

VMware Horizon HTML Access Installations- und Einrichtungshandbuch

Geändert am 4. Januar 2018

VMware Horizon HTML Access 4.7

VMware Horizon 7 7.4



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

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

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

Copyright © 2013–2018 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 6
- Vorbereiten von Verbindungsservern und Sicherheitsservern für HTML Access 9
 - Firewallregeln für HTML Access 10
- Konfigurieren von View zum Entfernen von Anmeldedaten aus dem Cache 11
- Vorbereiten von Desktops, Pools und Farmen für HTML Access 12
- Anforderungen für die Funktion „Session Collaboration“ 14
- Konfigurieren von HTML Access-Agents zur Verwendung von neuen SSL-Zertifikaten 15
 - Hinzufügen des Zertifikat-Snap-In zur MMC auf einem View-Desktop 16
 - Importieren eines Zertifikats für den HTML Access Agent in den Windows-Zertifikatspeicher 16
 - Importieren von Stamm- und Zwischenzertifikaten für den HTML Access-Agent 18
 - Festlegen des Zertifikatfingerabdrucks in der Windows-Registrierung 18
- Konfiguration der HTML Access-Agents zur Verwendung spezifischer Verschlüsselungsansammlungen 19
- Konfigurieren von iOS zur Verwendung von durch Zertifizierungsstellen signierten Zertifikaten 20
- Upgrade der HTML Access-Software 21
- Deinstallieren von HTML Access vom View-Verbindungsserver 21
- Von VMware erfasste Daten 21

2 Konfigurieren von HTML Access für Endbenutzer 24

- Konfigurieren der VMware Horizon-Webportalseite für Endbenutzer 24
- Verwenden von URIs zur Konfiguration von HTML Access-Webclients 28
 - Syntax für die Erstellung von URIs für HTML Access 28
 - Beispiele für URIs 31
- Gruppenrichtlinieneinstellungen für HTML Access 34

3 Verwenden eines Remote-Desktops oder einer Remoteanwendung 35

- Funktionsunterstützungs-Matrix 36
- Internationalisierung 37
- Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung 37
 - Einstufen eines selbstsignierten Zertifikats als vertrauenswürdig 39
- Herstellen einer Verbindung mit einem Server im Workspace ONE-Modus 40
- Verwenden des nicht authentifizierten Zugriffs zur Verbindung mit Remoteanwendungen 41
- Tastenkombinationen 42
- Internationale Tastaturen 46
- Bildschirmauflösung 47

H.264-Decodierung	48
Festlegen der Zeitzone	48
Verwenden der Sidebar	49
Verwenden mehrerer Monitore	53
Verwendung der DPI-Synchronisierung	54
Sound	55
Kopieren und Einfügen von Text	55
Verwenden der Kopier- und Einfügen-Funktion	56
Übertragen von Dateien zwischen dem Client und einem Remote-Desktop	58
Herunterladen von Dateien von einem Desktop auf den Client	59
Hochladen von Dateien vom Client zu einem Desktop	59
Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone	60
Verwenden der Funktion „Session Collaboration“	60
Einladen eines Benutzers zu einer Remote-Desktop-Sitzung	61
Verwalten einer gemeinsamen Sitzung	63
Teilnehmen an einer gemeinsamen Sitzung	64
Abmelden oder trennen	65
Zurücksetzen eines Remote-Desktops oder von veröffentlichten Anwendungen	66
Neustarten eines Remote-Desktops	67

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 den Dokumenten *ViewInstallation von* und *ViewVerwaltung von* heranziehen.

Konfiguration und Installation

Bei der Einrichtung einer View-Bereitstellung für HTML Access müssen Sie HTML Access auf dem View-Verbindungsserver 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 den View-Verbindungsserver eingeben.

Dieses Kapitel enthält die folgenden Themen:

- [Systemanforderungen für HTML Access](#)
- [Vorbereiten von Verbindungsservern und Sicherheitsservern für HTML Access](#)
- [Konfigurieren von View zum Entfernen von Anmeldedaten aus dem Cache](#)
- [Vorbereiten von Desktops, Pools und Farmen für HTML Access](#)
- [Anforderungen für die Funktion „Session Collaboration“](#)
- [Konfigurieren von HTML Access-Agents zur Verwendung von neuen SSL-Zertifikaten](#)
- [Konfiguration der HTML Access-Agents zur Verwendung spezifischer Verschlüsselungsansammlungen](#)
- [Konfigurieren von iOS zur Verwendung von durch Zertifizierungsstellen signierten Zertifikaten](#)
- [Upgrade der HTML Access-Software](#)
- [Deinstallieren von HTML Access vom View-Verbindungsserver](#)
- [Von VMware erfasste Daten](#)

Systemanforderungen für HTML Access

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

Hinweis Ab der Version 7.0 wird View Agent in Horizon Agent umbenannt.

Browser auf Clientsystemen

Browser	Version
Chrome	62, 63
Chrome auf Android-Gerät	59 oder höher

Browser	Version
Internet Explorer	11
Safari	11
Safari auf mobilen Geräten	iOS 9, iOS 10
Firefox	56, 57
Microsoft Edge	40, 41

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)
Windows	8.x (32 Bit und 64 Bit)
Windows	10 (32 Bit und 64 Bit)
Mac OS X	10.12.x (Sierra)
Mac OS	10.13.x (High Sierra)
iOS	9, 10
Chrome OS	28.x und höher
Android	7, 8

Remote-Desktops

HTML Access erfordert Horizon Agent 7.0 oder höher und unterstützt alle Desktop-Betriebssysteme, die Horizon 7.0 unterstützt. Weitere Informationen finden Sie unter „Unterstützte Betriebssysteme für Horizon Agent“ in *View-Installation* für Version 7.0 oder höher.

Pool-Einstellungen

HTML Access erfordert die folgenden Pooleinstellungen in Horizon Administrator:

- 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 [Bildschirmauflösung](#).

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

Konfigurationsanweisungen werden unter [Vorbereiten von Desktops, Pools und Farmen für HTML Access](#) 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 Verbindungsservern und Sicherheitsservern für HTML Access

Administratoren müssen spezifische Aufgaben ausführen, damit Endbenutzer über einen Webbrowser eine Verbindung mit Remote-Desktops herstellen können.

Bevor Endbenutzer eine Verbindung mit dem Verbindungsserver oder einem Sicherheitsserver herstellen und auf einen Remote-Desktop zugreifen können, müssen Sie den Verbindungsserver zusammen mit der HTML Access-Komponente sowie Sicherheitsserver installieren.

Im Folgenden finden Sie eine Checkliste mit Aufgaben, die vor der Verwendung von HTML Access auszuführen sind:

- 1 Installieren Sie den Verbindungsserver zusammen mit der HTML Access-Option auf dem Server oder den Servern, der bzw. die eine replizierte Verbindungsserver-Gruppe darstellt bzw. darstellen.

Die HTML Access-Komponente ist im Installationsprogramm standardmäßig bereits ausgewählt. Anweisungen zur Installation finden Sie im Dokument *Installation von View*.

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 „View HTML Access“ suchen.

- 2 Wenn Sie Sicherheitsserver verwenden, installieren Sie Sicherheitsserver.

Anweisungen zur Installation finden Sie im Dokument *Installation von View*.

Wichtig Die Version des Sicherheitsservers muss mit der Version des Verbindungsservers übereinstimmen.

- 3 Vergewissern Sie sich, dass jede Verbindungsserver-Instanz oder jeder Sicherheitsserver ein Sicherheitszertifikat besitzt, das der Client unter Verwendung des Hostnamens, den Sie im Browser eingeben, vollständig überprüfen kann.

Weitere Informationen finden Sie im Dokument *Installation von View*.

- 4 Zum Verwenden der zweistufigen Authentifizierung, z. B. der RSA SecurID- oder RADIUS-Authentifizierung, muss diese Funktion auf dem Verbindungsserver aktiviert sein.

Weitere Informationen finden Sie in den Themen zur zweistufigen Authentifizierung im Dokument *Administration von View*.

Wichtig Wenn Sie die Einstellung **Domänenliste in der Kunden-Benutzeroberfläche ausblenden** aktivieren und die zweistufige Authentifizierung (RSA SecureID oder RADIUS) für die Verbindungsserver-Instanz auswählen, dürfen Sie nicht die Windows-Benutzernamenübereinstimmung erzwingen. Wenn die Windows-Benutzernamenübereinstimmung erzwungen wird, können Benutzer keine Domäneninformationen in das Textfeld „Benutzername“ eingeben und es ist keine Anmeldung mehr möglich. Weitere Informationen finden Sie in den Themen zur zweistufigen Authentifizierung im Dokument *Administration von View*.

- 5 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 View-Servern) am TCP-Port 22443 auf Remote-Desktops im Datacenter. Weitere Informationen finden Sie unter [Firewallregeln für HTML Access](#).
- 6 Um Benutzern einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen in Horizon Client zu ermöglichen, müssen Sie diese Funktion im Verbindungsserver aktivieren. Weitere Informationen finden Sie in den Themen zum nicht authentifizierten Zugriff im Dokument *Administration von View*.

Nach der Installation der Server werden Sie in Horizon Administrator feststellen, dass die Einstellung des **Blast-Sicherheitsgateway** für die betreffenden Verbindungsserver-Instanzen und Sicherheitsserver aktiviert ist. Darüber hinaus ist für die Einstellung **Externe Blast-URL** automatisch die Verwendung des Blast-Sicherheitsgateway 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 *Installation von View*.

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 *Administration von View*.

Firewallregeln für HTML Access

Um Client-Webbrowsern zu ermöglichen, HTML Access zur Herstellung einer Verbindung zum Sicherheitsserver, zu View-Verbindungsserverinstanzen und zu Remote-Desktops zu verwenden, 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 View-Verbindungsserverinstanz oder eines Sicherheitsservers wird standardmäßig die Regel **VMware Horizon View-Verbindungsserver (Blast-In)** für die Windows-Firewall konfiguriert, damit eingehender Datenverkehr auf dem TCP-Port 8443 zugelassen wird.

