus

Sie können einen Remote-Desktop oder eine veröffentlichte Anwendung im Vollbildmodus anzeigen.

Sie können den Vollbildmodus in den folgenden Situationen nicht verwenden.

- Sie verwenden mehrere Monitore.
- Der Browser befindet sich im Vollbildmodus oder wurde mithilfe der Maus maximiert.
- Sie verwenden Safari.

### Voraussetzungen

Stellen Sie die Verbindung zum Remote-Desktop oder zur veröffentlichten Anwendung her.

### Verfahren

- ◆ Um den Remote-Desktop oder eine veröffentlichte Anwendung im Vollbildmodus anzuzeigen, klicken Sie auf die Schaltfläche **Menü öffnen** oben in der Sidebar und dann Sie auf **Vollbild**.
- ◆ Um den Vollbildmodus zu beenden, klicken Sie auf die Schaltfläche **Menü öffnen** oben in der Sidebar und dann auf **Vollbildmodus beenden**.

Alternativ drücken Sie die Esc-Taste auf der Tastatur des Clientsystems.

## Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone

Mit der Echtzeit-Audio/Video-Funktion können Sie die Webcam oder das Mikrofon des Clientcomputers auf einem Remote-Desktop oder in einer veröffentlichten Anwendung verwenden. Echtzeit-Audio/Video

ist mit Standard-Konferenzanwendungen und browserbasierten Videoanwendungen kompatibel und unterstützt standardmäßige Webcams, USB-Audiogeräte und analoge Audioeingänge.

Echtzeit-Audio/Video wird nur in Chrome, Microsoft Edge und Firefox unterstützt. Die Standardvideoauflösung lautet 320 x 240 Pixel. Die standardmäßigen Echtzeit-Audio/Video-Einstellungen funktionieren problemlos mit den meisten Webcam- und Audioanwendungen.

Informationen zum Ändern der Echtzeit-Audio/Video-Einstellungen finden Sie im *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*-Dokument unter „Konfigurieren von Echtzeit-Audio/Video-Einstellungen“.

Wenn ein Remote-Desktop oder eine veröffentlichte Anwendung mit der Webcam oder dem Mikrofon des Clientcomputers verbunden ist, bevor sie diese verwenden können, fragt der Browser eventuell nach der entsprechenden Berechtigung. Unterschiedliche Browser verhalten sich unterschiedlich.

- Microsoft Edge fragt jedes Mal nach der Berechtigung. Dieses Verhalten können Sie nicht ändern. Weitere Informationen finden Sie unter <https://blogs.windows.com/msedgedev/2015/05/13/announcing-media-capture-functionality-in-microsoft-edge>.
- Firefox fragt jedes Mal nach der Berechtigung. Dieses Verhalten können Sie jedoch ändern. Weitere Informationen finden Sie unter <https://support.mozilla.org/en-US/kb/permissions-manager-give-ability-store-passwords-set-cookies-more?redirectlocale=en-US&redirectslug=how-do-i-manage-website-permissions>.
- Chrome fragt beim ersten Mal nach der Berechtigung. Wenn Sie die Verwendung des Geräts zulassen, wird Chrome nicht mehr nach einer Berechtigung fragen.

Wenn ein Remote-Desktop mit der Webcam oder dem Mikrofon des Clientcomputers verbunden ist, wird oben in der Sidebar ein Symbol für jedes Gerät angezeigt. Über dem Gerätesymbol in der Sidebar taucht ein rotes Fragezeichen auf, das auf eine Berechtigungsanforderung hinweist. Wenn Sie die Verwendung eines Geräts zulassen, verschwindet das rote Fragezeichen. Wenn Sie eine Berechtigungsanforderung zurückweisen, verschwindet das Gerätesymbol.

Wenn in einer Sitzung eines Remote-Desktops oder einer veröffentlichten Anwendung Echtzeit-Audio/Video verwendet wird und Sie eine Verbindung zu einem zweiten Remote-Desktop oder einer zweiten veröffentlichten Anwendung herstellen möchten und eine Sicherheitswarnung angezeigt wird (z. B. wenn kein gültiges Zertifikat installiert wurde), kann es zum Ausfall von Echtzeit-Audio/Video in der ersten Sitzung kommen, wenn Sie die Warnung ignorieren und sich mit dem zweiten Remote-Desktop oder der zweiten veröffentlichten Anwendung verbinden.

## 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 beitrifft, 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 7*. Informationen zur Aktivierung der Funktion „Session Collaboration“ für eine Farm erhalten Sie im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*. Informationen zur Verwendung von Gruppenrichtlinieneinstellungen zur Konfiguration der Funktion „Session Collaboration“ finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Informationen zur Aktivierung der Funktion „Session Collaboration“ für Linux-Desktops finden Sie im Dokument *Einrichten von Horizon 7 for Linux-Desktops*.

## 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 beitrifft, 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 4.7 oder höher für Windows, Mac oder Linux installiert haben oder HTML Access 4.7 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
<b>E-Mail</b>	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.
<b>Chat</b>	(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.
<b>Link kopieren</b>	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.

