

# Verwendung von VMware Horizon View Client für Mac OS X

Januar 2014  
Horizon View

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter <http://www.vmware.com/de/support/pubs>.

DE-000668-00

**vmware**<sup>®</sup>

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

<http://www.vmware.com/de/support/>

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

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

Copyright © 2010–2014 VMware, Inc. Alle Rechte vorbehalten. [Informationen zu Copyright und Marken.](#)

**VMware, Inc.**

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

**VMware Global, Inc.**

Zweigniederlassung Deutschland  
Freisinger Str. 3  
85716 Unterschleißheim/Lohhof  
Germany  
Tel.: +49 (0) 89 3706 17000  
Fax: +49 (0) 89 3706 17333  
[www.vmware.com/de](http://www.vmware.com/de)

# Inhalt

Verwendung von VMware Horizon View Client für Mac OS X	5
<b>1 Konfiguration und Installation</b>	<b>7</b>
Systemanforderungen für Mac-Clients	7
Systemanforderungen für Echtzeit-Audio/Video	8
Unterstützte Desktop-Betriebssysteme	9
Vorbereiten des View-Verbindungsservers für Horizon View Client	9
Konfigurieren der im View Portal angezeigten View Client-Download-Links	9
Installieren von Horizon View Client auf Mac OS X	11
Hinzufügen von Horizon View Client zu Ihrem Dock	12
Konfigurieren der Zertifikatsprüfungen für Endbenutzer	12
Durch VMware gesammelte Horizon View Client -Daten	13
<b>2 Verwenden von URIs zur Konfiguration von Horizon View Client</b>	<b>15</b>
Syntax für die Erstellung von vmware-view-URIs	16
Beispiele für vmware-view-URIs	18
<b>3 Verwaltung der Serververbindungen und Desktops</b>	<b>21</b>
Erstmaliges Anmelden an einem Remote-Desktop	21
Zertifikatsprüfungsmodi für Horizon View Client	23
Suchen nach Desktops	24
Wechseln zwischen Desktops	25
Abmelden oder Trennen von Desktops	25
Entfernen einer View Server-Verknüpfung von der Startseite	26
Neuanordnen von View Server- und Remote-Desktop-Verknüpfungen	27
Rollback eines Desktops	27
<b>4 Verwenden eines Microsoft Windows-Desktops auf einem Mac</b>	<b>29</b>
Funktionsunterstützungs-Matrix	29
Internationalisierung	30
Monitore und Bildschirmauflösung	30
Verbinden von USB-Geräten	31
Konfigurieren der USB-Umleitung auf einem Mac OS X-Client	33
Eigenschaften der USB-Umleitung	35
USB-Gerätefamilien	37
Aktivieren der Protokollierung für die USB-Umleitung	38
Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone	39
In diesen Fällen können Sie Ihre Webcam verwenden	39
Auswählen eines Standardmikrofons auf einem Mac OS X-Clientsystem	40
Konfigurieren von Echtzeit-Audio/Video auf einem Mac OS X-Client	40

Konfigurieren einer bevorzugten Webcam oder eines bevorzugten Mikrofons auf einem Mac OS X-Clientsystem	41
Kopieren und Einfügen von Text und Bildern	43
Drucken von einem Remote-Desktop aus	44
Aktivieren des virtuellen Drucks auf dem Mac OS X-Client	44
Festlegen von Druckeinstellungen für die virtuelle Druckfunktion	45
Verwenden von USB-Druckern	46
PCoIP-Client-Bildcache	46
<b>5 Fehlerbehebung für Horizon View Client</b>	<b>49</b>
Zurücksetzen eines Desktops	49
Deinstallieren von Horizon View Client	50
 Index	 51

# Verwendung von VMware Horizon View Client für Mac OS X

---

Dieses Handbuch, *Verwendung von VMware Horizon View Client für Mac OS X*, bietet Informationen über die Installation und Verwendung der VMware® Horizon View™-Software auf einem Mac-Rechner zur Herstellung einer Verbindung mit einem Remote-Desktop im Rechenzentrum.

Die Informationen in diesem Dokument enthalten Systemanforderungen und Anleitungen zur Installation und Verwendung von Horizon View Client für Mac OS X.

Diese Informationen sind für Administratoren vorgesehen, die eine Bereitstellung von Horizon View mit Mac-Clientgeräten ermöglichen müssen. Die Informationen wurden für erfahrene Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen sowie mit Rechenzentrum-Vorgängen vertraut sind.



# Konfiguration und Installation

---

Bei der Einrichtung einer Horizon View-Bereitstellung für Mac-Clients müssen bestimmte View-Verbindungsserver-Konfigurationseinstellungen verwendet, die Systemanforderungen für View Server und Mac-Clients erfüllt und Horizon View Client für Mac von der VMware-Website heruntergeladen und installiert werden.

Dieses Kapitel behandelt die folgenden Themen:

- [„Systemanforderungen für Mac-Clients“](#), auf Seite 7
- [„Systemanforderungen für Echtzeit-Audio/Video“](#), auf Seite 8
- [„Unterstützte Desktop-Betriebssysteme“](#), auf Seite 9
- [„Vorbereiten des View-Verbindungservers für Horizon View Client“](#), auf Seite 9
- [„Konfigurieren der im View Portal angezeigten View Client-Download-Links“](#), auf Seite 9
- [„Installieren von Horizon View Client auf Mac OS X“](#), auf Seite 11
- [„Hinzufügen von Horizon View Client zu Ihrem Dock“](#), auf Seite 12
- [„Konfigurieren der Zertifikatsprüfungen für Endbenutzer“](#), auf Seite 12
- [„Durch VMware gesammelte Horizon View Client-Daten“](#), auf Seite 13

## Systemanforderungen für Mac-Clients

Sie können Horizon View Client für Mac OS X auf allen Intel-basierten Modellen installieren, die Mac OS X 10.6.8 oder ein höheres Betriebssystem verwenden.

Sowohl der Mac, auf dem Sie Horizon View Client installieren, als auch die Peripheriegeräte müssen bestimmte Systemanforderungen erfüllen.

<b>Modell</b>	Intel-basierter Mac
<b>Arbeitsspeicher</b>	Mindestens 2GB Arbeitsspeicher (RAM)
<b>Betriebssysteme</b>	<ul style="list-style-type: none"> <li>■ Horizon View Client für Mac OS X 2.2 und 2.3: Mac OS X Snow Leopard (10.6.8), Mac OS X Lion (10.7), Mac OS X Mountain Lion (10.8) und Mac OS X Mavericks (10.9)</li> <li>■ Horizon View Client für Mac OS X 2.0 und 2.1: Mac OS X Snow Leopard (10.6.8), Mac OS X Lion (10.7) und Mac OS X Mountain Lion (10.8)</li> <li>■ View Client für Mac OS X 1.6 und 1.7: Mac OS X Snow Leopard (10.6.8), Mac OS X Lion (10.7) und Mac OS X Mountain Lion (10.8)</li> </ul>

	<ul style="list-style-type: none"><li>■ View Client für Mac OS X 1.4 und 1.5: Mac OS X Snow Leopard (10.6.8) und Mac OS X Lion (10.7)</li></ul>
<b>View-Verbindungsserver, Sicherheitsserver und View Agent</b>	Aktuelle Wartungsversion von VMware View 4.6.x und spätere Versionen Wenn Clientsysteme von außerhalb der firmeneigenen Firewall eine Verbindung herstellen, empfiehlt VMware die Verwendung eines Sicherheitservers. Mit einem Sicherheitsserver erfordern die Clientsysteme keine VPN-Verbindung.
<b>Anzeigeprotokoll für Horizon View</b>	PCoIP oder RDP
<b>Softwareanforderungen für RDP</b>	Microsoft Remotedesktopverbindungs-Client für Mac, Version 2.0 bis 2.1.1. Dieser Client steht auf der Microsoft-Website zum Download zur Verfügung. <hr/> <b>HINWEIS</b> Horizon View Client für Mac OS X ist nicht mit Microsoft Remotedesktop 8.0 und höheren Versionen kompatibel. <hr/>
<b>Softwareanforderungen für den virtuellen Druck</b>	Horizon View Client 2.1 oder höher

## Systemanforderungen für Echtzeit-Audio/Video

Echtzeit-Audio/Video arbeitet mit Standardwebcams, USB-Audio- und analogen Audiogeräten und kann mit standardmäßigen Konferenzanwendungen wie z. B. Skype, WebEx und Google Hangouts verwendet werden. Zur Unterstützung von Echtzeit-Audio/Video muss Ihre Horizon View-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

<b>Horizon View-Remote-Desktop</b>	Auf den Desktops muss View Agent 5.2 oder später installiert sein. Auf den Desktops muss außerdem die entsprechende Version von Remote Experience Agent installiert sein. Wenn View Agent 5.3 installiert ist, müssen Sie auch Remote Experience Agent aus dem Horizon View 5.3 Feature Pack 1 installieren. Weitere Informationen finden Sie im Dokument <i>Installation und Verwaltung von VMware Horizon View Feature Pack</i> für VMware Horizon View-
<b>Horizon View Client-Software</b>	Horizon View Client 2.3 für Mac OS X oder höher
<b>Horizon View Client-Computer oder Clientzugriffsgesamt</b>	<ul style="list-style-type: none"><li>■ Echtzeit-Audio/Video wird unter Mac OS X Mountain Lion (10.8) und höher unterstützt. Auf allen älteren Mac OS X-Betriebssystemen ist diese Funktion deaktiviert.</li><li>■ Auf dem Clientcomputer müssen Treiber für Webcam und Audiogeräte installiert sein, und die Webcam oder das Audiogerät muss betriebsbereit sein. Zur Unterstützung von Echtzeit-Audio/Video ist es nicht erforderlich, die Gerätetreiber auf dem Desktop-Betriebssystem zu installieren, auf dem View Agent installiert ist.</li></ul>
<b>Anzeigeprotokoll für Horizon View</b>	PCoIP Echtzeit-Audio/Video wird in RDP-Desktop-Sitzungen nicht unterstützt.



## Unterstützte Desktop-Betriebssysteme

Administratoren erstellen virtuelle Maschinen mit einem Gastbetriebssystem und installieren View Agent auf diesem Gastbetriebssystem. Die Endbenutzer können sich an diesen virtuellen Maschinen von einem Client-Gerät aus anmelden.