Tabelle 1-1. Firewallregeln für HTML Access

Quelle	Standard- quell- Port	Protokoll	Ziel	Standard- ziel-Port	Hinweise
Client- Webbrowser	TCP beliebig	HTTPS	Sicherheitsserver oder View- Verbindungs- serverinstanz	TCP 443	Um die erste Verbindung mit Horizon herzustellen, verbindet sich der Webbrowser auf einem Clientgerät mit einem Sicherheitsserver oder einer Horizon-Verbindungsserver-Instanz über den TCP-Port 443.
Client- Webbrowser	TCP beliebig	HTTPS	Blast-Sicherheitsgateway	TCP 8443	Nachdem die erste Verbindung mit Horizon hergestellt wurde, stellt der Webbrowser auf einem Clientgerät eine Verbindung mit dem Blast-Sicherheitsgateway über den TCP-Port 8443 her. Die zweite Verbindung kann nur hergestellt werden, wenn das Blast-Sicherheitsgateway auf einem Sicherheitsserver oder einer Horizon-Verbindungsserver-Instanz aktiviert ist.
Blast-Sicherheitsgateway	TCP beliebig	HTTPS	HTML Access-Agent	TCP 22443	Wenn, nachdem der Benutzer einen Remote-Desktop ausgewählt hat, das Blast-Sicherheitsgateway aktiviert ist, stellt das Blast-Sicherheitsgateway über den TCP-Port 22443 auf dem Desktop 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 das Blast-Sicherheitsgateway, nachdem der Benutzer einen View-Desktop ausgewählt hat, nicht aktiviert ist, erstellt der Webbrowser auf einem Clientgerät über den TCP-Port 22443 auf dem Desktop eine direkte Verbindung zum HTML Access-Agent. Diese Agent-Komponente ist Bestandteil der Installation von Horizon Agent.

Konfigurieren von View zum Entfernen von Anmeldedaten aus dem Cache

Sie können View so konfigurieren, dass die Anmeldedaten aus dem Cache gelöscht werden, wenn der Benutzer eine Registerkarte schließt, die eine Verbindung zu einem Remote-Desktop oder einer Remoteanwendung herstellt, oder wenn er eine Registerkarte schließt, die eine Verbindung zur Seite für die Auswahl von Desktop und Anwendung im HTML Access-Client herstellt.

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 Remoteanwendung aufruft 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 Administrator **View-Konfiguration > Globale Einstellungen** aus und klicken Sie im Bereich „Allgemein“ 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 für HTML Access

Bevor Endbenutzer auf einen Remote-Desktop oder eine Remoteanwendung zugreifen können, müssen Administratoren bestimmte Pool- und Farmeinstellungen konfigurieren und Horizon Agent auf den virtuellen Maschinen des Remote-Desktops sowie auf 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 Ihre vSphere-Infrastruktur- und 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 Verbindungsservern und Sicherheitsservern für HTML Access](#).
- Wenn Sie eine Firewall eines Drittanbieters verwenden, konfigurieren Sie eine Regel, mit der eingehender Datenverkehr von Horizon Servern am TCP-Port 22443 für die Horizon-Desktops im Datacenter zugelassen wird.
- Stellen Sie sicher, dass die folgende Software in der angegebenen Reihenfolge auf der virtuellen Maschine installiert wurde, die Sie als Desktop-Quelle oder RDS-Host verwenden möchten: ein unterstütztes Betriebssystem und VMware Tools.

Eine Liste der unterstützten Betriebssysteme finden Sie unter [Systemanforderungen für HTML Access](#).

- Machen Sie sich mit den Verfahren für das Erstellen von Pools sowie Farmen und für das Zuweisen von Benutzerberechtigungen vertraut. Weitere Informationen finden Sie in den Themen zur Erstellung von Pools und Farmen im Dokument *Einrichten von Desktops und Anwendungen in View*.
- Um sicherzustellen, dass der Remote-Desktop oder die Remoteanwendung für Endbenutzer zugänglich ist, müssen Sie überprüfen, ob die Horizon Client-Software auf einem Clientsystem installiert wurde. Testen Sie die Verbindung, indem Sie die Horizon Client-Software verwenden, bevor Sie über einen Browser eine Verbindung herzustellen versuchen.

Anweisungen zur Installation von Horizon Client finden Sie auf der Website für die Horizon Client-Dokumentation unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

- Stellen Sie sicher, dass Sie einen der unterstützten Browser für den Zugriff auf einen Remote-Desktop verwenden. Siehe [Systemanforderungen für HTML Access](#).

Verfahren

- 1 Erstellen oder bearbeiten Sie für RDS-Desktops und -Anwendungen die Farm mit Horizon Administrator und aktivieren Sie die Option **HTML Access für Desktops und Anwendungen in dieser Farm zulassen** in den Farmeinstellungen.
- 2 Bei Einzelsitzung-Desktop-Pools erstellen oder bearbeiten Sie den Desktop-Pool mit Horizon Administrator, damit dieser mit HTML Access verwendet werden kann.
 - a Aktivieren Sie **HTML Access** in den Desktop-Pool-Einstellungen.

Die Einstellung **HTML Access** erscheint nicht im Assistenten „Desktop-Pool hinzufügen“ beim Erstellen von RDS-Desktop-Pools. Stattdessen aktivieren Sie die Option **HTML Access für Desktops und Anwendungen in dieser Farm zulassen** beim Erstellen oder Bearbeiten der Farm von RDS-Hosts.
 - b Stellen Sie sicher, dass in den Pool-Einstellungen die **Maximale Auflösung für alle Monitore** auf **1920x1200** oder höher festgelegt ist.
- 3 Nach der Erstellung, Neuzusammenstellung oder Aktualisierung der Pools für die Verwendung von Horizon Agent mit der **HTML Access**-Option melden Sie sich mit Horizon Client bei einem Desktop oder einer Anwendung an.