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 7* unter der Gruppenrichtlinieneinstellung **Übergabe der Kontrolle an Kollaboratoren zulassen** nach. Bei Linux-Remote-Desktops sehen Sie im Dokument *Einrichten von Horizon 7 for Linux-Desktops* 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
<b>Einladung widerrufen oder Teilnehmer entfernen</b>	Klicken Sie in der Spalte „Status“ auf <b>Entfernen</b> .
<b>Kontrolle an Sitzungsteilnehmer übergeben</b>	Nachdem ein Teilnehmer der Sitzung beigetreten ist, setzen Sie die Umschaltoption in der Spalte „Steuerung“ auf <b>Ein</b> . 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 <b>Aus</b> setzt oder auf die Schaltfläche <b>Steuerung zurückgeben</b> klickt.

Option	Aktion
<b>Teilnehmer hinzufügen</b>	Klicken Sie auf <b>Teilnehmer hinzufügen</b> .
<b>Gemeinsame Sitzung beenden</b>	<p>Klicken Sie auf <b>Teilnahme beenden</b>. Die Verbindung mit allen aktiven Teilnehmern wird getrennt.</p> <p>Bei Windows-Remote-Desktops können Sie die gemeinsame Sitzung auch beenden, indem Sie auf die Schaltfläche <b>Beenden</b> neben dem Symbol <b>VMware Horizon Session Collaboration</b> klicken. Die Schaltfläche <b>Beenden</b> ist bei Linux-Remote-Desktops nicht verfügbar.</p>

## 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.

- Echtzeit-Audio/Video (RTAV)
- Standortbasiertes Drucken
- 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 4.7 für Windows, Mac oder Linux installiert sein oder HTML Access 4.7 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 in der Seitenleiste auf **Schließen**.

## Kopieren und Einfügen von Text

Sie können sowohl einfachen als auch HTML-Rich-Text vom Clientgerät in einen und von einem Remote-Desktop bzw. von einer oder in eine veröffentlichte Anwendung kopieren und einfügen. Ein Horizon Administrator kann 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 kann die Möglichkeit zum Kopieren und Einfügen durch die Verwendung von Gruppenrichtlinieneinstellungen konfigurieren, die View Agent oder Horizon Agent auf den Remote-Desktops zugeordnet sind. Weitere Informationen finden Sie unter [Gruppenrichtlinieneinstellungen für HTML Access](#).

Wenn Sie Rich-Text kopieren und einfügen, gelten die folgenden Einschränkungen.

- Das Kopieren und Einfügen von Bildern wird nicht unterstützt.
- Wenn Sie Rich-Text aus dem Client-Gerät kopieren und das Ziel die Anwendung WordPad ist, wird nur der einfache Text kopiert und eingefügt.
- Das Kopieren und Einfügen von Rich-Text wird bei Verwendung von HTML Access bei den Browsern Internet Explorer (IE), Microsoft Edge oder Safari nicht unterstützt. Sie müssen das Fenster **Kopieren und Einfügen** verwenden. Siehe [Verwenden des Fenster „Kopieren und Einfügen“](#).
- Ein Horizon-Administrator kann mithilfe von Gruppenrichtlinieneinstellungen die Zwischenablageformate für das Kopieren/Einfügen beschränken. Da HTML Access nur die Übertragung von Text in der Zwischenablage unterstützt, funktionieren nur die Textfilter mit HTML Access. Informationen zu Filterrichtlinieneinstellungen für das Zwischenablageformat finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Wenn Sie HTML Access mit einem Chrome- oder Firefox-Browser verwenden, finden Sie im Folgenden Tipps für die Verwendung der Zwischenablagefunktion.

- Nachdem Sie zum ersten Mal eine Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung hergestellt haben, wird das Dialogfeld mit dem Benutzerhandbuch für die Zwischenablage angezeigt. Klicken Sie auf **OK**, um das Dialogfeld zu schließen und nicht mehr erneut anzuzeigen.

- Standardmäßig ist das Symbol der Zwischenablage  in der Sidebar aktiviert und wird grau angezeigt.
  - Wenn das Symbol der Zwischenablage beim Kopieren von Text von einem Remote-Desktop oder einer veröffentlichten Anwendung ausgewählt ist, wird ein Dialogfeld angezeigt, in dem Sie um Ihre Bestätigung gebeten werden, dass Text in die Zwischenablage des lokalen Clientsystems kopiert werden soll. Klicken Sie auf **OK**.
  - Wenn das Symbol der Zwischenablage deaktiviert ist, wird das Dialogfeld zur Bestätigung nicht angezeigt, wenn Sie Text vom Remote-Desktop oder einer veröffentlichten Anwendung in die Zwischenablage des lokalen Clientsystems kopieren.
- Wenn Sie den Mauszeiger auf dem Symbol der Zwischenablage auf der Sidebar positionieren, wird in der QuickInfo erläutert, was die Funktion für die Zwischenablage bewirkt.

In der Zwischenablage kann maximal 1 MB an Daten für alle Kopier- und Einfügevorgänge gespeichert werden. Beträgt die Gesamtmenge von einfachen Text- und RTF-Daten weniger als die maximale Größe der Zwischenablage, wird der formatierte Text eingefügt. Es ist häufig der Fall, dass der Rich-Text nicht gekürzt werden kann, sodass er verworfen und nur der einfache 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 einzufügen, versuchen Sie, geringere Teilmengen zu speichern und einzufügen.