Eine Liste mit unterstützten Gastbetriebssystemen finden Sie unter dem Thema „Unterstützte Betriebssysteme für View Agent“ in der Dokumentation „Installation von Horizon View 4.6.x oder 5.x“.

## Vorbereiten des View-Verbindungsservers für Horizon View Client

Administratoren müssen bestimmte Aufgaben durchführen, um Endbenutzern die Verbindung zu den Remote-Desktops zu ermöglichen.

Bevor Endbenutzer eine Verbindung mit dem View-Verbindungsserver oder einem Sicherheitsserver herstellen und auf einen Remote-Desktop zugreifen können, müssen bestimmte Pool- und Sicherheitseinstellungen konfiguriert werden:

- Wenn Sie einen Sicherheitsserver verwenden, wie von VMware empfohlen, stellen Sie sicher, dass Sie die aktuellen Wartungsversionen für einen View-Verbindungsserver der Version 4.6.x und für einen View-Sicherheitsserver der Version 4.6.x oder höher verwenden. Siehe die Dokumentation *Installation von VMware Horizon View*.
- Wenn Sie eine sichere Tunnelverbindung für Clientgeräte verwenden möchten und die sichere Verbindung mit einem DNS-Hostnamen für den View-Verbindungsserver oder einen Sicherheitsserver konfiguriert ist, muss sichergestellt werden, dass das Clientgerät diesen DNS-Namen auflösen kann.  
  
Navigieren Sie zur Aktivierung oder Deaktivierung der sicheren Tunnelverbindung in View Administrator auf das Dialogfeld View-Verbindungsserver-Einstellungen bearbeiten und setzen Sie einen Haken in das Kontrollkästchen **Sichere Tunnelverbindung zum Desktop verwenden**.
- Vergewissern Sie sich, dass ein Desktop-Pool erstellt wurde und das Benutzerkonto, das Sie verwenden möchten, über die Rechte zum Zugriff auf diesen Remote-Desktop verfügt. Siehe Hilfetemen zur Erstellung von Desktop-Pools in der Dokumentation *Verwaltung von VMware Horizon View*.
- Zum Verwenden der zweistufigen Authentifizierung für Horizon View Client, z. B. der RSA SecurID- oder RADIUS-Authentifizierung, müssen Sie diese Funktion auf dem View-Verbindungsserver aktivieren. Die RADIUS-Authentifizierung ist bei View-Verbindungsservern mit View 5.1 oder höher verfügbar. Weitere Informationen finden Sie in den Themen über zweistufige Authentifizierung in der Dokumentation *Verwaltung von VMware Horizon View*.

## Konfigurieren der im View Portal angezeigten View Client-Download-Links

Standardmäßig enthält die Portalseite, die angezeigt wird, wenn Sie einen Browser öffnen und die URL einer View-Verbindungsserverinstanz eingeben, Links zur VMware-Download-Site, um Horizon View Client herunterzuladen. Die Standard können geändert werden.

Die Standardlinks für Horizon View Client auf der Portalseite sorgen dafür, dass Sie zu den derzeit kompatiblen Horizon View Client-Installationsprogrammen umgeleitet werden. In einigen Fällen sollen die Links jedoch auf einen internen Webserver verweisen oder Sie möchten bestimmte Clientversionen auf Ihrem eigenen View-Verbindungsserver zur Verfügung stellen. Sie können die Seite neu konfigurieren, sodass sie auf eine andere URL verweist.

Wenn Sie Links für Mac OS X-, Linux- und Windows-Clientsysteme erstellen, wird der entsprechende Link zum jeweiligen Betriebssystem auf der Portalseite angezeigt. Wenn Sie beispielsweise die Portalseite auf einem Windows-System öffnen, werden die Links für die Windows-Installationsprogramme angezeigt. Sie können auch separate Links für die 32-Bit- und 64-Bit-Installationsprogramme erstellen. Sie können auch Links für iOS- und Android-Systeme erstellen. Diese Betriebssysteme werden jedoch nicht automatisch erkannt, sodass Sie beispielsweise beim Öffnen der Portalseite auf einem iPad die Links für iOS und Android sehen, sofern Sie Links für die beiden erstellt haben.

---

**WICHTIG** Wenn Sie die Portalseiten-Links anpassen, wie in diesem Thema beschrieben, und später VMware Horizon View HTML Access auf dem Server installieren, wird Ihre benutzerdefinierte Portalseite durch eine HTML-Zugriff-Seite ersetzt. Informationen zum Anpassen dieser Seite finden Sie unter *Verwendung von VMware Horizon View HTML Access*.

---

### Voraussetzungen

- Laden Sie die Installationsdateien für die Horizon View Client-Typen herunter, die Sie in Ihrer Umgebung einsetzen möchten. Die URL für die Client-Download-Seite ist <https://www.vmware.com/go/viewclients>.
- Legen Sie fest, auf welchem HTTP-Server die Installationsdateien liegen sollen. Die Dateien können sich auf einer View-Verbindungsserver-Instanz oder auf einem anderen HTTP-Server befinden.

### Vorgehensweise

- 1 Erstellen Sie auf dem HTTP-Server, auf dem sich die Installationsdateien befinden sollen, einen Ordner für die Dateien des Installationsprogramms.

Um die Dateien beispielsweise in einen Ordner `downloads` im Standardinstallationsverzeichnis auf dem View-Verbindungsserver-Host zu stellen, verwenden Sie den folgenden Pfad:

```
C:\Programme\VMware\VMware View\Server\broker\webapps\downloads
```

Die Links zu den Dateien würden dann URLs mit dem Format `https://Servername/downloads/Client-Installer-Dateiname` verwenden. Ein Server mit dem Namen `view.mycompany.com` kann die folgende URL für View Client für Windows verwenden: `https://view.mycompany.com/downloads/VMware-Horizon-View-Client.exe`. Bei diesem Beispiel befindet sich der Ordner mit dem Namen `downloads` im Stammordner `webapps`.

- 2 Kopieren Sie die Installationsdateien in den Ordner.

Wenn sich der Ordner auf einem View-Verbindungsserver-Dienst neu befindet, können Sie alle Dateien in diesem Ordner ersetzen, ohne den VMware View-Verbindungsserver-Dienst neu starten zu müssen.

- 3 Kopieren Sie auf dem View-Verbindungsserver die Datei `portal-links.properties` und die Datei `portal.properties`, die sich unter `Installationspfad\Server\Extras\PortalExamples` befinden.
- 4 Legen Sie einen Ordner `portal` im Verzeichnis `C:\ProgramData\VMware\VDM` an, und kopieren Sie die Dateien `portal-links.properties` und `portal.properties` in den Ordner `portal`.
- 5 Bearbeiten Sie die Datei `C:\ProgramData\VMware\VDM\portal\portal-links.properties` so, dass sie auf den neuen Speicherort der Installationsdateien verweist.

Sie können die Zeilen in dieser Datei bearbeiten und ihnen weitere hinzufügen, falls Sie weitere Links erstellen müssen. Sie können auch Zeilen löschen.

Die folgenden Beispiele zeigen Eigenschaften zum Erstellen von zwei Links für View Client für Windows sowie zwei Links für View Client für Linux:

```
link.win=https://<varname id="VARNAME_B2B27F517DB04754B1CCF5F1411BA59E">server-name</varname>/downloads/VMware-Horizon-View-Client-x86_64-<varname id="VARNAME_ME_7CD50CBABC614BCD976B2575FEDEF1F2">y.y.y-XXXX</varname>.exe#win
link.win.1=https://<varname id="VARNAME_8243922EA8B44DC3A2E9A360C4DDC304">server-name</varname>
```

```
me>/downloads/VMware-Horizon-View-Client-<varname id="VARNA-
ME_9D2A6519E01D4ADA9B701FDB8785B141">y.y.y-XXXX</varname>.exe#win
link.linux=https://<varname id="VARNAME_C62EA29FFF1047D1A350C57AD8006223">server-name</varna-
me>/downloads/VMware-Horizon-View-Client-x86_64-<varname id="VARNA-
ME_B664011E02154BBD9479411042551944">y.y.y-XXXX</varname>.rpm#linux
link.linux.1=https://<varname id="VARNAME_C498001B66334F39A59E2610D499EAA8">server-name</var-
name>/downloads/VMware-Horizon-View-Client-<varname id="VARNA-
ME_D5652EFD7B75490F873921D2AFF8D9B0">y.y.y-XXXX</varname>.tar.gz#linux
```

Bei diesem Beispiel gibt `y.y.y-XXXX` die Versions- und Build-Nummer an. Der Text `win` am Ende der Zeile weist darauf hin, dass dieser Link im Browser angezeigt werden soll, wenn der Client über ein Windows-Betriebssystem verfügt. Verwenden Sie `win` für Windows, `linux` für Linux und `mac` für Mac OS X. Verwenden Sie für andere Betriebssysteme `unknown`.

- 6 Bearbeiten Sie für Text die Datei `C:\ProgramData\VMware\VDM\portal\portal.properties` so, dass sie den anzuzeigenden Text für die Links angibt.

Diese Zeilen stehen im Abschnitt der Datei namens `# keys based on key names in portal-links.properties` zur Verfügung.

Das folgende Beispiel zeigt den Text, der den für `link.win` und `link.win.1` angegebenen Links entspricht:

```
text.win=View Client for Windows 32 bit Client users
text.win.1=View Client for Windows 64 bit Client users
```

- 7 Starten Sie den VMware View-Verbindungsserver-Dienst neu.

Wenn Endbenutzer den View-Verbindungsserver öffnen, sehen sie Links mit dem von Ihnen angegebenen Text. Die Links verweisen auf die von Ihnen angegebenen Stellen.

## Installieren von Horizon View Client auf Mac OS X

Endbenutzer öffnen Horizon View Client, um von einem physischen Mac OS X-Computer eine Verbindung zu Remote-Desktops herstellen zu können. Horizon View Client wird auf Mac OS X-Clientsystemen von einer Festplatten-Image-Datei aus installiert.

### Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „[Systemanforderungen für Mac-Clients](#)“, auf Seite 7.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Wenn Sie beabsichtigen, das RDP-Anzeigeprotokoll zur Verbindung mit einem Remote-Desktop zu verwenden, müssen Sie vorab sicherstellen, dass auf dem Mac-Clientsystem der Microsoft Remotedesktopverbindungs-Client für Mac (Version 2.0 oder höher) installiert ist.
- Stellen Sie sicher, dass Sie über die URL für eine Download-Seite verfügen, auf der sich das VMware Horizon View Client-Installationsprogramm befindet. Bei dieser URL kann es sich um die VMware Downloads-Seite unter <http://www.vmware.com/go/viewclients> oder um die URL für eine View-Verbindungsserver-Instanz handeln.