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
```

Stellen Sie sicher, dass Sie **https** in der URL verwenden.

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

Sie können jetzt über einen Webbrowser auf einen Remote-Desktop oder eine Remoteanwendung zugreifen, wenn Sie ein Clientgerät verwenden, für das die Horizon Client-Software nicht im Betriebssystem installiert ist oder installiert werden kann.

Nächste Schritte

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

Anforderungen für die Funktion „Session Collaboration“

Mit der Funktion „Session Collaboration“ können Benutzer andere Benutzer zur Teilnahme an einer vorhandenen Windows-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 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 Gruppenrichtlinieneinstellungen die Funktion „Session Collaboration“ konfigurieren. Informationen hierzu finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Die Funktion „Session Collaboration“ unterstützt keine Linux-Remote-Desktop-Sitzungen und keine Linux-Sitzungen veröffentlichter Anwendungen.

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

Anzeigeprotokolle VMware Blast

Konfigurieren von HTML Access-Agents zur Verwendung von neuen SSL-Zertifikaten

Um Industrie- oder Sicherheitsvorschriften zu entsprechen, ersetzen Sie die Standard-SSL-Zertifikate, die vom HTML Access-Agent mit Zertifikaten erstellt wurden, die von einer Certificate Authority (CA) signiert wurden.

Wenn Sie den HTML Access-Agent auf View-Desktops installieren, erstellt der HTML Access-Agent-Dienst standardmäßig selbst signierte Zertifikate. Der Dienst liefert die Standardzertifikate an Browser, die HTML Access zur Herstellung einer Verbindung zu View verwenden.

Hinweis Im Gast-Betriebssystem 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 View-Desktop ein Zertifikat in den lokalen Windows-Zertifikatspeicher des Computers importieren. Außerdem müssen Sie auf jedem Desktop einen Registrierungswert festlegen, der es dem HTML Access-Agent ermöglicht, das neue Zertifikat zu verwenden.

Wenn Sie die standardmäßigen HTML Access-Agent-Zertifikate durch CA-signierte Zertifikate ersetzt haben, empfiehlt VMware, dass Sie ein eindeutiges Zertifikat auf jedem einzelnen Desktop konfigurieren. Konfigurieren Sie kein CA-Zertifikat auf einer übergeordneten virtuellen Maschine oder Vorlage, die Sie für das Erstellen eines Desktop-Pools verwenden. Dieser Ansatz würde zu Hunderten oder Tausenden Desktops mit identischen Zertifikaten führen.

Verfahren

1 Hinzufügen des Zertifikat-Snap-In zur MMC auf einem View-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 View-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 CA-Zertifikat zu ersetzen, müssen Sie das CA-Zertifikat in den lokalen Windows-Zertifikatspeicher des Computers importieren. Führen Sie diese Prozedur auf jedem Desktop durch, auf dem 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 Desktop vornehmen, auf dem Sie das Standardzertifikat durch ein durch eine Zertifizierungsstelle signiertes Zertifikat ersetzen.

Hinzufügen des Zertifikat-Snap-In zur MMC auf einem View-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 View-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 View-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 entfernenZertifikate** aus und klicken Sie auf **Hinzufügen**.
- 4 Wählen Sie im Fenster **Zertifikat-Snap-InComputerkonto**, 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 CA-Zertifikat zu ersetzen, müssen Sie das CA-Zertifikat in den lokalen Windows-Zertifikatsspeicher des Computers importieren. Führen Sie diese Prozedur auf jedem Desktop durch, auf dem der HTML Access-Agent installiert ist.

Voraussetzungen

- Stellen Sie sicher, dass der HTML Access-Agent auf dem View-Desktop installiert ist.
- Stellen Sie sicher, dass das CA-Zertifikat auf den Desktop kopiert wurde.
- Überprüfen Sie, ob das Zertifikat-Snap-In der MMC hinzugefügt wurde. Siehe [Hinzufügen des Zertifikat-Snap-In zur MMC auf einem View-Desktop](#).

Verfahren

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

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

- 5 Geben Sie das Kennwort für den privaten Schlüssel in der Zertifikatsdatei ein.
- 6 Aktivieren Sie **Schlüssel als exportierbar markieren**.
- 7 Aktivieren Sie **Alle erweiterbaren Eigenschaften mit einbeziehen**.
- 8 Klicken Sie auf **Weiter** und dann 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 Überprüfen Sie, ob im Dialogfeld „Zertifikatinformationen“ auf der Registerkarte „Allgemein“ die folgende Aussage angezeigt wird: Sie besitzen einen privaten Schlüssel für dieses Zertifikat.

Nächste Schritte

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

Konfigurieren Sie die entsprechenden Registrierungsschlüssel mit dem Fingerabdruck des Zertifikats. 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-Zertifikatsspeicher des Computers importieren.

Verfahren

- 1 Auf der MMC-Konsole auf View-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, übergehen Sie diese Prozedur.
 - 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 **Fertigstellen**.
- 6 Wenn Ihr Serverzertifikat von einer Zwischenzertifizierungsstelle signiert wurde, importieren Sie alle Zwischenzertifikate in der Zertifikatskette in den Zertifikatsspeicher des lokalen Windows-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 die entsprechenden Registrierungsschlüssel mit dem Fingerabdruck des Zertifikats. 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 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 View-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 Desktop herstellt, stellt der HTML Access-Agent dem Browser des Benutzers das durch eine Zertifizierungsstelle signierte Zertifikat aus.

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 den View-Verbindungsserver auf dem HTML Access Agent erstellt wurden.

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

Upgrade der HTML Access-Software

Für die meisten Versionen von HTML Access ist nur ein Upgrade der Verbindungsserver und von View Agent erforderlich.

Wenn Sie ein Upgrade für HTML Access durchführen, müssen Sie sicherstellen, dass die entsprechende Version des View-Verbindungsservers 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 von HTML Access vom View-Verbindungsserver

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

Verfahren

- 1 Öffnen Sie auf den View-Verbindungsserverhosts, auf denen HTML Access installiert ist, in der Windows-Systemsteuerung das Applet zum Deinstallieren von Programmen.
- 2 Wählen Sie das Programm VMware Horizon 7 HTML Access aus, und klicken Sie auf **Deinstallieren**.
- 3 (Optional) Stellen Sie in der Windows-Firewall für diesen 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 diesen View-Verbindungsserverhost zu verbieten.

Von VMware erfasste Daten

Wenn Ihr Unternehmen am Programm zur Verbesserung der Benutzerfreundlichkeit teilnimmt, erhebt VMware Daten aus bestimmten Client-Feldern. Felder mit vertraulichen Informationen werden anonymisiert.

VMware sammelt die Daten auf den Clients zur Priorisierung der Hardware- und Softwarekompatibilität. Wenn sich ein Horizon-Administrator zur Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit entscheidet, sammelt VMware anonyme Daten über Ihre Bereitstellung, um die Reaktion von VMware auf die 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 VMware-Programm zur Verbesserung der Benutzerfreundlichkeit kann der Administrator, der die Installation des Verbindungservers durchführt, bei der Ausführung des Installationsassistenten für den Verbindungsserver diese Option „abonnieren“ oder nach der Installation eine entsprechende Option in Horizon Administrator festlegen.

Tabelle 1-2. Für das Programm zur Verbesserung der Benutzerfreundlichkeit 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	4.7.0-Build_Nummer
Client-Binärarchitektur	<client-arch>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> ■ Browser ■ arm
Systemeigene Architektur des Browsers	<browser-arch>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> ■ Win32 ■ Win64 ■ MacIntel ■ iPad ■ Linux armv81 (zur Unterstützung von Android Chrome)
Zeichenfolge zum Browserbenutzer-Agent	<browser-user-agent>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> ■ Mozilla/5.0 (Windows NT 6.1; WOW64) ■ AppleWebKit/703.00 (KHTML, wie Gecko) ■ Chrome/3.0.1750 ■ Safari/703.00 ■ Edge/13.10586
Interne Versionszeichenfolge des Browsers	<browser-version>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> ■ 7.0.3 (für Safari), ■ 44.0 (für Firefox) ■ 13.10586 (für Edge)

Beschreibung	Feldname	Wird dieses Feld anonymisiert?	Beispielswert
Core-Implementierung des Browsers	<browser-core>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> ■ Chrome ■ Safari ■ Firefox ■ Internet Explorer ■ Edge
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/
pckbpdplfajmgaip1jfamclkinbjdnma
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.

Wichtig Wenn Sie ein Upgrade von View-Verbindungsserver 5.x oder einer älteren Version durchgeführt haben, die HTML Access-Komponente bisher nicht installiert war und Sie die Portalseite zuvor so bearbeitet haben, dass sie auf Ihren eigenen Server zum Download von Horizon Client verweist, werden diese Anpassungen möglicherweise ausgeblendet, wenn Sie View-Verbindungsserver 6.0 oder höher installieren. Bei Horizon 6 oder höher wird die HTML Access-Komponente bei einem Upgrade von View-Verbindungsserver automatisch installiert.

Wenn Sie die HTML Access-Komponente bereits separat für View 5.x installiert hatten, werden alle Anpassungen, die Sie an der Webseite vorgenommen haben, beibehalten. Wenn Sie die HTML Access-Komponente nicht installiert hatten, werden Ihre Anpassungen ausgeblendet. Die Anpassungen für frühere Versionen befinden sich in der Datei `portal-links.properties`, die nicht mehr verwendet wird.

Verfahren

- 1 Öffnen Sie auf dem View-Verbindungsserverhost 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 View 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
HTML Access deaktivieren	<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.“