Sie können keine Grafiken kopieren und einfügen. Sie können außerdem keine Dateien zwischen einem Remote-Desktop und dem Dateisystem auf dem Clientcomputer kopieren und einfügen.

---

**Hinweis** Die Funktion zum Kopieren und Einfügen wird in iOS Safari und auf Android-Geräten nicht unterstützt.

---

## Verwenden des Fenster „Kopieren und Einfügen“

Für das Kopieren und Einfügen von Text aus den Browsern Internet Explorer (IE), Microsoft Edge oder Safari müssen Sie die Schaltfläche **Kopieren und Einfügen** oben in der Sidebar verwenden, um das Fenster **Kopieren und Einfügen** anzuzeigen.

Dieser Vorgang beschreibt, wie Sie das Fenster **Kopieren und Einfügen** verwenden können, um Text aus den Browsern IE, Edge oder Safari auf dem lokalen Clientsystem in eine Anwendung auf einem Remote-Desktop oder in eine veröffentlichte Anwendung zu kopieren, und wie Sie Text von einer Anwendung auf einem Remote-Desktop oder von einer veröffentlichten Anwendung auf das Clientsystem kopieren können.

Wenn Sie Text zwischen veröffentlichten Anwendungen oder zwischen Remote-Desktops kopieren und einfügen, können Sie einfach wie gewohnt vorgehen und benötigen dafür nicht das Fenster **Kopieren und Einfügen**.

Wenn Sie die Browser IE, Edge oder Safari verwenden, ist das Fenster **Kopieren und Einfügen** nur erforderlich, um die Zwischenablage auf dem lokalen System mit der Zwischenablage auf dem Remote-Computer zu synchronisieren.

Der Text im Fenster **Kopieren und Einfügen** zeigt eine der folgenden Meldungen an, um anzugeben, in welche Richtung Sie Inhalt kopieren und einfügen können.

- Verwenden Sie dieses Fenster zum Kopieren und Einfügen von Inhalt zwischen Ihrem lokalen Client und dem Remote-Desktop bzw. der –Anwendung.
- Verwenden Sie das Fenster zum Kopieren und Einfügen von Inhalt von Ihrem lokalen Client zum Remote-Desktop bzw. zur –Anwendung.
- Verwenden Sie das Fenster zum Kopieren und Einfügen von Inhalt von Ihrem Remote-Desktop bzw. Ihrer Remote-Anwendung zum lokalen Client.

---

**Hinweis** Die standardmäßige Gruppenrichtlinieneinstellung für die Zwischenablageumleitung ermöglicht Ihnen nur, Text aus dem Clientsystem zu kopieren und auf einem Remote-Desktop oder in eine veröffentlichte Anwendung einzufügen. Damit Sie Text von einem Remote-Desktop oder einer veröffentlichten Anwendung auf das Clientsystem kopieren können, muss die Gruppenrichtlinieneinstellung in beide Richtungen aktiviert sein.

---

### Voraussetzungen

Wenn Sie mit einem Mac arbeiten, stellen Sie sicher, dass die Zuordnung der Befehlstaste ⌘ (command, cmd) zur Windows-Strg-Taste aktiviert wurde, wenn Sie Tastenkombinationen für das Auswählen, Kopieren und Einfügen von Text verwenden. Klicken Sie auf die Schaltfläche **Einstellungenfenster öffnen** in der Symbolleiste der Sidebar und aktivieren Sie **⌘-A**, **⌘-C**, **⌘-V** und **⌘-X aktivieren**. Wenn Sie einen Mac verwenden, wird diese Option nur im Fenster **Einstellungen** angezeigt.

Ein Horizon-Administrator muss die Standardrichtlinie beibehalten, die es Benutzern ermöglicht, Text aus ihren Clientsystemen zu kopieren und in ihren Remote-Desktops und veröffentlichten Anwendungen einzufügen, oder eine andere Richtlinie konfigurieren, die das Kopieren und Einfügen zulässt. Weitere Informationen finden Sie unter [Gruppenrichtlinieneinstellungen für HTML Access](#).

### Verfahren

- ◆ Führen Sie diese Schritte aus, um Text aus dem Clientsystem in eine Anwendung auf einem Remote-Desktop oder aus dem Clientsystem in eine veröffentlichte Anwendung zu kopieren.

- a Kopieren Sie den Text in der lokalen Clientanwendung.
- b Öffnen Sie in HTML Access die Sidebar und klicken Sie oben in der Sidebar auf **Kopieren und Einfügen**.

Das Fenster **Kopieren und Einfügen** wird angezeigt. Sollte in diesem Fenster noch Text von einem früheren Kopiervorgang enthalten sein, wird dieser durch das Einfügen des neu kopierten Textes überschrieben.

- c Um den Text in das Fenster **Kopieren und Einfügen** einzufügen, drücken Sie STRG+V auf einem Windows-System oder Befehlstaste-V auf einem Mac.

Es wird kurz die folgende Meldung angezeigt: „Die Remote-Zwischenablage wurde synchronisiert.“

- d Klicken Sie in der Anwendung an die Stelle, an der Sie den Text einfügen möchten, und drücken Sie STRG+V.