Wenn Sie zu einer View-Verbindungsserver-URL navigieren, verweisen die Links auf dieser Portalseite standardmäßig auf die VMware Downloads-Seite. Sie können die Links konfigurieren, sodass sie auf einen anderen Speicherort verweisen. Weitere Informationen finden Sie unter „[Konfigurieren der im View Portal angezeigten View Client-Download-Links](#)“, auf Seite 9. Je nach Konfiguration dieser Seite wird unter Umständen auch ein Link für VMware Horizon View HTML Access angezeigt.

HTML-Zugriff ermöglicht es Ihnen, eine Verbindung zu einem virtuellen Desktop über den Browser herzustellen, ohne Clientsoftware installieren zu müssen. VMware Horizon View Client bietet mehr Funktionen und eine höhere Leistung als der HTML Access-Client, weshalb VMware im Allgemeinen die Installation der Clientsoftware empfiehlt.

### Vorgehensweise

- 1 Navigieren Sie auf Ihrem Mac zur URL zum Herunterladen der Horizon View Client-Installationsdatei. Das Dateinamensformat ist `VMware-Horizon-View-Client-y.y.y-xxxxxx.dmg`, wobei `xxxxxx` die Build-Nummer und `y.y.y` die Versionsnummer ist.
- 2 Klicken Sie zum Öffnen doppelt auf die `.dmg`-Datei und anschließend auf **Akzeptieren**. Die Inhalte des Festplatten-Image werden in einem Horizon View Client-Finder-Fenster angezeigt.
- 3 Ziehen Sie im Finder-Fenster das Symbol **View Client VMware Horizon View** zum Symbol **Anwendungsordner**. Wenn Sie nicht als Administrator angemeldet sind, werden Sie nach dem Administrator-Benutzernamen und -Kennwort gefragt.

### Weiter

Starten Sie Horizon View Client und stellen Sie sicher, dass Sie sich am richtigen Remote-Desktop anmelden können. Siehe „[Erstmaliges Anmelden an einem Remote-Desktop](#)“, auf Seite 21.

## Hinzufügen von Horizon View Client zu Ihrem Dock

Sie können Horizon View Client auf dieselbe Weise wie alle anderen Anwendungen zu Ihrem Dock hinzufügen.

### Vorgehensweise

- 1 Wählen Sie im **Anwendungen-Ordner** **VMware Horizon View Client** aus.
- 2 Ziehen Sie das Symbol **VMware Horizon View Client** zum Dock.
- 3 Wenn Sie das Dock-Symbol so konfigurieren möchten, dass Horizon View Client beim Anmelden geöffnet oder das Symbol im Finder angezeigt wird, wählen Sie **Optionen** und dann den entsprechenden Befehl im Kontextmenü aus.

Wenn Sie Horizon View Client beenden, verbleibt die Anwendungsverknüpfung im Dock.

## Konfigurieren der Zertifikatsprüfungen für Endbenutzer

Administratoren können den Zertifikatüberprüfungsmodus so konfigurieren, dass beispielsweise immer die vollständige Überprüfung durchgeführt wird.

Die Zertifikatsprüfung wird für SSL-Verbindungen zwischen View-Verbindungsserver und Horizon View Client durchgeführt. Die Administratoren können den Überprüfungsmodus so konfigurieren, dass eine der folgenden Strategien verwendet wird:

- Die Endbenutzer wählen selbst den Überprüfungsmodus. In der restlichen Liste werden die drei Überprüfungsmodi beschrieben.
- (Keine Überprüfung) Es werden keine Zertifikatsprüfungen durchgeführt.
- (Warnen) Die Endbenutzer werden gewarnt, wenn der Server ein selbstsigniertes Zertifikat vorlegt. Die Benutzer können dann selbst entscheiden, ob sie diesen Verbindungstyp zulassen.
- (Volle Sicherheit) Es wird eine vollständige Überprüfung durchgeführt. Die Verbindungen, für die diese Prüfung nicht erfolgreich verläuft, werden abgelehnt.

Einzelheiten zu den verschiedenen Arten der durchgeführten Überprüfungen finden Sie unter „[Zertifikatprüfungsmodi für Horizon View Client](#)“, auf Seite 23.

Sie können den Überprüfungsmodus so einstellen, dass er von den Endbenutzern nicht geändert werden kann. Legen Sie den Schlüssel „Security Mode“ in der Datei `/Library/Preferences/com.vmware.view.plist` auf den Mac-Clients auf einen der folgenden Werte fest:

- 1 implementiert Nie mit nicht vertrauenswürdigen Servern verbinden.
- 2 implementiert Warnung vor Verbindung mit nicht vertrauenswürdigen Servern ausgeben.
- 3 implementiert Server-Identitätszertifikate nicht überprüfen.

## Durch VMware gesammelte Horizon View Client -Daten

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

---

**HINWEIS** Diese Funktion ist nur verfügbar, wenn Ihre Horizon View-Bereitstellung den View-Verbindungsserver der Version 5.1 oder einer höheren Version verwendet. Client-Informationen werden für Clients mit View Client 1.7 und höher gesendet.

---

VMware sammelt die Daten auf den Clients zur Priorisierung der Hardware- und Softwarekompatibilität. Wenn sich ein Administrator Ihres Unternehmens 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 Horizon View Client-Informationen werden erst an den View-Verbindungsserver und dann an VMware gesendet, zusammen mit den Daten der Horizon View-Server, Desktop-Pools und Remote-Desktops.

Auch wenn die Informationen bei der Übertragung an den View-Verbindungsserver verschlüsselt werden, werden die Informationen des Client-Systems unverschlüsselt in einem benutzerspezifischen Verzeichnis protokolliert. Die Protokolle enthalten jedoch keine personen- oder unternehmensbezogenen Informationen.

Zur Teilnahme am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit kann der Administrator, der die Installation des View-Verbindungsservers durchführt, bei der Ausführung des Installations-Assistenten für den View-Verbindungsserver diese Option „abonnieren“ oder nach der Installation eine entsprechende Option in View Administrator festlegen.

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

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Unternehmen, das die die Horizon View Client-Anwendung entwickelte	No (Nein)	VMware
Produktname	No (Nein)	VMware Horizon View Client
Client-Produktversion	No (Nein)	Das Format lautet <i>x.x.x-yyyyyy</i> , wobei <i>x.x.x</i> für die Client-Versionsnummer und <i>yyyyyy</i> für die Build-Nummer steht.
Client-Binärarchitektur	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> <li>■ i386</li> <li>■ x86_64</li> <li>■ arm</li> </ul>

**Tabelle 1-1.** Von den Horizon View Client-Instanzen gesammelte Daten für das Programm zur Verbesserung der Benutzerfreundlichkeit (Fortsetzung)

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Client-Build-Name	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> <li>■ VMware-Horizon-View-Client-Win32-Windows</li> <li>■ VMware-Horizon-View-Client-Linux</li> <li>■ VMware-Horizon-View-Client-iOS</li> <li>■ VMware-Horizon-View-Client-Mac</li> <li>■ VMware-Horizon-View-Client-Android</li> <li>■ VMware-Horizon-View-Client-WinStore</li> </ul>
Host-Betriebssystem	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> <li>■ Windows 8.1</li> <li>■ Windows 7, Service Pack 1 für 64 Bit (Build 7601)</li> <li>■ iPhone OS 5.1.1 (9B206)</li> <li>■ Ubuntu 10.04.4 LTS</li> <li>■ Mac OS X 10.7.5 (11G63)</li> </ul>
Host-Betriebssystemkernel	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> <li>■ Windows 6.1.7601 SP1</li> <li>■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X</li> <li>■ Darwin 11.4.2</li> <li>■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012</li> <li>■ unbekannt (für Windows Store)</li> </ul>
Host-Betriebssystemarchitektur	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> <li>■ x86_64</li> <li>■ i386</li> <li>■ armv7l</li> <li>■ ARM</li> </ul>
Hostsystem-Modell	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> <li>■ Dell Inc. OptiPlex 960</li> <li>■ iPad3,3</li> <li>■ MacBookPro8,2</li> <li>■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)</li> </ul>
Hostsystem-CPU	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> <li>■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH</li> <li>■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH</li> <li>■ unbekannt (für iPad)</li> </ul>
Anzahl der Cores bzw. Kerne im Prozessor des Hostsystems	No (Nein)	Beispiel: 4
MB Arbeitsspeicher auf dem Hostsystem	No (Nein)	Beispiele hierfür sind: <ul style="list-style-type: none"> <li>■ 4096</li> <li>■ unbekannt (für Windows Store)</li> </ul>

# Verwenden von URIs zur Konfiguration von Horizon View Client

---

# 2

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 Horizon View Client, zur Verbindung mit dem View-Verbindungsserver oder zum Start eines bestimmten Desktops mit bestimmten Konfigurationsoptionen klicken.

Sie können die Anmeldung am Remote-Desktop 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-Verbindungsservers
- Portnummer für den View-Verbindungsserver
- Active Directory-Benutzername
- Domänenname
- Desktopanzeigename
- Fenstergröße
- Desktop-Aktionen, darunter „Zurücksetzen“, „Abmelden“ und „Sitzung starten“
- Anzeigeprotokoll
- Optionen zur Umleitung von USB-Geräten

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

---

**HINWEIS** Sie können URIs nur zum Start von Horizon View Client verwenden, wenn die Clientsoftware bereits auf den Clientcomputern der Endbenutzer installiert ist.

---

Dieses Kapitel behandelt die folgenden Themen:

- [„Syntax für die Erstellung von vmware-view-URIs“](#), auf Seite 16
- [„Beispiele für vmware-view-URIs“](#), auf Seite 18

## Syntax für die Erstellung von vmware-view-URIs

Die Syntax umfasst das URI-Schema `vmware-view`, einen Pfadauszug zur Angabe des Desktops sowie optional eine Abfrage zur Angabe der Desktopaktionen oder Konfigurationsoptionen.