Herunterladen von Horizon Client deaktivieren	<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.“
Ändern der URL für die Webseite zum Herunterladen von Horizon Client	<code>link.download=https:// url-of-web-server</code> Verwenden Sie diese Eigenschaft, wenn Sie Ihre eigene Webseite erstellen möchten.

Option	Eigenschafteneinstellung
Create links for specific installers (Links für bestimmte Installationsprogramme erstellen)	<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 View-Verbindungsserver befindet.</p> <ul style="list-style-type: none"> ■ Allgemeiner Link zum Herunterladen des Installationsprogramms: <pre>link.download=https://server/downloads</pre> ■ 32-Bit-Windows-Installationsprogramm: <pre>link.win32=https://Server/downloads/VMware-Horizon-Client-x86-Build-Nr..exe</pre> ■ 64-Bit-Windows-Installationsprogramm: <pre>link.win64=https://Server/downloads/VMware-Horizon-Client-x86_64-Build-Nr..exe</pre> ■ Windows Phone-Installationsprogramm: <pre>link.winmobile=https://Server/downloads/VMware-Horizon-Client-Build-Nr..appx</pre> ■ 32-Bit-Linux-Installationsprogramm: <pre>link.linux32=https://Server/downloads/VMware-Horizon-Client-Build-Nr..x86.bundle</pre> ■ 64-Bit-Linux-Installationsprogramm: <pre>link.linux64=https://Server/downloads/VMware-Horizon-Client-Build-Nr..x64.bundle</pre> ■ Mac OS X-Installationsprogramm: <pre>link.mac=https://Server/downloads/VMware-Horizon-Client-Build-Nr..dmg</pre> ■ iOS-Installationsprogramm: <pre>link.ios=https://Server/downloads/VMware-Horizon-Client-iPhoneOS-Build-Nr..ipa</pre> ■ Android-Installationsprogramm: <pre>link.android=https://Server/downloads/VMware-Horizon-Client-AndroidOS-Build-Nr..apk</pre> ■ Chrome OS-Installationsprogramm: <pre>link.chromeos=https://Server/downloads/VMware-Horizon-Client-ChromeOS-Build-Nr..apk</pre>
Ändern der URL für den Hilfe-Link auf der Anmeldeseite	<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 View-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 View Web-Komponentendienst 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 dem View-Verbindungsserver 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:

- Adresse des View-Verbindungservers
- Portnummer für den View-Verbindungsserver
- 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 Desktops oder der Anwendung sowie Aktionen oder Konfigurationsoptionen.

URI-Spezifikation

Verwenden Sie zum Generieren von URIs für den Start von HTML Access-Webclients 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.

- 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 den HTML Access Web client unterstützt werden. Wenn Sie URIs für mehrere Clienttypen generieren, so zum Beispiel für Desktop-Clients oder mobile Clients, finden Sie für jede Art von Clientssystem weitere Informationen im Dokument *Verwenden von VMware Horizon Client*.

action

Tabelle 2-1. Werte, die mit der Abfrage „action“ verwendet werden können

Wert	Beschreibung
browse	Zeigt eine Liste der verfügbaren, auf dem angegebenen Server gehosteten Desktops und Anwendungen an. Bei Verwendung dieser Aktion müssen Sie keinen Desktop bzw. keine Anwendung angeben.
start-session	Startet den angegebenen Desktop oder die angegebene Anwendung. Wenn keine „action“-Abfrage bereitgestellt wird und der Desktop- oder Anwendungsname angegeben wird, ist start-session die Standardaktion.
reset	Führt den angegebenen 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 Anwendung ungültig.
logout	Meldet den Benutzer vom Gastbetriebssystem auf dem Remote-Desktop ab. Diese Aktion ist für eine Anwendung ungültig.
restart	Führt den primären Desktop herunter und startet diesen neu, wenn der Benutzer die Anforderung für den Neustart bestätigt. Diese Aktion ist für eine Anwendung ungültig.

applicationId

Der Anzeigename der Anwendung. Dieser Anzeigename ist der Name, der in Horizon Administrator 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 beim Start einer Remoteanwendung an. 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 Desktops. Dieser Anzeigename ist der Name, der in View Administrator beim Erstellen des Desktop-Pools angegeben wurde.

	Weist der Anzeigename ein Leerzeichen auf, verwendet der Browser %20 zur Darstellung des Leerzeichens.
domainName	Der NETBIOS-Domänenname, der mit dem Benutzer verknüpft ist, der eine Verbindung zum Remote-Desktop oder zur Remoteanwendung herstellt. Beispielsweise ist es sinnvoller, <i>MeineFirma</i> als <i>MeineFirma.com</i> zu verwenden.
tokenUserName	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.
userName	Der Active Directory-Benutzer, der eine Verbindung zum Remote-Desktop oder zur Remoteanwendung herstellt. Für den Benutzernamen sind folgende Formate zulässig: <ul style="list-style-type: none"> ■ <i>Benutzername</i> ■ <i>Domänenname%5CBenutzername</i> ■ Benutzerprinzipalname (User Principal Name, UPN) in der Form <i>Benutzername@Domänenname</i>
unauthenticatedAccess Enabled	Wenn für diese Option True festgelegt ist, ist die Funktion für den nicht authentifizierten Zugriff standardmäßig aktiviert. HTML Access Web client wird gestartet und ein Benutzerkonto für anonyme Benutzer wird angezeigt. Ein Beispiel für die Syntax ist etwa unauthenticatedAccessEnabled=true .
unauthenticatedAccess Account	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 anonymous1 dann unauthenticatedAccessAccount=anonymous1 .

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*.

Verwenden eines Remote-Desktops oder einer Remoteanwendung

3

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 Remoteanwendung 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](#)
- [Internationalisierung](#)
- [Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung](#)
- [Herstellen einer Verbindung mit einem Server im Workspace ONE-Modus](#)
- [Verwenden des nicht authentifizierten Zugriffs zur Verbindung mit Remoteanwendungen](#)
- [Tastenkombinationen](#)
- [Internationale Tastaturen](#)
- [Bildschirmauflösung](#)
- [H.264-Decodierung](#)
- [Festlegen der Zeitzone](#)
- [Verwenden der Sidebar](#)
- [Verwenden mehrerer Monitore](#)
- [Verwendung der DPI-Synchronisierung](#)
- [Sound](#)
- [Kopieren und Einfügen von Text](#)
- [Übertragen von Dateien zwischen dem Client und einem Remote-Desktop](#)
- [Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone](#)
- [Verwenden der Funktion „Session Collaboration“](#)
- [Abmelden oder trennen](#)

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

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 3-1. 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-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
Wyse MMR						
Windows Media MMR						
Virtuelles Drucken						
Standortbasierter Druck	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 View-Architektur*.

Funktionsunterstützung für sitzungsbasierte Desktops und gehostete Anwendungen auf RDS-Hosts

RDS-Hosts sind Server-Computer, auf denen Windows-Remotedesktopdienste und View 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 3-2. Unterstützte Funktionen für HTML Access für RDS-Hosts mit installiertem View Agent 6.1.1 oder höher bzw. mit installiertem Horizon Agent 7.0 oder höher

Funktion	Windows Server 2008 R2 RDS-Host	Windows Server 2012 oder 2012 R2 RDS-Host	Windows Server 2016
RSA SecurID oder RADIUS	X	X	Horizon Agent 7.0.2 und höher
Einmaliges Anmelden	X	X	Horizon Agent 7.0.2 und höher
VMware Blast-Anzeigeprotokoll	X	X	Horizon Agent 7.0.2 und höher
Standortbasierter Druck	X (nur virtuelle Maschine)	X (nur virtuelle Maschine)	Horizon Agent 7.0.2 und höher (nur virtuelle Maschine)
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
Mehrere Monitore (nur für sitzungsbasierte Desktops)	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 *View-Installation*.

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](#).

Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung

Verwenden Sie Ihre Active Directory-Anmeldedaten zum Herstellen einer Verbindung mit den Remote-Desktops und -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 den RADIUS-Authentifizierungsbennamen oder -Passcode.
- 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 Remoteanwendung 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 Remoteanwendung als Favorit auf den grauen Stern im Symbol des Desktops oder der 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 Remoteanwendung, auf den oder die Sie zugreifen möchten.

Der Remote-Desktop oder die Remoteanwendung 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 -anwendungen zugreifen, das Fenster „Einstellungen“ aufrufen, Text kopieren und einfügen und vieles mehr.

Nächste Schritte

Unmittelbar nach der Verbindungsherstellung mit einem Desktop oder einer 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 ersten Herstellung einer Verbindung mit einem Remote-Desktop oder mit einer Remoteanwendung vom Browser aufgefordert, ein selbstsigniertes Zertifikat, das von diesem Remotecomputer verwendet wird, zu akzeptieren. Bevor die Verbindung mit dem Remote-

Desktop oder der Remoteanwendung hergestellt werden kann, müssen Sie dieses Zertifikat als vertrauenswürdig einstufen.

Die meisten Browser bieten die Möglichkeit, das selbstsignierte Zertifikat dauerhaft als vertrauenswürdig zu akzeptieren. Wenn Sie dieses Zertifikat nicht dauerhaft als vertrauenswürdig einstufen, müssen Sie das Zertifikat bei jedem Start Ihres Browsers neu überprüfen. Bei einem Safari-Browser muss das Sicherheitszertifikat dauerhaft als vertrauenswürdig akzeptiert werden, damit eine Verbindung hergestellt werden kann.

Verfahren

- 1 Wenn in Ihrem Browser eine Warnmeldung zu einem nicht vertrauenswürdigen Zertifikat oder zum Status der Verbindung als nicht privat eingeblendet wird, müssen Sie das Zertifikat überprüfen, um sicherzustellen, dass es dem Zertifikat Ihres Unternehmens entspricht.

Gegebenenfalls wenden Sie sich an Ihren Horizon-Administrator, der Ihnen weiterhelfen kann. In einem Chrome-Browser gehen Sie beispielsweise wie nachfolgend dargestellt vor.

- a Klicken Sie auf das Schlosssymbol in der Adressleiste.
- b Klicken Sie auf den Link **Zertifikatsinformationen**.
- c Überprüfen Sie, ob das Zertifikat dem Zertifikat Ihres Unternehmens entspricht.