Der Text wird in die Anwendung eingefügt.

- ◆ Führen Sie diese Schritte aus, um Text aus einer Anwendung auf einem Remote-Desktop in das Clientsystem oder aus einer veröffentlichten Anwendung in das Clientsystem zu kopieren.

- a Kopieren Sie den Text in der Anwendung.
- b Öffnen Sie in HTML Access die Sidebar und klicken Sie oben in der Sidebar auf **Kopieren und Einfügen**.

Das Fenster **Kopieren und Einfügen** wird angezeigt. Dort ist der eingefügte Text zu sehen. Es wird kurz die folgende Meldung angezeigt: „Die Remote-Zwischenablage wurde synchronisiert.“

- c Um den Text wieder zu kopieren, klicken Sie in das Fenster **Kopieren und Einfügen** und drücken Sie STRG+C auf einem Windows-System oder Befehlstaste-C auf einem Mac.

Der Text wird dabei nicht ausgewählt und kann auch von Ihnen nicht ausgewählt werden. Es wird kurz die folgende Meldung angezeigt: „Aus der Zwischenablage kopiert.“

- d Klicken Sie auf dem Clientsystem an die Stelle, an der Sie den Text einfügen möchten, und drücken Sie STRG+V.

Der Text wird in die Anwendung auf dem Clientsystem eingefügt.

## Übertragen von Dateien zwischen dem Client und einem Remote-Desktop oder einer veröffentlichten Anwendung

Mit der Funktion zur Dateiübertragung können Sie Dateien zwischen dem Clientsystem und einem Remote-Desktop oder einer veröffentlichten Anwendung übertragen.

Ein Horizon-Administrator kann die Fähigkeit zum Zulassen, Verweigern oder unidirektionalen Erlauben der Übertragung von Dateien konfigurieren, indem er die Gruppenrichtlinieneinstellung **Dateiübertragung konfigurieren** für VMware Blast ändert. Diese Gruppenrichtlinieneinstellung hat die folgenden Werte.

- Wenn der Wert **Upload und Download deaktiviert** ausgewählt ist, ist die Schaltfläche für die **Dateiübertragung** deaktiviert.
- Wenn der Wert **Nur Dateiapload aktiviert** ausgewählt ist (Standardeinstellung), wird nur die Registerkarte **Hochladen** im Fenster **Dateien übertragen** angezeigt.
- Wenn der Wert **Nur Dateidownload aktiviert** ausgewählt ist, wird nur die Registerkarte **Herunterladen** im Fenster **Dateien übertragen** angezeigt.

Wenn die Gruppenrichtlinieneinstellung **Zwischenablagenumleitung konfigurieren** vom Server zum Client deaktiviert ist, ist der Dateidownload ebenfalls deaktiviert.

Weitere Informationen zu diesen Gruppenrichtlinieneinstellungen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Für diese Funktion gelten die im Folgenden aufgeführten Einschränkungen.


- Sie können Dateien mit bis zu 500 MB herunterladen und Dateien mit bis zu 2 GB hochladen.
- Das Herunterladen einer Datei, die größer als 300 MB ist, ist für die 32-Bit-Version von Internet Explorer 11 nicht möglich. Führen Sie zum Beheben des Problems Internet Explorer 11 im 64-Bit-Modus aus.
- Sie können Ordner oder Dateien mit einer Größe von 0 weder herunter- noch hochladen.
- Safari für iOS und Safari 8 unterstützen weder Up- noch Downloads. Safari 9 und höher unterstützen keinen Download.
- Wenn eine Dateiübertragung in einer Remotesitzung läuft, Sie eine Verbindung mit einer zweiten Remotesitzung herstellen und eine Sicherheitswarnung angezeigt wird, wird die Dateiübertragung in der ersten Sitzung abgebrochen, wenn Sie die Warnung ignorieren und die Verbindung mit der zweiten Remotesitzung weiter herstellen.
- Wenn Sie eine Datei mit Internet Explorer 11 oder mit Chrome auf einem Chromebook hochladen, wenn Sie Ordner, Dateien mit einer Größe von 0 oder Dateien, die größer als 2 GB sind, per Drag & Drop verschieben, erhalten Sie erwartungsgemäß eine Fehlermeldung. Nach dem Verwerfen der Fehlermeldung können übertragbare Dateien nicht weiter gezogen und abgelegt werden.
- Sie können diese Funktion nicht mit Linux-Remote-Desktops oder Android-Geräten verwenden.

## Herunterladen von Dateien von einem Remote-Desktop oder einer veröffentlichten Anwendung auf das Clientsystem

Sie können Dateien von einem Remote-Desktop oder einer veröffentlichten Anwendung auf das Clientsystem herunterladen.

Ein Horizon-Administrator kann diese Funktion deaktivieren. Weitere Informationen finden Sie unter [Übertragen von Dateien zwischen dem Client und einem Remote-Desktop oder einer veröffentlichten Anwendung](#).