### Spezifikationen für VMware Horizon View-URIs

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

```
vmware-view://[<varname id="VARNAME_E0F8F9951BC4471D9871655A18782C9E">authority-part</varname>]
[/<varname id="VARNAME_7B21DCA6CDE942BBB914ADD20452590B">path-part</varname>][?<varname id="VAR-
NAME_217F9AF17A3745369FD8E2154505D735">query-part</varname>]
```

Das einzig erforderliche Element ist das URI-Schema `vmware-view`. Für einige Versionen bestimmter Clientbetriebsysteme muss für den Namen des Schemas die Groß- und Kleinschreibung beachtet werden. Verwenden Sie daher `vmware-view`.

---

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

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

---

#### **authority-part**

Gibt die Serveradresse und optional einen Benutzernamen, eine nicht standardmäßige Portnummer oder beides an. Die Servernamen müssen der DNS-Syntax entsprechen.

Verwenden Sie zur Angabe eines Benutzernamens die folgende Syntax:

```
user1@<varname id="VARNAME_640D14F5E64B44E189F204DC09A8248B">server-
address</varname>
```

Beachten Sie dabei, dass Sie keine UPN-Adresse angeben können. Hierzu zählt auch die Domäne. Zur Angabe des Domänennamens können Sie den Abfrageteil `domainName` im URI verwenden.

Verwenden Sie zur Angabe einer Portnummer die folgende Syntax:

```
<varname id="VARNAME_1BAB6153D2834B1490509093A1961D1F">server-add-
ress</varname>:<varname id="VARNA-
ME_2296A4E54893485C852FFE94067114D7">port-number</varname>
```

#### **path-part**

Gibt den Desktop an. Verwenden Sie den Anzeigenamen des Desktops. Weist der Anzeigename ein Leerzeichen auf, müssen Sie den Codierungsmechanismus `%20` verwenden, um das Leerzeichen darzustellen.

#### **query-part**

Gibt die zu verwendenden Konfigurationsoptionen oder die durchzuführenden Desktopaktionen 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:

```
<varname id="VARNAME_48A6B3A0E1184943BC1206017B78B9D5">query1</varna-
me>=<varname id="VARNAME_9B9916FF3D3540D4AA5622F9C828F072">va-
lue1</varname>[&<varname id="VARNA-
ME_6BCA2912EC454A5683D586754BF89DCE">query2</varname>=<varname
id="VARNAME_F698C39E83D34D639C943ACDF828BAFE">value2</varname>...]
```



## Unterstützte Abfragen

In diesem Abschnitt werden die Abfragen aufgeführt, die für diesen Horizon View Client-Typ unterstützt werden. Wenn Sie URIs für mehrere Clienttypen generieren, so zum Beispiel für Desktopclients oder mobile Clients, finden Sie für jede Art Clientsystem weitere Anweisungen im Handbuch *Verwendung von VMware Horizon View 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 an. Bei Verwendung dieser Aktion müssen Sie keinen Desktop angeben. Wenn Sie die Aktion <code>browse</code> verwenden und einen Desktop angeben, wird der Desktop in der Liste der verfügbaren Desktops hervorgehoben.
start-session	Startet den angegebenen Desktop. Wenn keine „action“-Abfrage bereitgestellt wird und der Desktopname angegeben wird, ist <code>start-session</code> die Standardaktion.
zurücksetzen	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.
logoff	Meldet den Benutzer vom Gastbetriebssystem auf dem Remote-Desktop ab.
rollback	Verwirft die Änderungen, die am angegebenen Desktop vorgenommen wurden, während dieser zur Verwendung im lokalen Modus auf einem Windows-PC oder Laptop ausgecheckt wurde.

### connectUSBOnInsert

(Für Horizon View Client 1.7 und höher) Verbindet ein USB-Gerät mit dem virtuellen Desktop im Vordergrund, wenn Sie das Gerät anschließen. Diese Abfrage wird bedingungslos festgelegt, wenn Sie die Abfrage `unattended` angeben. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf `start-session` setzen oder ohne die Abfrage `action` arbeiten. Gültige Werte sind `true` und `false`. Ein Beispiel für die Syntax ist etwa `connectUSBOnInsert=true`.

### connectUSBOnStartup

(Für Horizon View Client 1.7 und höher) Leitet alle aktuell mit dem Client-system verbundenen USB-Geräte an den Desktop um. Diese Abfrage wird bedingungslos festgelegt, wenn Sie die Abfrage `unattended` angeben. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf `start-session` setzen oder ohne die Abfrage `action` arbeiten. Gültige Werte sind `true` und `false`. Ein Beispiel für die Syntax ist etwa `connectUSBOnStartup=true`.

### desktopLayout

Legt die Größe des Fensters für die Anzeige des Remote-Desktops fest. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf `start-session` setzen oder ohne die Abfrage `action` arbeiten.

**Tabelle 2-2.** Gültige Werte für `desktopLayout`-Abfrage

Wert	Beschreibung
fullscreen	Vollbild auf allen angeschlossenen externen Monitoren. Hierbei handelt es sich um die Standardeinstellung.
windowLarge	Großes Fenster.

**Tabelle 2-2.** Gültige Werte für desktopLayout-Abfrage (Fortsetzung)

Wert	Beschreibung
windowSmall	Kleines Fenster.
WxH	Benutzerdefinierte Auflösung, bei der Sie die Breite mal Höhe in Pixel angeben. Ein Beispiel für die Syntax ist etwa <b>desktopLayout=1280x800</b> .

<b>desktopProtocol</b>	Gültige Werte sind <b>RDP</b> und <b>PCoIP</b> . Zur Angabe von PCoIP verwenden Sie beispielsweise die Syntax <b>desktopProtocol=PCoIP</b> .
<b>domainName</b>	Die Domäne, die mit dem Benutzer verknüpft ist, der eine Verbindung zum Remote-Desktop herstellt.

## Beispiele für vmware-view-URIs

Sie können Hypertext-Links oder Schaltflächen mit dem URI-Schema `vmware-view` 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 mit den von Ihnen angegebenen Startoptionen zu starten.

### URI-Syntaxbeispiele

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

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

Horizon View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigename als **Primary Desktop** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet.

---

**HINWEIS** Die Standardvorgaben für das Anzeigeprotokoll und die Fenstergröße werden verwendet. Das Standardanzeigeprotokoll ist PCoIP. Die Standardfenstergröße ist Vollbild.

---

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

Dieser URI hat die gleiche Wirkung wie im vorherigen Beispiel, außer dass er den nicht standardmäßigen Port 7555 für den View-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.

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

Horizon View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Im Anmeldefeld wird das Textfeld **Benutzername** mit dem Namen `fred` gefüllt. Der Benutzer muss den Domänennamen und das Kennwort eingeben. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigename als **Finance Desktop** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet. Die Verbindung nutzt das PCoIP-Anzeigeprotokoll.

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

Horizon View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Im Anmeldefeld wird das Textfeld **Benutzername** mit dem Namen **fred** und das Textfeld **Domäne** mit **mycompany** gefüllt. Der Benutzer muss das Kennwort eingeben. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigenamen als **Finance Desktop** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet.

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

Horizon View Client wird gestartet und der Benutzer wird an die Anmeldeaufforderung für die Verbindung mit dem Server `view.mycompany.com` weitergeleitet.

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

Horizon View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domännennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung zeigt Horizon View Client ein Dialogfeld an, in dem der Benutzer aufgefordert wird, das Zurücksetzen für „Primary Desktop“ zu bestätigen. Nach dem Zurücksetzen wird je nach Clienttyp eine Meldung angezeigt, die über den Erfolg des Zurücksetzens informiert.

---

**HINWEIS** Diese Aktion ist nur verfügbar, wenn die Funktion vom View-Administrator für den Endbenutzer aktiviert wurde.

---

7 `vmware-view://`

Horizon View Client wird gestartet und der Benutzer wird zu der Seite weitergeleitet, auf der die Adresse einer View-Verbindungsserver-Instanz eingegeben werden kann.