Gegebenenfalls wenden Sie sich an Ihren Horizon-Administrator, 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)**.

In einem Safari-Browser gehen Sie für die permanente Einstufung eines Zertifikats als vertrauenswürdig vor, wie im Folgenden beschrieben.

- 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 bzw. die Remoteanwendung wird gestartet.

Herstellen einer Verbindung mit einem Server im Workspace ONE-Modus

Ab Horizon 7 Version 7.2 hat ein 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 -anwendungen nur über das Workspace ONE-Webportal starten.

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 Desktops oder einer Anwendung über das Workspace ONE-Webportal können Ihre Remote-Desktops oder -anwendungen nicht in HTML Access angezeigt oder gestartet werden.

Verwenden des nicht authentifizierten Zugriffs zur Verbindung mit Remoteanwendungen

Ein Horizon-Administrator kann mit der Funktion des nicht authentifizierten Zugriffs Benutzer für einen nicht authentifizierten Zugriff erstellen und diesen Benutzern Berechtigungen für Remoteanwendungen auf einer Verbindungsserver-Instanz erteilen. Benutzer für einen nicht authentifizierten Zugriff können sich anonym beim Server anmelden, um eine Verbindung zu ihren Remoteanwendungen herzustellen.

Voraussetzungen

- Führen Sie die unter [Vorbereiten von Verbindungsservern und Sicherheitsservern für HTML Access](#) 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 *Administration von View*.

Verfahren

- 1 Öffnen Sie einen Browser. Verwenden Sie eine der im Folgenden aufgeführten URI-Syntaxen für die Herstellung einer Verbindung mit der Verbindungsserver-Instanz, auf der Sie über einen nicht authentifizierten Zugriff auf Remoteanwendungen verfügen.

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

In den obigen URI-Syntaxen gibt *authority-part* die Adresse des Servers an und optional eine nicht standardmäßige Portnummer. Die Servernamen müssen einer DNS-Syntax entsprechen. Verwenden Sie zur Angabe einer Portnummer die folgende Syntax: *Serveradresse:Portnummer*. *anonymous_account* ist das zur anonymen Anmeldung erstellte Benutzerkonto für den nicht authentifizierten Zugriff.

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.

- 2 (Optional) Wenn Sie die `unauthenticatedAccessAccount`-Abfrage nicht festgelegt haben, wählen Sie, falls erforderlich, aus dem Dropdown-Menü **Benutzerkonto** ein Benutzerkonto für den nicht authentifizierten Zugriff aus und klicken Sie auf **Absenden**.

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

Das Auswahlfenster für Anwendungen wird angezeigt.

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






Die Remoteanwendung wird in Ihrem Browser angezeigt. Es ist auch eine Navigations-Sidebar verfügbar. Um die Sidebar einzublenden, klicken Sie auf die Registerkarte links im Browser. Mit der Sidebar können Sie auf andere Remoteanwendungen zugreifen, das Fenster „Einstellungen“ aufrufen, Text kopieren und einfügen und vieles mehr.

Hinweis Sie können mit nicht authentifizierten Anwendungssitzungen keine erneuten Verbindungen herstellen. Wenn Sie die Verbindung mit einem Client trennen, meldet der RDS-Host die lokale Benutzersitzung automatisch ab.

Tastenkombinationen

Unabhängig von der verwendeten Sprache können einige Tastenkombinationen nicht an einen Remote-Desktop oder an eine Remoteanwendung gesendet werden.

Webbrowser ermöglichen es, bestimmte Tasteneingaben und Tastenkombinationen sowohl an den Client 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 Schaltfläche **Einstellungenfenster öffnen** in der Symbolleiste der Sidebar und aktivieren **-A**, **-C**, **-V** und **-X aktivieren**. (Diese Option erscheint im Fenster „Einstellungen“ nur bei Verwendung eines Mac.)

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 Schaltfläche **Strg+Alt+Entf senden** der Symbolleiste oben auf der Sidebar.

- Feststelltaste+*Zusatztaste* (z. B. Alt oder Umschalttaste)
- Funktionstasten, wenn Sie ein Chromebook verwenden
- Windows-Tastenkombinationen

Die folgenden Windows-Tastenkombinationen können in Remote-Desktops verwendet werden, wenn Sie die Windows-Taste (Win) für Desktops aktivieren. Um diese Taste zu aktivieren, klicken Sie auf die Schaltfläche **Einstellungenfenster öffnen** in der Symbolleiste der Sidebar und aktivieren **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 können nicht für von RDS-Hosts bereitgestellten Remoteanwendungen verwendet werden. Sie gelten wie angegeben für Windows Server 2008 R2-, Windows Server 2012 R2- und Windows Server 2016-Einzelbenutzer-Desktops sowie für von einem RDS-Host bereitgestellte sitzungsbasierte Desktops.


Einige Tastenkombinationen, die mit einem Windows 8.x- oder einem Windows Server 2012 R2-Betriebssystem verwendet werden können, funktionieren nicht in Remote-Desktops mit einem Windows 7-, Windows Server 2008 R2- oder Windows 10-Betriebssystem.

Tabelle 3-3. 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.	

Schlüssel	Aktion	Einschränkungen
Win+X	Öffnet das Menü Quicklink .	
Win+, (Komma)	Ermöglicht eine temporäre Vorschau am 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 Desktop wieder her.	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden.
Win+Alt+Num	Öffnet den Desktop und die Sprungliste für die an der Taskleiste an der durch die Ziffer angegebenen Position angeheftete App.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Enter	Öffnet die Sprachausgabe.	

Tabelle 3-4. 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-Browsern verwendet werden.
Windows-Taste	Blendet den Startbildschirm ein oder aus.	
Win+B	Setzt den Fokus auf den Infobereich.	
Win+C	Öffnet den Charms-Bereich	
Win+D	Blendet den Desktop ein oder aus.	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden. Problemumgehung: Drücken Sie  -D auf Macs.
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“ für eine allgemeine Suche oder für eine Suche in der geöffneten App, wenn diese eine App-Suche unterstützt.	
Win+R	Öffnet das Dialogfeld „Ausführen“.	
Win+S	Öffnet den Charm „Suche“ für eine Suche in Windows oder im Internet.	
Win+X	Öffnet das Menü Quicklink .	
Win+Z	Zeigt die in der App verfügbaren Befehle an.	
Win+, (Komma)	Zeigt vorübergehend den Desktop an, solange Sie diese Tasten drücken.	Hinweis Diese Tastenkombination kann nicht für Windows 2012 R2-Betriebssysteme verwendet werden.

Schlüssel	Aktion	Einschränkungen
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 Desktop wieder her.	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden. Problemumgehung: Drücken Sie ⌘-D auf Macs.
Win+Alt+Num	Öffnet den Desktop und die Sprungliste für die an der Taskleiste an der durch die Ziffer angegebenen Position angeheftete App.	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 Desktop-Fenster.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach links	Maximiert das App- oder Desktop-Fenster zur linken Seite des Bildschirms.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach rechts	Maximiert das App- oder Desktop-Fenster zur rechten Seite des Bildschirms.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pos1	Minimiert alle Fenster bis auf das aktive Desktop-Fenster (durch nochmaliges Drücken werden alle Fenster wiederhergestellt).	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden.
Win+Umschalt+Pfeil nach oben	Zieht das Desktop-Fenster nach oben und unten auf.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Umschalt+Pfeil nach unten	Stellt das Desktop-Fenster vertikal unter Beibehaltung der Breite wieder her, nachdem es mit der Tastenkombination „Win+Umschalt+Pfeil nach oben“ aufgezogen wurde, oder minimiert das aktive Desktop-Fenster.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Enter	Öffnet die Sprachausgabe.	

Tabelle 3-5. Windows-Tastenkombinationen für Windows 7- und Windows Server 2008 R2-Remote-Desktops

Schlüssel	Aktion	Einschränkungen
Windows-Taste	Öffnet oder schließt das Startmenü.	
Win+Pause	Stellt das Dialogfeld für die Systemeigenschaften dar.	Auf Chromebooks oder Macs ist keine Pause-Taste verfügbar.
Win+D	Blendet den Desktop ein oder aus.	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden. Problemumgehung: Drücken Sie ⌘-D auf Macs.
Win+M	Minimiert alle Fenster.	
Win+E	Öffnet den Computerordner.	
Win+R	Öffnet das Dialogfeld „Ausführen“.	
Win+Pfeil nach oben	Maximiert das Fenster.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.

Schlüssel	Aktion	Einschränkungen
Win+Pfeil nach unten	Minimiert das Fenster.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach links	Maximiert das App- oder Desktop-Fenster zur linken Seite des Bildschirms.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach rechts	Maximiert das App- oder Desktop-Fenster zur rechten Seite des Bildschirms.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pos1	Minimiert alle Fenster bis auf das aktive Desktop-Fenster.	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden.
Win+Umschalt+Pfeil nach oben	Zieht das Desktop-Fenster nach oben und unten auf.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+G	Wechselt der Reihe nach zu den ausgeführten Desktop-Minianwendungen.	
Win+U	Öffnet das „Center für erleichterte Bedienung“.	

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 3-6. Erforderliche Einstellungen für die Eingabesprache

Sprache	Eingabesprache auf dem lokalen Clientsystem	IME auf dem lokalen Clientsystem erforderlich?	Browser und Eingabesprache auf dem Remote-Desktop	Ist IME auf dem Remote-Desktop erforderlich?
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

Bildschirmauflösung

Wenn ein Remote-Desktop vom Horizon-Administrator mit ausreichend Video-RAM (VRAM) konfiguriert wurde, ist der Webclient in der Lage, die Größe eines Remote-Desktops an die Größe des Browserfensters anzupassen. Standardmäßig sind 36 MB an Video-RAM konfiguriert, d. h. der verfügbare Arbeitsspeicher liegt deutlich 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 Remoteanwendung auf diese Auflösung festlegen. Aktivieren Sie die Option **Modus mit hoher Auflösung** im Fenster „Einstellungen“, das auf der Sidebar verfügbar ist. (Diese Option wird nur im Einstellungsfenster angezeigt, wenn Sie eine hochauflösende oder eine normale Anzeige verwenden, die eine Skalierung größer als 100 % aufweist.)