### Verfahren

- 1 Stellen Sie die Verbindung zum Remote-Desktop oder zur veröffentlichten Anwendung her.
- 2 Um die Sidebar anzuzeigen, klicken Sie auf die Registerkarte der Sidebar.
- 3 Klicken Sie oben auf der Seitenleiste auf das Symbol für die Dateiübertragung .
- Das Fenster **Dateien übertragen** wird angezeigt.
- 4 Klicken Sie im Fenster **Dateien übertragen** auf **Herunterladen**.
- 5 Wählen Sie eine oder mehrere Dateien zum Herunterladen aus.



- 6 Drücken Sie Strg+C, um die Dateiübertragung zu starten.

Die Dateien werden im Fenster **Dateien übertragen** auf der Registerkarte **Herunterladen** angezeigt.

- 7 Klicken Sie auf das Downloadsymbol (Pfeil nach unten), um die Dateien auf das Clientsystem herunterzuladen.

Die Dateien werden auf dem Clientsystem im Ordner Downloads angezeigt.


## Hochladen von Dateien vom Clientsystem auf einen Remote-Desktop oder eine veröffentlichte Anwendung

Sie können Dateien vom Clientsystem auf einen Remote-Desktop oder eine veröffentlichte Anwendung hochladen.

Ein Horizon-Administrator kann diese Funktion deaktivieren. Weitere Informationen finden Sie unter [Übertragen von Dateien zwischen dem Client und einem Remote-Desktop oder einer veröffentlichten Anwendung](#).

### Verfahren

- 1 Stellen Sie die Verbindung zum Remote-Desktop oder zur veröffentlichten Anwendung her.
- 2 Um die Sidebar anzuzeigen, klicken Sie auf die Registerkarte der Sidebar.

- 3 Klicken Sie oben auf der Seitenleiste auf das Symbol für die Dateiübertragung .

Das Fenster **Dateien übertragen** wird angezeigt.

- 4 Wenn Sie Dateien hochladen möchten, können Sie diese per Drag & Drop auf die Registerkarte **Hochladen** im Fenster **Dateien übertragen** verschieben oder auf **Dateien auswählen** auf der Registerkarte **Hochladen** klicken und die Dateien zum Hochladen auswählen.

Die hochgeladenen Dateien werden im Ordner Dokumente angezeigt.

## Verwenden mehrerer Sitzungen einer veröffentlichten Anwendung von unterschiedlichen Clientgeräten aus

Wenn der Mehrfach Sitzungsmodus 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 Mehrfach Sitzungsmodus 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 Mehrfach Sitzungsmodus hingegen deaktiviert ist (Einzelsitzungsmodus), wird die Sitzung der veröffentlichten Anwendung auf Client A unterbrochen und auf Client B wiederhergestellt.

Für die Funktion „Mehrfach Sitzungsmodus“ gelten die im Folgenden aufgeführten Einschränkungen.

- Der Mehrfach Sitzungsmodus funktioniert nicht bei Anwendungen, die nicht mehrere Instanzen unterstützen, beispielsweise Skype for Business.

- Wenn die Anwendungssitzung unterbrochen wird, während Sie eine veröffentlichte Anwendung im Mehrfach Sitzungsmodus verwenden, werden Sie automatisch abgemeldet, und alle nicht gespeicherten Daten gehen verloren.

### Voraussetzungen

Ein Horizon Administrator muss den Mehrfach Sitzungsmodus für den Anwendungspool aktivieren. Benutzer können den Mehrfach Sitzungsmodus für eine veröffentlichte Anwendung nur dann ändern, wenn ein Horizon Administrator es zulässt. Siehe *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*. Diese Funktion erfordert Horizon 7 Version 7.7 oder höher.

### Verfahren

- 1 Stellen Sie eine Verbindung mit einem Server her.
- 2 Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf die Schaltfläche **Einstellungen** in der Symbolleiste, scrollen Sie nach unten zur Einstellung **Mehrfachstart** und klicken Sie auf **Festlegen**.

Wenn Sie zuvor einen Remote-Desktop oder eine veröffentlichte Anwendung gestartet haben, können Sie alternativ auf die Schaltfläche **Menü öffnen** in der Symbolleiste klicken, auf **Einstellungen** klicken und nach unten zur Einstellung **Mehrfachstart** scrollen. Wenn keine veröffentlichten Anwendungen zur Verwendung im Mehrfach Sitzungsmodus verfügbar sind, wird die Einstellung **Mehrfachstart** abgeblendet.

- 3 Wählen Sie die veröffentlichten Anwendungen aus, die Sie im Mehrfach Sitzungsmodus verwenden möchten, und klicken Sie auf **OK**.

Wenn ein Horizon Administrator den Mehrfach Sitzungsmodus für eine veröffentlichte Anwendung erzwungen hat, können Sie diese Einstellung nicht ändern.

## Sound

Sie können auf Remote-Desktops und in veröffentlichten Anwendungen Audioinhalte wiedergeben, wobei einige Einschränkungen zu beachten sind.

Standardmäßig ist die Audiowiedergabe für Remote-Desktops und veröffentlichte Anwendungen aktiviert, allerdings kann ein Horizon-Administrator eine Richtlinie festlegen, um die Audiowiedergabe zu deaktivieren.