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

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

</body>
</html>
```



# Verwaltung der Serververbindungen und Desktops

---

# 3

Mit Horizon View Client können Sie eine Verbindung zu einem View-Verbindungsserver oder Sicherheitsserver herstellen und sich bei einem Remote-Desktop an- oder abmelden. Zur Fehlersuche können Sie auch einen Ihnen zugewiesenen Remote-Desktop zurücksetzen.

Je nachdem, wie der Administrator die Richtlinien für Remote-Desktops festlegt, können die Endbenutzer viele verschiedene Vorgänge auf ihren Desktops durchführen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Erstmaliges Anmelden an einem Remote-Desktop“](#), auf Seite 21
- [„Zertifikatsprüfungsmodi für Horizon View Client“](#), auf Seite 23
- [„Suchen nach Desktops“](#), auf Seite 24
- [„Wechseln zwischen Desktops“](#), auf Seite 25
- [„Abmelden oder Trennen von Desktops“](#), auf Seite 25
- [„Entfernen einer View Server-Verknüpfung von der Startseite“](#), auf Seite 26
- [„Neuanordnen von View Server- und Remote-Desktop-Verknüpfungen“](#), auf Seite 27
- [„Rollback eines Desktops“](#), auf Seite 27

## Erstmaliges Anmelden an einem Remote-Desktop

Bevor Endbenutzer auf ihre Remote-Desktops zugreifen, sollten Sie testen, ob Sie sich über ein Clientsystem an einem Remote-Desktop anmelden können.

### Voraussetzungen

- Besorgen Sie sich die zur Anmeldung benötigten Informationen, so etwa den Active Directory-Benutzernamen und das Active Directory-Kennwort, den RSA SecurID-Benutzernamen und -Passcode oder den RADIUS-Authentifizierungsbenutzernamen oder -Passcode.
- Besorgen Sie sich den Domänennamen für die Anmeldung.
- Führen Sie die unter [„Vorbereiten des View-Verbindungservers für Horizon View Client“](#), auf Seite 9 beschriebenen administrativen Aufgaben aus.
- Wenn Sie sich außerhalb des Firmennetzwerks befinden und für den Zugriff auf den Remote-Desktop keinen Sicherheitsserver verwenden, stellen Sie sicher, dass Ihr Clientgerät für die Verwendung einer VPN-Verbindung konfiguriert ist, und aktivieren Sie diese Verbindung.

---

**WICHTIG** VMware empfiehlt die Verwendung eines Sicherheitsservers anstelle eines VPNs.

---

- Stellen Sie sicher, dass Sie über den vollqualifizierten Domänennamen (FQDN) des Servers verfügen, der Zugriff auf diesen Remote-Desktop gewährt. Sie benötigen zudem auch die Portnummer, wenn es sich beim Port nicht um 443 handelt.
- Wenn Sie beabsichtigen, das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem Remote-Desktop zu verwenden, müssen Sie sicherstellen, dass die View Agent-Gruppenrichtlinieneinstellung AllowDirectRDP aktiviert ist.
- Wenn Ihr Administrator dies zulässt, können Sie den Zertifikatsprüfungsmodus für das von View Server vorgelegte SSL-Zertifikat konfigurieren. Siehe „Zertifikatsprüfungsmodi für Horizon View Client“, auf Seite 23.
- Vergewissern Sie sich, sofern die Endbenutzer zur Verwendung des Microsoft RDP-Anzeigeprotokolls berechtigt sind, dass das Clientsystem über den Microsoft Remotedesktopverbindungs-Client für Mac, Version 2.0 oder höher, verfügt. Dieser Client steht auf der Microsoft-Website zum Download zur Verfügung.

### Vorgehensweise

- 1 Doppelklicken Sie im **Anwendungen**-Ordner auf **VMware Horizon View Client**.
- 2 Klicken Sie auf **Weiter**, um die USB- und Druckdienste für Remote-Desktops zu starten, oder klicken Sie auf **Abbrechen**, um Horizon View Client ohne USB- und Druckdienste für Remote-Desktops zu verwenden.

Wenn Sie auf **Weiter** klicken, müssen Sie Informationen zur Systemanmeldung eingeben. Wenn Sie auf **Abbrechen** klicken, können Sie die USB- und Druckdienste für Remote-Desktops später aktivieren.

---

**HINWEIS** Die Aufforderung zum Starten der USB- und Druckdienste für Remote-Desktops wird beim ersten Start von Horizon View Client angezeigt. Sie erscheint nicht erneut, unabhängig davon, ob Sie auf **Abbrechen** oder **Weiter** klicken.

---

- 3 Klicken Sie auf das Symbol **Server hinzufügen** auf der Startseite von Horizon View Client.
- 4 Geben Sie den Servernamen und eine Portnummer ein, falls dies erforderlich ist, und klicken Sie dann auf **Weiter**.  
Ein Beispiel für die Verwendung eines nicht standardmäßigen Ports ist **view.company.com:1443**.
- 5 Wenn Sie zur Eingabe von RSA SecurID- oder RADIUS-Authentifizierungs-Anmeldeinformationen aufgefordert werden, geben Sie den Benutzernamen und den Passcode ein und klicken Sie auf **Weiter**.
- 6 Geben Sie Ihren Benutzernamen und das Kennwort ein, wählen Sie eine Domäne aus und klicken Sie auf **Weiter**.

Es wird eventuell eine Meldung eingeblendet, die Sie bestätigen müssen, bevor das Anmeldedialogfenster erscheint.

- 7 Wenn die Sicherheitsanzeige des Desktops rot angezeigt und eine Warnung ausgegeben wird, reagieren Sie auf die Eingabeaufforderung.

Normalerweise bedeutet diese Warnung, dass der View-Verbindungsserver keinen Zertifikat-Fingerabdruck an den Client gesendet hat. Ein Fingerabdruck ist ein Hash-Wert des öffentlichen Schlüssels des Zertifikats und wird als Abkürzung für den öffentlichen Schlüssel verwendet. View-Verbindungsserver der Version 4.6.1, 5.0.1 und höher senden Fingerabdruck-Informationen, frühere Versionen jedoch nicht.

- 8 (Optional) Wählen Sie das Protokoll aus.

Die Standardeinstellung ist **PCoIP**. Wenn Sie stattdessen das Microsoft RDP-Anzeigeprotokoll verwenden möchten, müssen Sie zum Umschalten auf **PCoIP** unter dem Desktop-Namen klicken und **RDP** auswählen.

- 9 Doppelklicken Sie auf eine Remote-Desktop-Verknüpfung, um die Verbindung herzustellen.

Nachdem die Verbindung hergestellt wurde, wird das Clientfenster angezeigt. Wenn Horizon View Client keine Verbindung mit dem Desktop herstellen kann, führen Sie die folgenden Aufgaben aus:

- Legen Sie fest, ob der View-Verbindungsserver dahingehend konfiguriert werden soll, SSL nicht zu verwenden. Horizon View Client erfordert SSL-Verbindungen. Prüfen Sie, ob die globale Einstellung in View Administrator für das Kontrollkästchen **SSL für Client-Verbindungen verwenden** deaktiviert ist. Ist dies der Fall, müssen Sie entweder das Kontrollkästchen markieren, sodass SSL verwendet wird, oder Ihre Umgebung so einrichten, dass die Clients eine Verbindung zu einem HTTPS-fähigen Lastenausgleich oder einem anderen Zwischengerät herstellen können, das zur Herstellung einer HTTP-Verbindung zum View-Verbindungsserver konfiguriert ist.
- Stellen Sie eine ordnungsgemäße Funktionsweise des Sicherheitszertifikats für View-Verbindungsserver sicher. Wenn dies nicht zutrifft, wird in View Administrator möglicherweise angezeigt, dass View Agent in Desktops nicht erreichbar ist.
- Stellen Sie sicher, dass die für die View-Verbindungsserver-Instanz festgelegten Kennzeichen Verbindungen von diesem Benutzer erlauben. Weitere Informationen finden Sie im Dokument *Verwaltung von VMware Horizon View*.
- Stellen Sie sicher, dass der Benutzer zum Zugriff auf diesen Desktop berechtigt ist. Weitere Informationen finden Sie im Dokument *Verwaltung von VMware Horizon View*.
- Wenn Sie das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem Remote-Desktop verwenden, müssen Sie bestätigen, dass der Clientcomputer Remote-Desktop-Verbindungen zulässt.

## Zertifikatsprüfungsmodi für Horizon View Client

Administratoren und manchmal auch Endbenutzer können über eine Konfiguration festlegen, ob Client-Verbindungen abgelehnt werden sollen, wenn bei Zertifikatsüberprüfungen Fehler auftreten.

Die Zertifikatsprüfung wird für SSL-Verbindungen zwischen View-Verbindungsserver und Horizon View Client durchgeführt. Die Zertifikatsüberprüfung umfasst die folgenden Checks:

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

Um diese Prüfung zu bestehen, muss sich das Stammzertifikat für die Zertifikatvertrauenskette im lokalen Zertifikatspeicher des Geräts befinden.

---

**HINWEIS** Anweisungen zur Verteilung eines selbstsignierten Stammzertifikats und Installation desselben auf Mac OS X-Clientsystemen finden Sie auf der Apple-Website im Dokument *Erweiterte Serververwaltung* des von Ihnen verwendeten Mac OS X-Servers.

---

Neben der Bereitstellung eines Serverzertifikats sendet der View-Verbindungsserver der Version 4.6.1, 5.0.1 und höher ebenfalls einen Zertifikat-Fingerabdruck an Horizon View Client. Ein Fingerabdruck ist ein Hash-Wert des öffentlichen Schlüssels des Zertifikats und wird als Abkürzung für den öffentlichen Schlüssel verwendet. Wenn View Server keinen Fingerabdruck sendet, wird eine Warnung ausgegeben, dass es sich um eine nicht vertrauenswürdige Verbindung handelt.

Wenn Ihr Administrator dies zulässt, können Sie den Zertifikatsprüfungsmodus festlegen. Wählen Sie **VMware Horizon View Client > Einstellungen** in der Menüleiste. Sie haben drei Auswahlmöglichkeiten:

- **Nie mit nicht vertrauenswürdigen Servern verbinden.** Sollte eine beliebige der Zertifikatsprüfungen fehlschlagen, kann der Client keine Verbindung mit dem Server herstellen. Die nicht bestandenen Prüfungen werden in einer Fehlermeldung aufgelistet.
- **Warnung vor Verbindung mit nicht vertrauenswürdigen Servern ausgeben.** Wenn eine Zertifikatsprüfung fehlschlägt, weil der Server ein selbstsigniertes Zertifikat verwendet, können Sie auf **Weiter** klicken, um die Warnung zu ignorieren. Bei selbstsignierten Zertifikaten muss der Zertifikatsname nicht mit dem Namen des View-Verbindungsservers übereinstimmen, den Sie in Horizon View Client eingegeben haben.
- **Server-Identitätszertifikate nicht überprüfen.** Bei Aktivierung dieser Option führt View keine Zertifikatsüberprüfung durch.

Ist der Zertifikatsprüfungsmodus auf **Warnen** gesetzt, können Sie immer noch eine Verbindung mit einer View-Verbindungsserverinstanz herstellen, die ein selbstsigniertes Zertifikat verwendet.

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

## Suchen nach Desktops

Nachdem Sie eine Verbindung zu einem View Server hergestellt haben, werden die auf diesem Server verfügbaren Desktops im Fenster zur Desktop-Auswahl angezeigt. In Horizon View Client 2.3 und höher können Sie nach einem bestimmten Desktop suchen, indem Sie eine Eingabe im Fenster zur Desktop-Auswahl vornehmen.

Wenn Sie mit der Eingabe beginnen, hebt Horizon View Client den ersten übereinstimmenden Desktop-Namen hervor. Drücken Sie die Eingabetaste, um eine Verbindung zu einem hervorgehobenen Desktop herzustellen. Wenn Sie die Eingabe fortsetzen, nachdem die erste Übereinstimmung gefunden wurde, sucht Horizon View Client weiterhin nach übereinstimmenden Desktops. Für den Fall, dass Horizon View Client mehrere übereinstimmende Desktops findet, können Sie durch Drücken der Tabulatortaste zum nächsten übereinstimmenden Desktop wechseln. Falls Sie zwei Sekunden lang keine Eingabe vornehmen und dann erneut Text eingeben, geht Horizon View Client davon aus, dass Sie eine neue Suche starten.