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

- Die softwarebeschleunigte Grafikfunktion, die ab vSphere 5.0 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 das 3D-Rendern 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 Abschnitt „Festlegen der Arbeitsspeichergröße für bestimmte Monitorkonfigurationen bei der Verwendung von PCoIP“ im Kapitel „Einschätzen der Arbeitsspeicheranforderungen für virtuelle Desktops“ des Dokuments *Planung der View-Architektur*.

H.264-Decodierung

Wenn Sie den Chrome-Browser verwenden, können Sie im HTML Access-Client eine H.264-Decodierung für Remote-Desktop- und -anwendungssitzungen zulassen.

Wenn Sie die H.264-Decodierung zulassen, verwendet der HTML Access-Client diese auch, sofern der Agent H.264-Kodierung unterstützt. Wenn der Agent keine H.264-Kodierung unterstützt, verwendet der HTML Access-Client die JPEG/PNG-Decodierung.

Wenn Sie mit einem Remote-Desktop oder einer Remoteanwendung 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 Remoteanwendung trennen und wiederherstellen, damit die neue Einstellung wirksam wird.

Wenn Sie nicht mit einem Remote-Desktop oder einer Remoteanwendung verbunden sind, können Sie rechts oben im Auswahlbildschirm 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.

Festlegen der Zeitzone

Die in einem Remote-Desktop oder einer Remoteanwendung verwendete Zeitzone wird automatisch als Zeitzone für Ihr lokales System festgelegt. Wenn allerdings bei der Verwendung des HTML Access-Client 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 Remoteanwendung 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.

Die ausgewählte Zone wird als Ihre bevorzugte Zeitzone gespeichert, die bei der Herstellung einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung verwendet werden soll.

Wenn Sie bereits mit einem Remote-Desktop oder einer Remoteanwendung 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 aus der Sidebar aufgerufen werden kann, verfügbar.

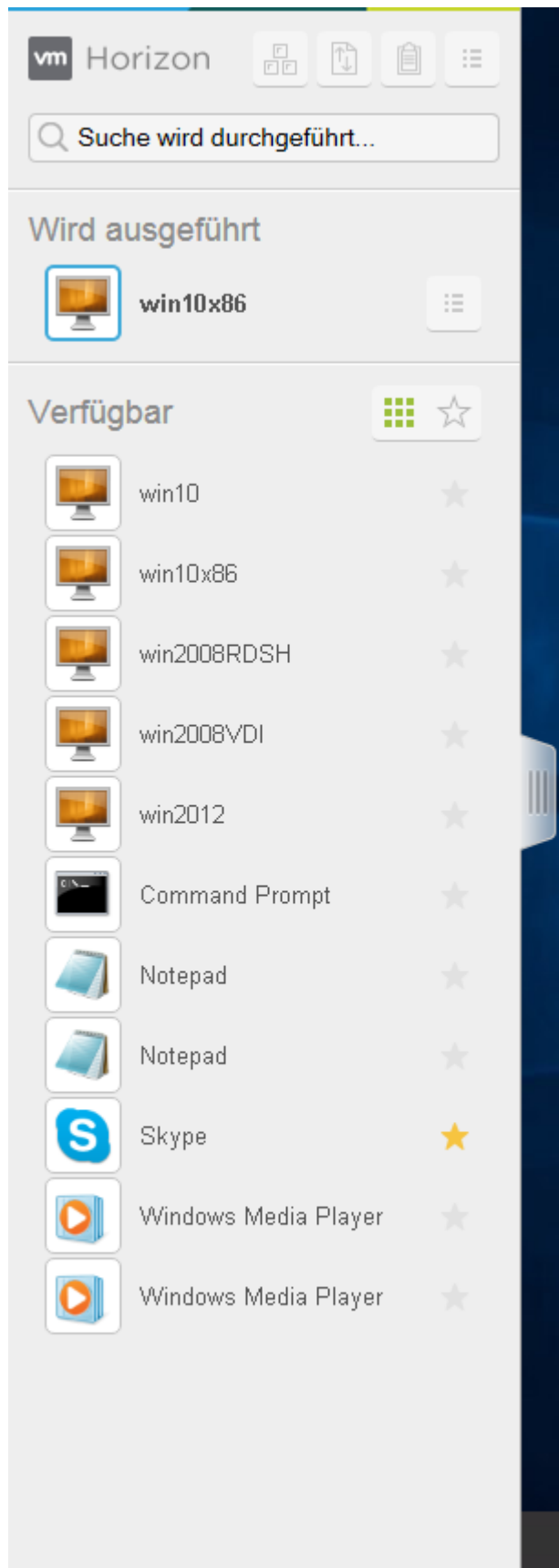
Hinweis Wenn Sie den Chrome-Browser auf einem Android-System verwenden, die Option **Zeitzone automatisch festlegen** auf **true** festgelegt ist und Sie die Zeitzone des Android-Systems ändern, wird die neue Zeitzone nicht automatisch mit dem Remote-Desktop synchronisiert. Dies ist eine Beschränkung von Chrome auf dem Android-System. Um die ausgewählte Zeitzone zu synchronisieren, müssen Sie Android und den Chrome-Browser neu starten.

Verwenden der Sidebar

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

Wenn Sie auf eine Remoteanwendung oder einen Remote-Desktop zugreifen, wird die Sidebar auf der linken Seite des Bildschirms angezeigt. Das Anklicken der Sidebar-Registerkarte blendet die Sidebar ein und aus. Sie können die Registerkarte auch nach oben oder unten verschieben.

Abbildung 3-1. Angezeigte Sidebar beim Starten eines Remote-Desktops oder einer Remoteanwendung



Klicken Sie auf den Erweiterungspfeil neben einer ausgeführten Anwendung und es erscheint die Liste der von dieser Anwendung geöffneten Dokumente. Beachten Sie, dass bei zwei mit eigenständigen Excel-Programmen auf zwei verschiedenen Servern geöffneten Excel-Dokumenten die Excel-Anwendung zweimal in der Liste **Wird ausgeführt** der Sidebar erscheint.

Sie können von der Sidebar aus verschiedene Aktionen ausführen.

Tabelle 3-7. Sidebar-Aktionen

Aktion	Prozedur
Anzeigen der Sidebar	Wenn eine Remoteanwendung oder ein Remote-Desktop geöffnet ist, klicken Sie auf die Registerkarte der Sidebar. Bei geöffneter Sidebar können Sie im Anwendungs- oder Desktop-Fenster weiterhin Aktionen ausführen.
Ausblenden der Sidebar	Klicken Sie auf die Registerkarte der Sidebar.
Starten einer Remoteanwendung oder eines Remote-Desktops	Klicken Sie auf den Namen der Anwendung oder des Desktops unter Verfügbar auf der Sidebar. Die Desktops werden zuerst aufgeführt.
Suchen nach einer Remoteanwendung oder einem Remote-Desktop	<ul style="list-style-type: none"> ■ Klicken Sie auf das Feld Suche und beginnen Sie mit der Eingabe des Namens der Anwendung oder des Desktops. ■ Um eine Anwendung oder einen Desktop zu starten, klicken Sie auf den Namen der Anwendung bzw. des Desktops in den Suchergebnissen. ■ Um zur Startansicht der Sidebar zurückzukehren, tippen Sie im Suchfeld auf X.
Erstellen einer Liste der beliebtesten Anwendungen und Desktops	Klicken Sie auf den grauen Stern neben dem Namen des Desktops oder der Anwendung in der Liste Verfügbar der Sidebar. Sie können dann mit der Schaltfläche Favoriten anzeigen in der Symbolleiste (Sternsymbol) neben Verfügbar eine Liste mit den festgelegten Favoriten aufrufen.
Wechseln zwischen Anwendungen und Desktops	Klicken Sie auf den Namen der Anwendung oder des Desktops in der Liste Wird ausgeführt der Sidebar.
Öffnen des Fensters zum Kopieren und Einfügen	Klicken Sie auf die Schaltfläche Kopieren und Einfügen 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 Kopieren und Einfügen von Text . 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 auf der Seitenleiste auf die Schaltfläche Dateiübertragung , um Dateien vom Remote-Desktop herunterzuladen oder zu diesem hochzuladen. Weitere Informationen dazu finden Sie unter Herunterladen von Dateien von einem Desktop auf den Client und Hochladen von Dateien vom Client zu einem Desktop .
Aktivieren von ⌘-A, ⌘-C, ⌘-V und ⌘-X	Die Option „⌘-A, ⌘-C, ⌘-V und ⌘-X aktivieren“ erscheint im Fenster „Einstellungen“ nur bei Verwendung eines Mac. Klicken Sie auf die Schaltfläche Menü öffnen in der Symbolleiste oben auf der Sidebar und klicken Sie dann auf Einstellungen . 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.

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

Aktion	Prozedur
Aktivieren und Deaktivieren 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 auf die Schaltfläche Menü öffnen in der Symbolleiste oben auf der Sidebar oder klicken Sie auf das Horizon-Logo oben auf der Sidebar und dann auf Hilfe .
Anzeige des Feldes „Info zu VMware Horizon“	Klicken Sie auf die Schaltfläche Menü öffnen in der Symbolleiste oben auf der Sidebar oder klicken Sie auf das Horizon-Logo oben auf der Sidebar und dann auf Info .

Verwenden mehrerer Monitore

Mithilfe eines Chrome-Browsers (Version 55 oder höher) können Sie in HTML Access Web client 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.

Ab HTML Access Web client 4. 5 wird die DPI-Synchronisierung pro Gerät angewendet, wenn die Funktion für mehrere Monitore aktiviert ist. Wenn Sie zwei Monitore mit unterschiedlichen DPI-Einstellungen verwenden, wird für die DPI-Einstellungen auf dem HTML Access-Agenten der DPI-Wert des Monitors des Clientcomputers festgelegt, der zum Starten der HTML Access Web client-Sitzung verwendet wurde.

Verfahren

- 1 Starten Sie Horizon Client 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 **Einstellungen anzeigen** aus.
- 5 Klicken Sie im Dialogfeld „Anzeigeeinstellungen“ auf **Display hinzufügen**.

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

- 6 Ziehen Sie das Fenster „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 „Einstellungen anzeigen“ Ihrer primären Anzeige grün dargestellt.

- 8 Klicken Sie im Fenster „Einstellungen anzeigen“ auf **OK**, wenn Sie die Monitoranzeigen für die Sitzung hinzugefügt haben.

Das Fenster „Einstellungen anzeigen“ 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.

Verwendung der DPI-Synchronisierung

Die DPI-Synchronisierungsfunktion stellt sicher, dass die DPI-Einstellung der Remotesitzung der DPI-Einstellung des Clientcomputers entspricht. Wenn Sie eine neue Remotesitzung starten, legt Horizon Agent den DPI-Wert für die Sitzung auf den DPI-Wert des Clientcomputers fest.

Die DPI-Synchronisierungsfunktion kann die DPI-Einstellung für aktive Remotesitzungen nicht verändern. Wenn Sie die Verbindung zu einer bestehenden Remotesitzung erneut herstellen, führt die Anzeigeskalierungsfunktion eine entsprechende Skalierung für den Remote-Desktop oder die Remoteanwendung durch.

Die DPI-Synchronisierungsfunktion wird automatisch aktiviert, wenn die Einstellung „Modus mit hoher Auflösung“ im Fenster „Einstellungen“ deaktiviert ist. Ab HTML Access Version 4.5 kann, wenn ein Administrator die Gruppenrichtlinieneinstellung Horizon Agent **DPI-Synchronisierung** deaktiviert, die Funktion der DPI-Synchronisierung deaktiviert werden. Das gilt nicht für die Funktion der Anzeigeskalierung. Sie müssen sich abmelden und erneut anmelden, damit Konfigurationsänderungen wirksam werden können. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Die DPI-Synchronisierung erfordert Windows 7 oder höher für Desktops mit Einzelsitzungen, Windows Server 2008 R2 oder höher für veröffentlichte Desktops und Anwendungen auf RDS-Hosts, Horizon Agent 7.0.2 oder höher und HTML Access Version 4.4 oder höher.

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

- Wenn Sie die DPI-Einstellung auf dem Clientcomputer ändern, müssen Sie sich abmelden und erneut anmelden, damit Horizon Client die neue Einstellung auf dem Clientcomputer erkennt. Diese Anforderung gilt auch für Clientcomputer, auf denen Windows 10 ausgeführt wird.

- Wenn Sie eine Remotesitzung auf einem Clientcomputer starten, dessen DPI-Einstellung auf einen Wert über 100 Prozent festgelegt ist, und dann die gleiche Sitzung auf einem anderen Clientcomputer verwenden, dessen DPI-Einstellung auf einen anderen Wert über 100 Prozent festgelegt ist, müssen Sie sich auf dem zweiten Clientcomputer von der Sitzung abmelden und erneut anmelden, damit die DPI-Synchronisierung auf dem zweiten Clientcomputer funktioniert.
- Obwohl Windows 10- und Windows 8.x-Maschinen unterschiedliche DPI-Einstellungen auf unterschiedlichen Monitoren unterstützen, verwendet die DPI-Synchronisierungsfunktion den DPI-Wert, der auf dem Monitor des Clientcomputers 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 Remoteanwendung abmelden, den Webbrowser, in dem Sie die HTML Access-Clientsitzung starten, zu diesem Monitor ziehen und sich erneut beim Remote-Desktop oder bei der Remoteanwendung anmelden, um die DPI-Einstellungen zwischen dem Clientsystem und dem Remote-Desktop bzw. der Remoteanwendung aneinander anzupassen.