Die folgenden Einschränkungen gelten für die Audiowiedergabe auf Remote-Desktops und in veröffentlichten Anwendungen.

- Verwenden Sie zum Erhöhen der Lautstärke die Sound-Steuerung auf dem Clientsystem und nicht die des Remote-Desktops.
- Gelegentlich kann es zu einer fehlerhaften Synchronisierung zwischen Audio und Video kommen.
- Bei starkem Netzwerkverkehr oder beim Durchführen vieler Aufgaben des Browsers kann es zu einer eingeschränkten Audioqualität kommen. Einige Browser eignen sich in dieser Hinsicht besser als andere.

## Tastenkombinationen

Einige Tastenkombinationen können nicht an einen Remote-Desktop oder eine veröffentlichte Anwendung gesendet werden, unabhängig von der von Ihnen verwendeten Sprache.

Webbrowser ermöglichen es, bestimmte Tasteneingaben und Tastenkombinationen sowohl an das Clientsystem als auch an das Zielsystem zu senden. Für andere Tasteneingaben und Tastenkombinationen wird die Eingabe nur lokal verarbeitet und nicht an das Zielsystem gesendet. Die Tastenkombinationen, die auf Ihrem System funktionieren, richten sich nach der Browsersoftware, dem Clientbetriebssystem und den Spracheinstellungen.

---

**Hinweis** Wenn Sie mit einem Mac arbeiten, können Sie die Befehlstaste ⌘ (command, cmd) der Windows-Strg-Taste zuordnen, wenn Sie Tastenkombinationen für das Auswählen, Kopieren und Einfügen von Text verwenden. Um diese Funktion zu aktivieren, klicken Sie auf die Symbolleistenschaltfläche **Einstellungenfenster öffnen** der Sidebar und aktivieren Sie **⌘-A, ⌘-C, ⌘-V und ⌘-X aktivieren**. Die Option „⌘-A, ⌘-C, ⌘-V und ⌘-X aktivieren“ erscheint im Fenster **Einstellungen** nur bei Verwendung eines Mac-Clientsystems.

---

Die folgenden Tasteneingaben und Tastenkombinationen funktionieren häufig nicht bei Remote-Desktops.

- Strg+T
- Strg+W
- Strg+N
- Befehlstaste
- Alt+Enter
- Strg+Alt+*beliebige\_Taste*

---

**Wichtig** Für die Eingabe von Strg+Alt+Entf verwenden Sie die Symbolleistenschaltfläche **Strg+Alt+Entf senden** oben in der Sidebar.

---

- Feststelltaste+*Zusatzaste* (z. B. Alt oder Umschalttaste)
- Funktionstasten auf einem Chromebook
- Windows-Tastenkombinationen

Wenn Sie die Windows-Taste für Remote-Desktops aktivieren, funktionieren die folgenden Windows-Tastenkombinationen auf Remote-Desktops. Um diese Taste zu aktivieren, klicken Sie auf die Symbolleistenschaltfläche **Einstellungenfenster öffnen** der Sidebar und aktivieren Sie **Windows-Tasten für Desktops aktivieren**.

---

**Wichtig** Nachdem Sie **Windows-Tasten für Desktops aktivieren** gedrückt haben, drücken Sie Strg+Win (auf Windows-Systemen), ctrl+⌘ (auf Macs) oder Strg+Suche (auf Chromebooks), um die Windows-Taste zu simulieren.

---

Diese Tastenkombinationen funktionieren nicht für veröffentlichte Anwendungen. Diese Tastenkombinationen funktionieren für Remote-Desktops und veröffentlichte Anwendungen unter Windows Server 2008 R2, Windows Server 2012 R2 und Windows Server 2016.

Einige Tastenkombinationen, die auf Remote-Desktops mit Windows 8.x- oder Windows Server 2012 R2-Betriebssystem funktionieren, funktionieren nicht auf Remote-Desktops mit Windows 7-, Windows Server 2008 R2- oder Windows 10-Betriebssystem.

**Tabelle 4-4. Windows-Tastenkombinationen für Windows 10-Remote-Desktops und Windows Server 2016-Remote-Desktops**

Schlüssel	Aktion	Einschränkungen
Windows-Taste	Öffnet oder schließt „Start“.	
Win+A	Öffnet das Wartungscenter.	
Win+E	Öffnet den Datei-Explorer.	
Win+G	Öffnet die Spieleleiste, wenn ein Spiel geöffnet ist.	
Win+H	Öffnet den Charm „Teilen“	
Win+I	Öffnet den Charm „Einstellungen“	
Win+K	Öffnet die Aktion „Schnelle Verbindung“.	
Win+M	Minimiert alle Fenster.	
Win+R	Öffnet das Dialogfeld „Ausführen“.	
Win+S	Öffnet die Suche.	
Win+X	Öffnet das Menü <b>Quicklink</b> .	
Win+, (Komma)	Ermöglicht eine temporäre Vorschau am Remote-Desktop.	
Win+Pause	Stellt das Dialogfeld für die Systemeigenschaften dar.	Auf Chromebooks oder Macs ist keine Pause-Taste verfügbar.
Win+Umschalt+M	Stellt minimierte Fenster auf dem Remote-Desktop wieder her.	Diese Tastenkombination kann nicht in Safari verwendet werden.
Win+Alt+Num	Öffnet den Remote-Desktop und die Sprungliste für die App, die an der durch die Ziffer angegebenen Position an der Taskleiste angeheftet ist.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Enter	Öffnet die Sprachausgabe.	