## Wechseln zwischen Desktops

Wenn Sie mit einem Desktop verbunden sind, können Sie zu einem anderen Desktop wechseln.

### Vorgehensweise

- ◆ Wählen Sie einen Remote-Desktop auf demselben oder einem anderen Server aus.

Option	Aktion
<b>Einen anderen Remote-Desktop auf demselben Server auswählen</b>	Für Horizon View Client 2.1 und höhere Versionen doppelklicken Sie im Fenster zur Desktop-Auswahl auf das Symbol, das einen anderen Desktop-Pool repräsentiert. Sie können in der Symbolleiste auch auf die Schaltfläche <b>Trennen</b> klicken oder aus der Menüleiste <b>Desktop &gt; Trennen</b> auswählen.  Für Horizon View Client 2.0 und Vorgängerversionen klicken Sie auf die Schaltfläche <b>Trennen</b> in der Symbolleiste oder wählen Sie aus der Menüleiste <b>Desktop &gt; Trennen</b> aus.
<b>Einen anderen Remote-Desktop auf einem anderen Server auswählen</b>	Wenn Sie Horizon View Client 2.1 und höher verwenden, zur Verwendung mehrerer Desktops berechtigt sind und das Fenster zur Desktop-Auswahl geöffnet ist, klicken Sie auf die Schaltfläche <b>Verbindung zu Server trennen</b> auf der rechten Seite der Symbolleiste im Fenster zur Desktop-Auswahl, und trennen Sie die Verbindung mit dem Server. Wenn Sie nur zur Verwendung eines Desktops berechtigt sind, ist das Fenster zur Desktop-Auswahl nicht geöffnet. Sie können in der Menüleiste auf <b>Desktop &gt; Trennen</b> klicken und dann Horizon View Client erneut starten, um eine Verbindung zu einem anderen Server herzustellen.  Für Horizon View Client 2.0 und Vorgängerversionen klicken Sie auf die Schaltfläche <b>Verbindung zu Server trennen</b> auf der rechten Seite der Symbolleiste im Horizon View Client-Fenster.

## Abmelden oder Trennen von Desktops

Wenn Sie die Verbindung zu einem Remote-Desktop trennen, ohne sich abzumelden, bleiben die Anwendungen geöffnet.

Selbst wenn Sie keinen Remote-Desktop geöffnet haben, können Sie sich vom Remote-Desktop-Betriebssystem abmelden. Die Verwendung dieser Option hat dieselbe Funktion, wie wenn Sie die Tastenkombination Strg+Alt+Delete drücken und anschließend auf **Abmelden** klicken.

**HINWEIS** Die Eingabe der Windows-Tastenkombination Strg+Alt+Entf wird für Remote-Desktops nicht unterstützt. Wählen Sie, um dieselben Resultate wie bei einer Betätigung von Strg+Alt+Entf zu erzielen, die Optionen **Desktop > Strg+Alt+Entf senden** aus der Menüleiste.

Alternativ können Sie auch die Tastenkombination Fn+Steuerung+Option+Entfernen auf einer Apple-Tastatur betätigen.

## Vorgehensweise

- Trennen Sie die Verbindung, ohne sich abzumelden.

Option	Aktion
<b>Verbindung zum Desktop trennen und Horizon View Client beenden</b>	Klicken Sie auf die Schaltfläche <b>Schließen</b> in der Ecke des Fensters oder wählen Sie <b>Datei &gt; Schließen</b> aus der Menüleiste aus.
<b>Verbindung zum Desktop trennen und in Horizon View Client verbleiben</b>	Klicken Sie auf die Schaltfläche <b>Trennen</b> in der Symbolleiste oder wählen Sie <b>Trennen &gt; Desktop</b> aus der Menüleiste aus.

**HINWEIS** Der View-Administrator kann Ihren Desktop so konfigurieren, dass Sie beim Trennen der Verbindung automatisch abgemeldet werden. In diesem Fall werden alle geöffneten Programme auf Ihrem Desktop angehalten.

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

Option	Aktion
<b>Aus dem Desktop-Betriebssystem heraus</b>	Melden Sie sich über das Windows- <b>Start</b> -Menü ab.
<b>Über die Menüleiste</b>	Wählen Sie <b>Desktop &gt; Abmelden</b> aus der Menüleiste aus. Bei Verwendung dieser Option werden alle Dateien, die auf dem Remote-Desktop geöffnet sind, ohne vorheriges Speichern geschlossen.

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

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

Option	Aktion
<b>Vom Startbildschirm aus (mit Server-Verknüpfungen)</b>	<p>a Doppelklicken Sie auf die Server-Verknüpfung und geben Sie die Anmeldeinformationen an.</p> <p>Dazu zählen möglicherweise die RSA SecurID-Anmeldeinformationen und die Anmeldeinformationen zur Anmeldung am Desktop.</p> <p>b Wählen Sie zuerst den Desktop und anschließend <b>Desktop &gt; Abmelden</b> aus der Menüleiste aus.</p>
<b>Vom Startbildschirm aus (mit Desktop-Verknüpfungen)</b>	Wählen Sie zuerst den Desktop und anschließend <b>Desktop &gt; Abmelden</b> aus der Menüleiste aus.

## Entfernen einer View Server-Verknüpfung von der Startseite

Nach der Verbindungsherstellung mit einer View Server-Instanz wird eine Server-Verknüpfung auf der Horizon View Client-Startseite gespeichert.

Sie können die View-Verbindungsserver-Verknüpfung durch Auswahl der Verknüpfung und Betätigen der Löschtaste oder durch einen Steuerklick/Rechtsklick auf die Verknüpfung auf der Startseite und Auswahl von **Löschen** entfernen.

Sie können die Remote-Desktop-Verknüpfungen nicht entfernen, die nach der Verbindungsherstellung mit einem Server angezeigt werden.

## Neuanordnen von View Server- und Remote-Desktop-Verknüpfungen

In Horizon View Client 2.3 und höher können Sie View Server- und Remote-Desktop-Verknüpfungen neu anordnen.

Bei jeder Verbindungsherstellung mit einer View Server-Instanz speichert Horizon View Client eine Server-Verknüpfung auf der Startseite. Diese View Server-Verknüpfungen können Sie neu anordnen, indem Sie eine Verknüpfung auswählen und an eine neue Position auf der Startseite ziehen.

Nachdem Sie eine Verbindung zu einem View Server hergestellt haben, werden die auf diesem Server verfügbaren Desktops im Fenster zur Desktop-Auswahl angezeigt. Diese Remote-Desktop-Verknüpfungen können Sie neu anordnen, indem Sie eine Verknüpfung auswählen und an eine neue Position im Fenster zur Desktop-Auswahl ziehen.

## Rollback eines Desktops

Bei einem Rollback werden alle an einem virtuellen Desktop vorgenommenen Änderungen verworfen, den Sie zur Verwendung im lokalen Modus auf einem Windows-PC oder -Laptop ausgecheckt haben.

Sie können ein Rollback eines Remote-Desktops nur dann durchführen, wenn Ihr View-Administrator diese Funktion aktiviert hat und auch nur dann, wenn Sie den Desktop ausgecheckt haben.



**VORSICHT** Wenn Änderungen am Desktop im lokalen Modus vorgenommen wurden und diese Änderungen nicht vor dem Rollback zurück auf den View Server repliziert wurden, gehen sie verloren.

### Voraussetzungen

- Besorgen Sie sich die zur Anmeldung benötigten Informationen, so etwa den Active Directory-Benutzernamen und das Active Directory-Kennwort, den RSA SecurID-Benutzernamen und -Passcode oder den RADIUS-Authentifizierungsbenutzernamen oder -Passcode.
- Sichern Sie den Desktop auf dem Server, um Daten oder Dateien zu speichern.

Sie können View Administrator zum Replizieren von Daten auf dem Server verwenden, oder, falls die Richtlinie dies zulässt, View Client with Local Mode auf dem Windows-Client verwenden, auf dem der Desktop aktuell ausgecheckt ist.

### Vorgehensweise

- 1 Wenn auf der Startseite von Horizon View Client View-Verbindungsserver-Verknüpfungen angezeigt werden, doppelklicken Sie auf die Verknüpfung für den Server mit Zugriff auf den Desktop und geben Sie die Anmeldeinformationen ein.
  - a Wenn Sie zur Eingabe von RSA SecurID- oder RADIUS-Authentifizierungs-Anmeldeinformationen aufgefordert werden, geben Sie den Benutzernamen und den Passcode ein und klicken Sie auf **Weiter**.
  - b Geben Sie im Anmeldedialogfeld Ihren Benutzernamen und Ihr Kennwort ein.
- 2 Wählen Sie auf der Horizon View Client-Startseite, auf der Remote-Desktop-Verknüpfungen angezeigt werden, den entsprechenden Desktop aus und wählen Sie anschließend **Desktop > Rollback** aus der Menüleiste.

Nach der Durchführung des Rollbacks auf dem Remote-Desktop können Sie sich über den Mac-Client am Remote-Desktop anmelden.



# Verwenden eines Microsoft Windows-Desktops auf einem Mac

# 4

Horizon View Client für Mac OS X unterstützt mehrere Funktionen.

Dieses Kapitel behandelt die folgenden Themen:

- „[Funktionsunterstützungs-Matrix](#)“, auf Seite 29
- „[Internationalisierung](#)“, auf Seite 30
- „[Monitore und Bildschirmauflösung](#)“, auf Seite 30
- „[Verbinden von USB-Geräten](#)“, auf Seite 31
- „[Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone](#)“, auf Seite 39
- „[Kopieren und Einfügen von Text und Bildern](#)“, auf Seite 43
- „[Drucken von einem Remote-Desktop aus](#)“, auf Seite 44
- „[PCoIP-Client-Bildcache](#)“, auf Seite 46

## Funktionsunterstützungs-Matrix

Einige Funktionen werden auf manchen Horizon View Client-Typen unterstützt, auf anderen nicht. Zum Beispiel wird der lokale Modus nur auf Horizon View Client für Windows unterstützt.

**Tabelle 4-1.** Auf Windows-Desktops für Mac OS X-Clients unterstützte Funktionen

Funktion	Windows 8.x-Desktop	Windows 7-Desktop	Windows Vista-Desktop	Windows XP-Desktop	Windows Server 2008 R2-Desktop
RSA SecurID oder RADIUS	X	X	X	X	X
Einmaliges Anmelden	X	X	X	X	X
PCoIP-Anzeigeprotokoll	X	X	X	X	X
RDP-Anzeigeprotokoll	X	X	X	X	X
USB-Zugriff	X	X	X	X	X
Echtzeit-Audio/Video (RTAV)	X	X	X	X	X
Wyse MMR					
Windows 7 MMR					
Virtuelles Drucken	X	X	X	X	
Standortbasiertes Drucken	X	X	X	X	
Smartcards					

**Tabelle 4-1.** Auf Windows-Desktops für Mac OS X-Clients unterstützte Funktionen (Fortsetzung)

Funktion	Windows 8.x-Desktop	Windows 7-Desktop	Windows Vista-Desktop	Windows XP-Desktop	Windows Server 2008 R2-Desktop
Mehrere Monitore	X	X	X	X	X
Lokaler Modus					

Für Funktionen, die auf Windows-Desktops für Mac OS X Horizon View Client unterstützt werden, gelten die folgenden Einschränkungen.

- Windows 8.x-Desktops werden nur unterstützt, wenn Sie über Server und Desktops mit Horizon View 5.2 oder höher verfügen.
- Windows 2008 R2-Desktops werden nur unterstützt, wenn Sie über Server und Desktops mit Horizon View 5.3 oder später verfügen.
- Informationen zum Herstellen einer RDP-Verbindung mit einem Windows 8.1-Desktop finden Sie im VMware KB-Artikel unter <http://kb.vmware.com/kb/2059786>.
- Die Echtzeit-Audio/Video-Funktion wird nur unterstützt, wenn Sie über Horizon View 5.2 mit Feature Pack 2 oder höher verfügen. Eine vollständige Aufstellung der Anforderungen finden Sie unter „Systemanforderungen für Echtzeit-Audio/Video“, auf Seite 8.

Weitere Erläuterungen zu diesen Funktionen und deren Einschränkungen finden Sie im Dokument *Planung von VMware Horizon View*.

## Internationalisierung

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

## Monitore und Bildschirmauflösung

Wenn Sie Horizon View Client 2.0 und höhere Versionen zusammen mit dem PCoIP-Anzeigeprotokoll verwenden, können Sie einen Remote-Desktop auf mehrere Monitore erweitern. Wenn Sie einen Mac mit Retina-Display besitzen, können Sie den Remote-Desktop in voller Auflösung sehen.