Sound

Sie können in Ihren Remote-Desktops und -anwendungen Sound abspielen, wobei einige Einschränkungen zu beachten sind.

Standardmäßig ist die Audiowiedergabe für Remote-Desktops und -anwendungen aktiviert, allerdings kann Ihr View-Administrator eine Richtlinie festlegen, um die Audiowiedergabe zu deaktivieren.

Berücksichtigen Sie die folgenden Richtlinien:

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

Kopieren und Einfügen von Text

Sie haben die Möglichkeit, Text in und aus Remote-Desktops und -anwendungen zu kopieren. Ihr View-Administrator kann diese Funktion so einstellen, dass Kopier- und Einfügevorgänge nur von Ihrem Clientsystem zu einem Remote-Desktop bzw. einer Anwendung oder nur von einem Remote-Desktop bzw. einer Anwendung zu Ihrem Clientsystem zugelassen werden oder beide bzw. keiner der beiden Vorgänge möglich sind.

Die Administratoren konfigurieren die Möglichkeit zum Kopieren/Einfügen durch die Verwendung von Gruppenrichtlinien, die View Agent oder Horizon Agent auf den Remote-Desktops zugeordnet sind. Weitere Informationen finden Sie unter [Gruppenrichtlinieneinstellungen für HTML Access](#).

Administratoren können Gruppenrichtlinien auch dazu verwenden, Zwischenablageformate für das Kopieren/Einfügen zu beschränken. Da HTML Access nur die Übertragung von Text in der Zwischenablage unterstützt, funktionieren nur die Textfilter mit dem HTML Access-Client. Informationen darüber, wie Sie Gruppenrichtlinien zum Filtern von Zwischenablageformaten verwenden, finden Sie im *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*-Dokument.

Sie haben die Möglichkeit, bis zu 1 MB Text zu kopieren, inklusive aller Unicode-Nicht-ASCII-Zeichen. Sie können Text aus Ihrem Clientsystem auf einen Remote-Desktop bzw. in eine Remoteanwendung kopieren und umgekehrt. Beim eingefügten Text handelt es sich aber immer um einfachen Text.

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

Hinweis Die Funktion zum Kopieren und Einfügen wird für iOS Safari und Android-Geräte nicht unterstützt.

Verwenden der Kopier- und Einfügen-Funktion

Für das Kopieren und Einfügen von Text verwenden Sie die Schaltfläche **Kopieren und Einfügen** oben auf der Sidebar.


Diese Prozedur beschreibt die Verwendung des Fensters „Kopieren und Einfügen“ für das Kopieren von Text von Ihrem lokalen Clientsystem in eine Remoteanwendung bzw. umgekehrt von Text von einer Remoteanwendung in Ihr lokales Clientsystem. Wenn Sie nur Text zwischen Remoteanwendungen und Remote-Desktops kopieren und einfügen, können Sie wie gewohnt vorgehen und benötigen dafür nicht das Fenster „Kopieren und Einfügen“.

Das Fenster „Kopieren und Einfügen“, das mit einer Schaltfläche oben in der HTML Access-Sidebar geöffnet werden kann, wird nur für die Synchronisierung der Zwischenablage auf Ihrem lokalen System mit der Zwischenablage des Remotecomputers benötigt.

Der Text im Fenster „Kopieren und Einfügen“ zeigt eine der folgenden Meldungen an, um anzugeben, in welcher Richtung der Benutzer Inhalt kopieren und einfügen kann.

- 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.


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**. (Diese Option erscheint im Fenster „Einstellungen“ nur bei Verwendung eines Mac.)

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

Verfahren

- ◆ So kopieren Sie Text von Ihrem Clientsystem auf den Remote-Desktop oder in die Remoteanwendung:
 - a Kopieren Sie den Text in die lokale Clientanwendung.
 - b In Ihrem Browser klicken Sie auf die Registerkarte der HTML Access-Sidebar, um die Sidebar zu öffnen, und dann auf **Kopieren und Einfügen** oben auf der Sidebar.

Das Fenster „Kopieren und Einfügen“ wird eingeblendet. Sollte in diesem Fenster noch Text von einem früheren Kopiervorgang enthalten sein, wird dieser durch das Einfügen des neu kopierten Textes überschrieben.
 - c Drücken Sie Strg+V (oder -V auf Macs), um den Text in das Fenster einzufügen.

Es wird kurz die folgende Meldung angezeigt: „Die Remote-Zwischenablage wurde synchronisiert.“
 - d Klicken Sie in der Remoteanwendung an die Stelle, an der Sie den Text einfügen möchten, und drücken Sie die Tastenkombination Strg-V.

Der Text wird in die Remoteanwendung eingefügt.
- ◆ So kopieren Sie Text aus Ihrem Remote-Desktop oder Ihrer Remoteanwendung in Ihr Clientsystem:
 - a Kopieren Sie den Text in Ihrer Remoteanwendung.
 - b In Ihrem Browser klicken Sie auf die Registerkarte der HTML Access-Sidebar, um die Sidebar zu öffnen, und dann auf **Kopieren und Einfügen** oben auf der Sidebar.

Das Fenster „Kopieren und Einfügen“ wird mit dem zuvor eingefügten Text dargestellt. Es wird kurz die folgende Meldung angezeigt: „Die Remote-Zwischenablage wurde synchronisiert.“

- c Klicken Sie in das Fenster „Kopieren und Einfügen“ und drücken Sie Strg+C (oder ⌘-C auf Macs), um erneut zu kopieren.

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 Ihrem Clientsystem an die Stelle, an der Sie den Text einfügen möchten, und drücken Sie die Tastenkombination Strg-V.

Der Text wird in die Anwendung auf Ihrem Clientsystem eingefügt.

Übertragen von Dateien zwischen dem Client und einem Remote-Desktop

Mithilfe der Funktion zum Übertragen von Dateien können Sie Dateien zwischen dem Client und einem Remote-Desktop übertragen (hochladen und herunterladen). Die Dateiübertragung zu oder aus Anwendungen wird nicht unterstützt.

Hinweis Diese Funktion ist nicht für die Verwendung mit Linux-Desktops oder Android-Geräten verfügbar.

Der Horizon-Administrator kann die Fähigkeit zum Zulassen, Verweigern oder unidirektionalen Erlauben der Übertragung von Dateien konfigurieren, indem er die Gruppenrichtlinieneinstellung

Dateiübertragung konfigurieren für das VMware Blast-Protokoll ändert. Der Standard lautet nur hochladen. Wenn in der Gruppenrichtlinieneinstellung **Dateiübertragung konfigurieren** der Wert **Upload und Download deaktiviert** für das VMware Blast-Protokoll ausgewählt ist, wird die Schaltfläche **Dateiübertragung** deaktiviert. Ist der Wert **Nur Dateiupload aktiviert** ausgewählt, wird im Dialogfeld **Dateien übertragen** nur die Registerkarte **Hochladen** angezeigt. Ist der Wert **Nur Dateidownload aktiviert** ausgewählt, enthält das Dialogfeld **Dateien übertragen** nur die Registerkarte **Herunterladen**. Weitere Informationen finden Sie unter [Gruppenrichtlinieneinstellungen für HTML Access](#).

Sie können eine Datei mit einer maximalen Dateigröße von 500 MB herunterladen und eine maximal 2 GB große Datei 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 mit einer Größe von 0 weder herunter- noch hochladen.

Safari für iOS und Safari 8 unterstützen weder Up- noch Downloads. Safari 9 oder höher unterstützt keinen Download.

Wenn die Dateiübertragung in einer Desktop-Sitzung im Gange ist und ein Benutzer eine Verbindung zu einem zweiten Desktop öffnet und wenn eine Sicherheitswarnung angezeigt wird (beispielsweise wenn kein gültiges Zertifikat installiert wurde), führt das Ignorieren der Warnung und das Fortsetzen der Verbindung zum zweiten Desktop dazu, dass die Dateiübertragung in der ersten Desktop-Sitzung abgebrochen wird. Dies ist das erwartete Verhalten.

Hinweis Die Fähigkeit zum Herunterladen wird durch die Gruppenrichtlinieneinstellung für die Zwischenablageumleitung beeinflusst. Wenn die Zwischenablageumleitung vom Server zum Client deaktiviert ist, ist der Dateidownload ebenfalls deaktiviert.

Herunterladen von Dateien von einem Desktop auf den Client

Mit Horizon Client können Sie Dateien von einem Remote-Desktop auf einen Clientcomputer herunterladen.

Verfahren

- 1 Klicken Sie oben auf der Seitenleiste auf das Symbol für die Dateiübertragung.
Das Fenster **Dateien übertragen** wird geöffnet.
- 2 Klicken Sie auf **Herunterladen**.
- 3 Wählen Sie mindestens eine Datei auf dem Remote-Desktop aus.
- 4 Drücken Sie Strg+C zum Starten des Downloads.
- 5 Klicken Sie nach Abschluss des Downloads auf das Downloadsymbol, um die Dateien auf dem Clientcomputer zu speichern.

Hochladen von Dateien vom Client zu einem Desktop

Mit Horizon Client können Sie Dateien von der Clientmaschine zu einem Remote-Desktop hochladen.

Verfahren

- 1 Klicken Sie oben auf der Seitenleiste auf das Symbol für die Dateiübertragung.
Das Fenster **Dateien übertragen** wird geöffnet.
- 2 Klicken Sie auf **Hochladen**.
- 3 Ziehen Sie Dateien und legen Sie sie im Fenster **Dateien übertragen** ab, oder klicken Sie auf **Dateien auswählen**, um Dateien auszuwählen.

Die ausgewählten Dateien werden in den Ordner **Eigene Dokumente** hochgeladen.

Wenn Sie bei Internet Explorer 11 und Chrome auf ChromeBook Ordner, Dateien, die eine Größe von 0 KB oder mehr als 2 GB aufweisen, ziehen und ablegen, wird erwartungsgemäß eine Fehlermeldung angezeigt. Nach dem Verwerfen der Fehlermeldung können übertragbare Dateien nicht weiter gezogen und abgelegt werden.

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

Mit der Echtzeit-Audio/Video-Funktion können Sie die Webcam oder das Mikrofon Ihres Clientcomputers auf Ihrem Remote-Desktop oder für eine Remoteanwendung 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. 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 Remoteanwendung 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 Remote-Desktop oder -anwendungssitzung Echtzeit-Audio/Video verwendet wird und Sie eine Verbindung zu einem zweiten Desktop oder einer weiteren Anwendung herstellen (z. B. wenn ein gültiges Zertifikat nicht installiert wurde), kann es zum Ausfall von Echtzeit-Audio/Video in der ersten Sitzung kommen, wenn Sie die Sicherheitswarnung ignorieren und sich mit dem zweiten Desktop oder einer weiteren Anwendung verbinden.

Verwenden der Funktion „Session Collaboration“

Sie können mit der Funktion „Session Collaboration“ andere Benutzer zur Teilnahme an einer vorhandenen Remote-Desktop-Sitzung einladen.

Einladen eines Benutzers zu einer Remote-Desktop-Sitzung

Wenn die Funktion „Session Collaboration“ für einen Remote-Desktop aktiviert ist, können Sie andere Benutzer zur Teilnahme an einer vorhandenen Remote-Desktop-Sitzung einladen.