**Tabelle 4-5. Windows-Tastenkombinationen für Windows 8.x- und Windows Server 2012 R2-Remote-Desktops**

Schlüssel	Aktion	Einschränkungen
Win+F1	Öffnet die Windows-Hilfe und den Windows-Support.	Diese Tastenkombination kann nicht in Safari verwendet werden.
Windows-Taste	Blendet das Startfenster ein oder aus.	
Win+B	Setzt den Fokus auf den Infobereich.	
Win+C	Öffnet den Charms-Bereich	

**Tabelle 4-5. Windows-Tastenkombinationen für Windows 8.x- und Windows Server 2012 R2-Remote-Desktops (Fortsetzung)**

Schlüssel	Aktion	Einschränkungen
Win+D	Blendet den Remote-Desktop ein und aus.	Diese Tastenkombination kann nicht in Safari verwendet werden. Drücken von ⌘-D auf einem Mac.
Win+E	Öffnet den Datei-Explorer.	
Win+H	Öffnet den Charm „Teilen“	
Win+I	Öffnet den Charm „Einstellungen“	
Win+K	Öffnet den Charm „Geräte“	
Win+M	Minimiert alle Fenster.	
Win+Q	Öffnet den Charm „Suche“, wenn Sie überall oder in der geöffneten App (wenn diese die App-Suche unterstützt) suchen möchten.	
Win+R	Öffnet das Dialogfeld „Ausführen“.	
Win+S	Öffnet den Charm „Suche“, wenn Sie in Windows und im Web suchen möchten.	
Win+X	Öffnet das Menü <b>Quicklink</b> .	
Win+Z	Zeigt die in der App verfügbaren Befehle an.	
Win+, (Komma)	Zeigt vorübergehend den Remote-Desktop an, solange Sie diese Tasten drücken.	Diese Tastenkombination kann nicht für Windows 2012 R2-Betriebssysteme verwendet werden.
Win+Pause	Zeigt das Dialogfeld für die Systemeigenschaften an.	Chromebooks und Macs verfügen nicht über eine Pause-Taste.
Win+Umschalt+M	Stellt minimierte Fenster auf dem Remote-Desktop wieder her.	Diese Tastenkombination kann nicht in Safari verwendet werden. Drücken von ⌘-D auf einem Mac.
Win+Alt+Num	Öffnet den Remote-Desktop und die Sprungliste für die App, die an der durch die Ziffer angegebenen Position an der Taskleiste angeheftet ist.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach oben	Maximiert das Fenster.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach unten	Entfernt die aktuelle App vom Bildschirm oder minimiert das Fenster des Remote-Desktops.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach links	Maximiert das Fenster der App oder des Remote-Desktops zur linken Seite des Bildschirms.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach rechts	Maximiert das Fenster der App oder des Remote-Desktops zur rechten Seite des Bildschirms.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pos1	Minimiert alle Fenster bis auf das Fenster des aktiven Remote-Desktops (durch nochmaliges Drücken werden alle Fenster wiederhergestellt).	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden.
Win+Umschalt+Pfeil nach oben	Zieht das Fenster des Remote-Desktops nach oben und unten auf.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.

**Tabelle 4-5. Windows-Tastenkombinationen für Windows 8.x- und Windows Server 2012 R2-Remote-Desktops (Fortsetzung)**

Schlüssel	Aktion	Einschränkungen
Win+Umschalt+Pfeil nach unten	Stellt das Fenster des Remote-Desktops vertikal unter Beibehaltung der Breite wieder her, nachdem es mit der Tastenkombination „Win+Umschalt+Pfeil nach oben“ aufgezogen wurde, oder minimiert das Fenster des aktiven Remote-Desktops.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Enter	Öffnet die Sprachausgabe.	

**Tabelle 4-6. Windows-Tastenkombinationen für Windows 7- und Windows Server 2008 R2-Remote-Desktops**

Schlüssel	Aktion	Einschränkungen
Windows-Taste	Öffnet oder schließt das <b>Startmenü</b> .	
Win+Pause	Zeigt das Dialogfeld für die Systemeigenschaften an.	Chromebooks und Macs verfügen nicht über eine Pause-Taste.
Win+D	Blendet den Remote-Desktop ein und aus.	Diese Tastenkombination kann nicht in Safari verwendet werden. Drücken von ⌘-D auf einem Mac.
Win+M	Minimiert alle Fenster.	
Win+E	Öffnet den Ordner Computer.	
Win+R	Öffnet das Dialogfeld „Ausführen“.	
Win+Pfeil nach oben	Maximiert das Fenster.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach unten	Minimiert das Fenster.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach links	Maximiert das Fenster der App oder des Remote-Desktops zur linken Seite des Fensters.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach rechts	Maximiert das Fenster der App oder des Remote-Desktops zur rechten Seite des Fensters.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pos1	Minimiert alle Fenster bis auf das Fenster des aktiven Remote-Desktops.	Diese Tastenkombination kann nicht in Safari verwendet werden.
Win+Umschalt+Pfeil nach oben	Zieht das Fenster des Remote-Desktops nach oben und unten auf.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+G	Wechselt der Reihe nach zu den ausgeführten Remote-Desktop-Minianwendungen.	
Win+U	Öffnet das „Center für erleichterte Bedienung“.	

## Internationalisierung

Die Benutzeroberfläche und die Dokumentation sind in den Sprachen Englisch, Japanisch, Französisch, Deutsch, vereinfachtes Chinesisch, traditionelles Chinesisch, Koreanisch und Spanisch verfügbar.

Weitere Informationen darüber, welche Sprachpakete Sie im Clientsystem, Browser und Remote-Desktop verwenden müssen, finden Sie unter [Internationale Tastaturen](#).

## Internationale Tastaturen

Wenn Sie nicht englische Tastaturen und Ländereinstellungen verwenden, müssen Sie bestimmte Einstellungen für das Clientsystem, den Browser und den Remote-Desktop festlegen. Einige Sprachen erfordern die Verwendung eines IME (Eingabemethoden-Editor) auf dem Remote-Desktop.

Wenn die richtigen lokalen Einstellungen und Eingabeverfahren installiert sind, können Sie für folgende Sprachen Zeichen eingeben: Englisch, Japanisch, Französisch, Deutsch, vereinfachtes Chinesisch, traditionelles Chinesisch, Koreanisch und Spanisch.

**Tabelle 4-7. Erforderliche Einstellungen für die Eingabesprache**

<b>Sprache</b>	<b>Eingabesprache auf dem lokalen Clientsystem</b>	<b>IME auf dem lokalen Clientsystem erforderlich?</b>	<b>Browser und Eingabesprache auf dem Remote-Desktop</b>	<b>Ist IME auf dem Remote-Desktop erforderlich?</b>
Englisch	Englisch	Nein	Englisch	Nein
Französisch	Französisch	Nein	Französisch	Nein
Deutsch	Deutsch	Nein	Deutsch	Nein
Chinesisch (Vereinfacht)	Chinesisch (Vereinfacht)	Englischer Eingabemodus	Chinesisch (Vereinfacht)	Ja
Chinesisch (Traditionell)	Chinesisch (Traditionell)	Englischer Eingabemodus	Chinesisch (Traditionell)	Ja
Japanisch	Japanisch	Englischer Eingabemodus	Japanisch	Ja
Koreanisch	Koreanisch	Englischer Eingabemodus	Koreanisch	Ja
Spanisch	Spanisch	Nein	Spanisch	Nein

# Fehlerbehebung für Horizon Client

# 5

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](#)
- [Zurücksetzen von Remote-Desktops oder veröffentlichten Anwendungen](#)

## 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 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

### Verfahren

- ◆ Verwenden Sie die Option **Neu starten**.

Option	Aktion
In der Sidebar	Besteht eine Verbindung mit einem Remote Desktop, klicken Sie auf die Schaltfläche <b>Menü öffnen</b> in der Symbolleiste neben dem Namen des Remote Desktops in der Liste <b>Wird ausgeführt</b> der Sidebar und wählen Sie <b>Neustarten</b> .
Verwenden eines URI	Verwenden Sie zum Neustart eines Desktops den URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&amp;action=restart</code> .

Das Betriebssystem im Remote Desktop wird neu gestartet, und Horizon 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 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

## Verfahren

- ◆ Verwenden Sie den **Zurücksetzen**-Befehl.

Option	Aktion
<b>Zurücksetzen von veröffentlichten Anwendungen im Fenster für die Anwendungsauswahl</b>	Im Fenster für die Desktop- und Anwendungsauswahl klicken Sie zum Zurücksetzen aller ausgeführten veröffentlichten Anwendungen vor der Herstellung einer Verbindung mit einem Remote Desktop oder mit einer veröffentlichten Anwendungen auf die Schaltfläche <b>Einstellungen</b> in der Symbolleiste rechts oben im Bildschirm und dann auf <b>Zurücksetzen</b> .
<b>Zurücksetzen eines Remote-Desktops auf der Sidebar</b>	Besteht eine Verbindung mit einem Remote-Desktop, klicken Sie auf die Schaltfläche <b>Menü öffnen</b> in der Symbolleiste neben dem Namen des Desktops in der Liste <b>Wird ausgeführt</b> der Sidebar und wählen Sie <b>Zurücksetzen</b> .
<b>Zurücksetzen von veröffentlichten Anwendungen auf der Sidebar</b>	Um alle ausgeführten Anwendungen zurückzusetzen, klicken Sie auf die Schaltfläche <b>Einstellungenfenster öffnen</b> in der Symbolleiste oben auf der Sidebar und klicken Sie dann auf <b>Zurücksetzen</b> .
<b>Zurücksetzen eines Remote-Desktops mithilfe eines URI</b>	Verwenden Sie zum Zurücksetzen eines Remote-Desktops den URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&amp;action=reset</code> .

Wenn Sie einen Remote Desktop zurücksetzen, wird das Betriebssystem im Remote Desktop neu gestartet und Horizon 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.