Standardmäßig können Sie Einladungen zur Teilnahme an einer gemeinsamen Sitzung per E-Mail, in einer Sofortnachricht (Instant Message, Chat) oder durch Kopieren eines Links in die Zwischenablage und Weiterleiten dieses Links an Benutzer senden. Um Einladungen per E-Mail zu versenden, muss eine E-Mail-Anwendung installiert sein. Um per Chat einzuladen, muss Skype for Business installiert und konfiguriert sein. Sie können nur Benutzer einer Domäne einladen, für die der Server die Authentifizierung erlaubt. Es lassen sich standardmäßig bis zu fünf Benutzer einladen.

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.
- Die Funktion „Session Collaboration“ unterstützt keine PCoIP- und RDP-Sitzungen. Sie müssen beim Erstellen einer Remote-Desktop-Sitzung das VMware Blast-Anzeigeprotokoll auswählen.
- 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 für Windows, Mac oder Linux installiert haben oder HTML Access 4.7 verwenden. Wenn ein Sitzungsteilnehmer eine nicht unterstützte Version von Horizon Client verwendet, wird eine Fehlermeldung angezeigt, sobald der Benutzer auf einen Link für eine gemeinsame Sitzung klickt.
- Sie können die Funktion „Session Collaboration“ nicht zur gemeinsamen Nutzung von Linux-Remote-Desktop-Sitzungen oder von Linux-Sitzungen veröffentlichter Anwendungen verwenden.

Voraussetzungen

Damit Benutzer zur Teilnahme an einer Remote-Desktop-Sitzung eingeladen werden können, muss ein Horizon Administrator die Funktion „Session Collaboration“ aktivieren.


Dazu gehört 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 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*. Informationen zur Verwendung von Gruppenrichtlinieneinstellungen zur Konfiguration der Funktion „Session Collaboration“ finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

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 Windows-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. Die Funktion „Session Collaboration“ speichert dann den Benutzer, wenn Sie das nächste Mal seinen Namen oder seine E-Mail-Adresse eingeben.

Es lassen sich standardmäßig bis zu fünf Benutzer einladen. Der Horizon-Administrator kann die maximale Anzahl der Benutzer, die eingeladen werden können, ändern.

- 4 Wählen Sie eine Einladungsmethode aus.

Die folgenden Einladungsmethoden sind standardmäßig verfügbar. Der Horizon-Administrator kann die E-Mail- und Chat-Einladungsmethoden deaktivieren.

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

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 und der Sitzung beitrifft, 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.

Nächste Schritte

Die gemeinsame Sitzung kann im Dialogfeld „VMware Horizon Collaboration“ verwaltet werden. Siehe [Verwalten einer gemeinsamen Sitzung](#).

Verwalten einer gemeinsamen 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 gemeinsamen Sitzung wiedergibt sowie Optionen für bestimmte Aktionen enthält.

Voraussetzungen

Starten Sie eine gemeinsame Sitzung. Siehe [Einladen eines Benutzers zu einer Remote-Desktop-Sitzung](#).

Verfahren

- 1 Klicken Sie im Remote-Desktop auf das Symbol von VMware Horizon Collaboration in der Taskleiste oder doppelklicken Sie auf das Symbol von VMware Horizon Collaboration auf dem Desktop.

Die Namen aller Teilnehmer der Sitzung werden in der Spalte „Name“ und deren Status in der Spalte „Status“ angezeigt.
- 2 Mit dem VMware Horizon Session Collaboration-Dashboard können Sie die gemeinsame Sitzung verwalten.

Option	Aktion
Einladung widerrufen oder Teilnehmer entfernen	Klicken Sie in der Spalte „Status“ auf Entfernen .
Kontrolle an Sitzungsteilnehmer übergeben	Nachdem ein Teilnehmer der Sitzung beigetreten ist, setzen Sie die Umschaltoption in der Spalte „Steuerung“ auf Ein . Um die Steuerung der Sitzung wieder zu übernehmen, doppelklicken Sie oder drücken Sie eine beliebige Taste. Der Sitzungsteilnehmer kann die Steuerung ebenfalls zurückgeben, indem er die Umschaltoption in der Spalte „Steuerung“ auf Aus setzt oder auf die Schaltfläche Steuerung zurückgeben klickt.

Option	Aktion
Teilnehmer hinzufügen	Klicken Sie auf Teilnehmer hinzufügen .
Gemeinsame Sitzung beenden	Klicken Sie auf Teilnahme beenden . Die Verbindung mit allen aktiven Teilnehmern wird getrennt. Sie können die gemeinsame Sitzung auch durch Klicken auf das Symbol von VMware Horizon Session Collaboration auf dem Desktop und durch Klicken auf die Schaltfläche Anhalten beenden.

Teilnehmen an einer gemeinsamen Sitzung

Um an einer gemeinsamen Sitzung teilzunehmen, klicken Sie auf den Link in der Einladung zur Teilnahme. 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 gemeinsame Sitzung im Fenster für die Remote-Desktop- und -anwendungsauswahl doppelzuklicken.

Dieser Vorgang beschreibt, wie Sie einer gemeinsamen Sitzung über eine Einladung zur Teilnahme 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.

Die folgenden Remote-Desktop-Funktionen stehen in einer gemeinsamen Sitzung nicht zur Verfügung.

- Echtzeit-Audio/Video (RTAV)
- Standortbasierter Druck
- Zwischenablagenumleitung

Die Auflösung des Remote-Desktops kann in einer gemeinsamen Sitzung nicht geändert werden.

Voraussetzungen

Um an einer gemeinsamen 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 für VMware Horizon Session 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**.

Abmelden oder trennen

Wenn Sie die Verbindung mit einem Remote-Desktop trennen, ohne sich abzumelden, bleiben bei einigen Konfigurationen die Anwendungen im Desktop 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 Desktop (ohne sich abzumelden) oder beenden Sie die gehostete Anwendung.

Option	Aktion
Im Auswahlbildschirm für Desktops und Anwendungen vor der Herstellung einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung	Klicken Sie in der rechten oberen Ecke des Bildschirms auf die Schaltfläche Abmelden der Symbolleiste.
In der Sidebar nach hergestellter Verbindung mit einem Remote-Desktop oder einer Remoteanwendung	Klicken Sie oben auf der Seitenleiste auf die Symbolleistenschaltfläche Abmelden .

- ◆ Schließen Sie eine veröffentlichte Anwendung.

Option	Aktion
In der Anwendung	Beenden Sie die Anwendung auf die übliche Weise. Klicken Sie beispielsweise in der Ecke des Anwendungsfensters auf die Schaltfläche X (Schließen).
In der Sidebar	Klicken Sie auf das X neben dem Dateinamen der Anwendung in der Liste Wird ausgeführt der Sidebar.

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

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Melden Sie sich über das Windows- Start -Menü ab.
In der Sidebar	<p>Um sich abzumelden und die Verbindung zu trennen, klicken Sie auf die Schaltfläche Menü öffnen neben dem Namen des Desktops in der Liste Wird ausgeführt der Sidebar und wählen Sie Abmelden. 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 Menü öffnen neben dem Namen des Desktops in der Liste Wird ausgeführt und wählen Sie Schließen.</p> <p>Hinweis Der 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 Desktop geschlossen.</p>
Verwendung eines URI	Verwenden Sie zum Abmelden den URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=logoff</code> .

Zurücksetzen eines Remote-Desktops oder von 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. Durch das Zurücksetzen von veröffentlichten Anwendungen werden alle geöffneten Anwendungen beendet.

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.

Das Zurücksetzen von veröffentlichten Anwendungen entspricht dem Beenden der Anwendungen, wobei nicht gespeicherte Daten verloren gehen. Alle geöffneten veröffentlichten Anwendungen werden geschlossen, auch die Anwendungen, die zu verschiedenen RDS-Serverfarmen gehören.

Sie können einen Remote-Desktop nur zurücksetzen, wenn ein Horizon-Administrator die Funktion zum Zurücksetzen eines Desktops für den Desktop 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
Zurücksetzen von veröffentlichten Anwendungen im Bildschirm zur Auswahl von Anwendungen	Im Bildschirm zur Auswahl von Desktops und Anwendungen 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 Einstellungen in der Symbolleiste rechts oben im Bildschirm und dann auf Zurücksetzen .
Zurücksetzen eines Remote-Desktops auf der Sidebar	Besteht eine Verbindung mit einem Remote-Desktop, klicken Sie auf die Schaltfläche Menü öffnen in der Symbolleiste neben dem Namen des Desktops in der Liste Wird ausgeführt der Sidebar und wählen Sie Zurücksetzen .
Zurücksetzen von veröffentlichten Anwendungen auf der Sidebar	Um alle ausgeführten Anwendungen zurückzusetzen, klicken Sie auf die Schaltfläche Einstellungenfenster öffnen in der Symbolleiste oben auf der Sidebar und klicken Sie dann auf Zurücksetzen .
Zurücksetzen eines Remote-Desktops mithilfe eines URI	Verwenden Sie zum Zurücksetzen eines Remote-Desktops den URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=reset</code> .

Wenn Sie einen Remote-Desktop zurücksetzen, wird das Betriebssystem im Remote-Desktop neu gestartet und Horizon Client getrennt bzw. vom Desktop abgemeldet. Wenn Sie veröffentlichte Anwendungen zurücksetzen, werden diese beendet.

Nächste Schritte

Warten Sie eine Weile, bis das System gestartet wurde, und versuchen Sie anschließend erneut, eine Verbindung mit dem Remote-Desktop oder der veröffentlichten Anwendung herzustellen.

Neustarten eines Remote-Desktops

Eventuell muss ein Remote-Desktop neu gestartet werden, wenn das Desktop-Betriebssystem nicht mehr reagiert. Der Neustart eines Remote-Desktops entspricht dem Neustart des Windows-Betriebssystems. In der Regel werden Sie dabei vom 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 eines Desktops für den Desktop 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 Menü öffnen in der Symbolleiste neben dem Namen des Desktops in der Liste Wird ausgeführt der Sidebar und wählen Sie Neu starten .
Verwenden eines URI	Verwenden Sie zum Neustart eines Desktops den URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=restart</code> .

Das Betriebssystem im Remote-Desktop wird neu gestartet und Horizon Client wird getrennt bzw. vom Desktop abgemeldet.

Nächste Schritte

Warten Sie eine Weile, bis das System 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 eines Remote-Desktops oder von veröffentlichten Anwendungen](#).