### Verwendung mehrerer Monitore

Wenn Sie beim Zugriff auf einen Remote-Desktop das PCoIP-Anzeigeprotokoll verwenden, können Sie maximal zwei Monitore mit einer Auflösung von bis zu 2560x1600 pro Display nutzen. Wenn Sie mit zwei Monitoren arbeiten, können die Monitore nebeneinander oder übereinander aufgestellt werden.

Haben Sie die 3D-Rendern-Funktion aktiviert, beträgt die maximale Auflösung 1920x1200. Beispiele für 3D-Anwendungen sind Windows Aero-Themen, Microsoft Office 2010 und Google Earth.

Wenn Sie einen Remote-Desktop auf mehrere Monitore erweitern möchten, können Sie das Menüelement **Fenster > Vollbild** oder die Erweiterungspfeile oben rechts im Horizon View Client-Fenster dafür verwenden.

Öffnen Sie unter Mac OS X Mavericks (10.9) die „Systemeinstellungen“, klicken Sie auf „Mission Control“ und deaktivieren Sie **Monitore haben separate Spaces**, um den Vollbildmodus mit mehr als einem Monitor zu verwenden. Zum Anwenden der Änderungen müssen Sie sich abmelden.

## Anzeigen eines Remote-Desktops auf einem hochauflösenden Mac mit Retina-Display

Wenn Sie das PCoIP-Anzeigeprotokoll verwenden, unterstützt Horizon View Client auch sehr hohe Auflösungen für Clientsysteme mit Retina-Display. Nachdem Sie sich bei einem Remote-Desktop angemeldet haben, wählen Sie das Menüelement **Desktop > Auflösung > Volle Auflösung**. Dieses Menüelement wird nur dann angezeigt, wenn das Clientsystem ein Retina-Display unterstützt.

Wenn Sie **Volle Auflösung** verwenden, erscheinen die Symbole auf dem Remote-Desktop kleiner, aber die Anzeige ist schärfer. Wenn Sie das Clientsystem mit einem externen Monitor verbinden, wechselt die Anzeige wieder nach **Normal**.

## Verbinden von USB-Geräten

Sie können lokal angeschlossene USB-Geräte, zum Beispiel Thumb-Flashlaufwerke, Kameras oder Drucker, von einem Remote-Desktop aus verwenden. Diese Funktion wird als USB-Umleitung bezeichnet.

Bei Aktivierung dieser Funktion stehen die meisten USB-Geräte, die an das lokale Clientsystem angeschlossen sind, in einem Menü in Horizon View Client zur Verfügung. Über das Menü können Sie die Geräte verbinden oder deren Verbindung trennen.

Bei der Verwendung von USB-Geräten mit Remote-Desktops gelten folgende Einschränkungen:

- Beim Zugriff auf ein USB-Gerät von einem Menü in Horizon View Client und Verwendung des Geräts in einem Remote-Desktop können Sie nicht auf dem lokalen Computer auf das Gerät zugreifen.
- Zu den USB-Geräten, die nicht im Menü angezeigt werden, aber auf dem Remote-Desktop verfügbar sind, zählen Eingabegeräte (Human Interface Devices) wie zum Beispiel Tastaturen und Zeigergeräte. Der Remote-Desktop und der lokale Computer verwenden diese Geräte gleichzeitig. Die Interaktion mit diesen Geräten kann aufgrund der Netzwerklatenz manchmal recht langsam sein.
- Große USB-Festplattenlaufwerke können erst nach mehreren Minuten auf dem Desktop angezeigt werden.
- Manche USB-Geräte erfordern bestimmte Treiber. Wenn der erforderliche Treiber nicht bereits auf dem Remote-Desktop installiert ist, werden Sie möglicherweise bei Verbindung des USB-Geräts mit dem Remote-Desktop zu Installation dieses Treibers aufgefordert.
- Wenn Sie USB-Geräte verbinden möchten, die MTP-Treiber verwenden, so zum Beispiel Android-basierte Samsung-Smartphones und -Tablets, müssen Sie Horizon View Client so einstellen, dass die USB-Geräte automatisch mit Ihrem Remote-Desktop verbunden werden. Anderenfalls wird das USB-Gerät beim Versuch der manuellen Umleitung über ein Menüelement nur umgeleitet, wenn Sie das Gerät trennen und es anschließend wieder verbinden.
- Webcams werden für die USB-Umleitung nicht unterstützt.
- Die Umleitung von USB-Audiogeräten ist vom Netzwerkstatus abhängig und daher nicht zuverlässig. Manche Geräte erfordern auch im Ruhezustand einen hohen Datendurchsatz.

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

---

**HINWEIS** Leiten Sie keinesfalls USB-Ethernet-Verbindungen an den Remote-Desktop um. Ihr Remote-Desktop kann sich mit dem Netzwerk verbinden, wenn Ihr lokales System verbunden ist. Wenn Sie Ihren Remote-Desktop zur automatischen Verbindung von USB-Geräten konfiguriert haben, können Sie eine Ausnahme hinzufügen, um Ihre Ethernet-Verbindung auszuschließen. Siehe „[Konfigurieren der USB-Umleitung auf einem Mac OS X-Client](#)“, auf Seite 33.

---

## Voraussetzungen

- Um USB-Geräte mit einem Remote-Desktop verwenden zu können, muss der View-Administrator die USB-Funktion für den Remote-Desktop aktiviert haben.

Diese Aufgabe umfasst die Installation der Komponente **USB-Umleitung** in View Agent. Weitere Informationen und Anweisungen finden Sie im Kapitel über die Erstellung und Vorbereitung der virtuellen Maschinen im Dokument *Verwaltung von VMware Horizon View*.

Die Aufgabe kann zudem auch das Festlegen von Gruppenrichtlinien zur Zulassung der USB-Umleitung umfassen. Weitere Informationen finden Sie im Abschnitt „USB-Einstellungen für View Agent“ im Dokument *Verwaltung von VMware Horizon View*.

- Beim erstmaligen Versuch der Verbindung eines USB-Geräts müssen Sie das Administrator-Kennwort eingeben. Horizon View Client fordert Sie zum entsprechenden Zeitpunkt zur Eingabe auf.

Einige der für die USB-Umleitung erforderlichen Komponenten, die bereits durch Horizon View Client installiert wurden, müssen konfiguriert werden. Für die Konfiguration dieser Komponenten sind Administratorberechtigungen erforderlich.

## Vorgehensweise

- Verbinden Sie das USB-Gerät manuell mit einem Remote-Desktop.
  - a Bei erstmaliger Verwendung der USB-Funktion klicken Sie in der VMware Horizon View Client-Menüleiste auf **Desktop > USB > Remote-Desktop-USB-Dienste starten** und geben Sie auf Aufforderung das Administrator-Kennwort an.

Alternativ können Sie auch auf das USB-Gerät-Symbol in der oberen linken Ecke des Horizon View Client-Fensters klicken.

- b Schließen Sie das USB-Gerät an Ihr lokales Clientsystem an.
- c Klicken Sie in der VMware Horizon View Client-Menüleiste auf **Desktop > USB**.
- d Wählen Sie das USB-Gerät aus.

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

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

Verwenden Sie diese Funktion zur automatischen Verbindungsherstellung unbedingt dann, wenn Sie Geräte mit MTP-Treibern verwenden möchten, so zum Beispiel Android-basierte Samsung-Smartphones und -Tablets.

- a Bevor Sie das USB-Gerät anschließen, starten Sie Horizon View Client und stellen Sie die Verbindung mit einem Remote-Desktop her.
- b Bei erstmaliger Verwendung der USB-Funktion klicken Sie in der VMware Horizon View Client-Menüleiste auf **Desktop > USB > Remote-Desktop-USB-Dienste starten** und geben Sie auf Aufforderung das Administrator-Kennwort an.

Alternativ können Sie auch auf das USB-Gerät-Symbol in der oberen linken Ecke des Horizon View Client-Fensters klicken.

- c Klicken Sie in der VMware Horizon View Client-Menüleiste auf **Desktop > USB > USB-Geräte bei Einführen automatisch verbinden**.
- d Schließen Sie das USB-Gerät an.

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



- Konfigurieren Sie Horizon View Client zur automatischen Verbindung von USB-Geräten mit dem Remote-Desktop, wenn Horizon View Client gestartet wird.
  - a Bei erstmaliger Verwendung der USB-Funktion klicken Sie in der VMware Horizon View Client-Menüleiste auf **Desktop > USB > Remote-Desktop-USB-Dienste starten** und geben Sie auf Aufforderung das Administrator-Kennwort an.  
  
Alternativ können Sie auch auf das USB-Gerät-Symbol in der oberen linken Ecke des Horizon View Client-Fensters klicken.
  - b Klicken Sie in der VMware Horizon View Client-Menüleiste auf **Desktop > USB > USB-Geräte bei Start automatisch verbinden**.
  - c Schließen Sie das USB-Gerät an und starten Sie Horizon View Client neu.

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

Das USB-Gerät wird auf dem Desktop angezeigt. Dieser Vorgang kann bis zu 20 Sekunden dauern. Bei erstmaliger Verbindung von Gerät und Desktop werden Sie eventuell dazu aufgefordert, bestimmte Treiber zu installieren.

Wird das USB-Gerät auch nach mehreren Minuten nicht auf dem Desktop angezeigt, sollten Sie die Verbindung trennen und das Gerät anschließend neu mit dem Clientcomputer verbinden.

#### Weiter

Bei Problemen mit der USB-Umleitung finden Sie weitere Informationen im Kapitel über die Behebung von Problemen bei der USB-Umleitung im Dokument *Verwaltung von VMware Horizon View*.

## Konfigurieren der USB-Umleitung auf einem Mac OS X-Client

Mit Horizon View Client 1.7 und höheren Versionen können Administratoren das Clientsystem zur Angabe der USB-Geräte konfigurieren, die an einen Remote-Desktop umgeleitet werden können.

Zum Erreichen der folgenden Ziele können Sie sowohl für View Agent auf dem Remote-Desktop als auch für Horizon View Client auf dem lokalen System einzelne USB-Richtlinien konfigurieren:

- Legen Sie bestimmte Einschränkungen für die USB-Gerättypen fest, die Horizon View Client zur Umleitung bereitstellt.
- Veranlassen Sie, dass View Agent das Weiterleiten bestimmter USB-Geräte von einem Clientcomputer aus verhindert.
- ((Horizon View Client 2.0 und höher) Definieren Sie, ob Horizon View Client USB-Verbundgeräte für die Umleitung in separate Komponenten aufschlüsseln soll oder nicht.

USB-Verbundgeräte bestehen aus einer Kombination von zwei oder mehr Geräten, so zum Beispiel einem Videoeingabegerät und einem Speichergerät.

Die Konfigurationseinstellungen auf dem Client können mit den entsprechenden, für View Agent auf dem Remote-Desktop festgelegten Richtlinien zusammengeführt oder von diesen überschrieben werden. Informationen zur Zusammenarbeit der USB-Einstellungen auf dem Client mit den View Agent-USB-Richtlinien finden Sie in den Abschnitten über die Verwendung von Richtlinien zur Steuerung der USB-Umleitung im Dokument *Verwaltung von VMware Horizon View*.

---

**WICHTIG** Die Funktion zur USB-Umleitung ist nur verfügbar, wenn View Agent und der View-Verbindungsserver über die Horizon View-Version 4.6.1 oder höher verfügen. Die in diesen Hilfetemen beschriebenen USB-Filterfunktionen und die Funktionen zur Geräteaufschlüsselung sind ab dem View-Verbindungsserver 5.1 und höher verfügbar.

---

## Syntax zur Konfiguration der USB-Umleitung

Sie können Filter- und Aufschlüsselungsregeln konfigurieren, um USB-Geräte-Typen von der Umleitung an einen Remote-Desktop auszuschließen oder sie einzuschließen. Konfigurieren Sie auf einem Mac OS X-Client die USB-Funktionalität, indem Sie Terminal (/Applications/Utilities/Terminal.app) verwenden und einen Befehl als „Root“ ausführen.

- Zur Auflistung der Regeln:

```
# sudo defaults read <varname id="VARNAME_95A3DC2017354B8FA8955CED8F69664D">domain</varname>
```

Beispiel:

```
# sudo defaults read com.vmware.viewusb
```

- Zum Entfernen einer Regel:

```
# sudo defaults delete <varname id="VARNAME_E3808110D7D140F3ABFD8180E81A519F">domain property</varname>
```

Beispiel:

```
# sudo defaults delete com.vmware.viewusb ExcludeVidPid
```

- Zum Festlegen oder Ersetzen einer Filterregel:

```
# sudo defaults write <varname id="VARNAME_46C33BABB1243C4AE3F4C9D16FE45C0">domain property value</varname>
```

Beispiel:

```
# sudo defaults write com.vmware.viewusb ExcludeVidPid vid-1234_pid-5678
```

---

**WICHTIG** Manche Konfigurationsparameter erfordern für ein USB-Gerät die VID (Hersteller-ID) und die PID (Produkt-ID). Die korrekte VID und PID finden Sie, indem Sie im Internet nach dem Produkt-namen plus VID und PID suchen. Alternativ können Sie nach Anschluss des USB-Geräts an das lokale System bei Ausführung von Horizon View Client auch in der USB-Protokolldatei nachsehen. Weitere Informationen finden Sie unter „[Aktivieren der Protokollierung für die USB-Umleitung](#)“, auf Seite 38.

---

- So stellen Sie eine Aufschlüsselungsregel für ein Verbundgerät ein bzw. ersetzen sie:

```
# sudo defaults write <varname id="VARNAME_5201E63FDD54D1ABEC023C9FF47AA34">domain property value</varname>
```

Beispiel:

```
# sudo defaults write com.vmware.viewusb AllowAutoDeviceSplitting true
# sudo defaults write com.vmware.viewusb SplitExcludeVidPid vid-03f0_Pid-2a12
# sudo defaults write com.vmware.viewusb SplitVidPid "'vid-0911_Pid-149a(exintf:03)'"
# sudo defaults write com.vmware.viewusb IncludeVidPid vid-0911_Pid-149a
```

USB-Verbundgeräte bestehen aus einer Kombination von zwei oder mehr Geräten, so zum Beispiel einem Videoeingabegerät und einem Speichergerät. Die erste Zeile in diesem Beispiel aktiviert die automatische Aufschlüsselung von Verbundgeräten. Die zweite Zeile schließt das angegebene USB-Verbundgerät (vid-03f0\_Pid-2a12) von der Aufschlüsselung aus.

Die dritte Zeile weist Horizon View Client dazu an, die Komponenten eines anderen Verbundgeräts (vid-0911\_Pid-149a) als separate Geräte zu behandeln, die folgende Komponente jedoch von der Umleitung auszuschließen: Die Komponente, deren Schnittstellenummer 03 lautet. Diese Komponente wird lokal beibehalten.

Da dieses Verbundgerät eine Komponente enthält, die im Regelfall standardmäßig ausgeschlossen wird, z. B. eine Maus oder eine Tastatur, ist die vierte Zeile notwendig, damit andere Komponenten des Verbundgeräts vid-0911\_Pid-149a an den Remote-Desktop umgeleitet werden können.

Die ersten drei Eigenschaften beziehen sich auf die Aufschlüsselung. Die letzte Eigenschaft bezieht sich auf das Filtern. Filtereigenschaften werden vor den Aufschlüsselungseigenschaften verarbeitet.

### Beispiel: Ausschließen eines USB-Ethernet-Geräts

Zu den USB-Geräten, die Sie von der Umleitung ausschließen sollten, zählen beispielsweise auch USB-Ethernet-Geräte. Ihr Mac nutzt möglicherweise ein USB-Ethernet-Gerät für die Verbindung des Netzwerks des Mac-Clientsystems mit einem Remote-Desktop. Wenn Sie das USB-Ethernet-Gerät umleiten, verliert Ihr lokales Clientsystem die Verbindung zum Netzwerk und zum Remote-Desktop.

Wenn Sie dieses Gerät dauerhaft aus dem USB-Verbindungs Menü ausblenden möchten oder Sie Ihren Remote-Desktop so eingerichtet haben, dass USB-Geräte automatisch verbunden werden, können Sie eine Ausnahme hinzufügen, um Ihre Ethernet-Verbindung auszuschließen.

```
sudo defaults write com.vmware.viewusb ExcludeVidPid vid-<varname id="VARNA-
ME_59F5F46045C64F50BC2EAC24D891DD2F">xxxx</varname>_pid-<varname id="VARNA-
ME_5901CF9553E84DC7A32D7C86D3892352">yyyy</varname>
```

In diesem Beispiel steht *xxxx* für die Hersteller-ID und *yyyy* für die Produkt-ID des USB-Ethernet-Adapters.

## Eigenschaften der USB-Umleitung

Bei der Erstellung von Filterregeln können Sie die Eigenschaften der USB-Umleitung verwenden.

**Tabelle 4-2.** Konfigurationseigenschaften für die USB-Umleitung

Name und Eigenschaft der Richtlinie	Beschreibung
Autom. Gerätesplitten zulassen Eigenschaft: AllowAutoDeviceSplitting	((Horizon View Client 2.0 und höher) Automatische Aufschlüsselung von USB-Verbundgeräten zulassen. Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>false</b> ist.
Exclude Vid/Pid Device From Split (Vid/Pid-Gerät vom Splitten ausschließen) Eigenschaft: SplitExcludeVidPid	((Horizon View Client 2.0 und höher) Ein USB-Verbundgerät, das durch die Hersteller- und Produkt-ID gekennzeichnet ist, von der Aufschlüsselung ausschließen. Das Format der Einstellung lautet <code>vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2]...</code> Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: <b>vid-0781_pid-55**</b> Der Standardwert ist nicht definiert.
Split Vid/Pid Device (Vid/Pid-Gerät splitten) Eigenschaft: SplitVidPid	((Horizon View Client 2.0 und höher) Die Komponenten eines USB-Verbundgeräts, das durch die Hersteller- und Produkt-ID gekennzeichnet ist, als separate Geräte behandeln. Das Format der Einstellung ist <code>vid-xxxx_pid-yyy([exintf:zz[;exintf:ww ]])[...]</code> Sie können das Stichwort <code>exintf</code> verwenden, um Komponenten durch Angabe ihrer Schnittstellenummer von der Umleitung auszuschließen. Sie müssen hexadezimale ID-Nummern und dezimale Schnittstellenummern einschließlich der 0 am Anfang angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: <b>vid-0781_pid-554c(exintf:01;exintf:02)</b> <b>HINWEIS</b> Enthält das Verbundgerät Komponenten, die automatisch ausgeschlossen werden, z. B. Maus- und Tastaturkomponenten, dann schließt View die Komponenten, die Sie nicht ausdrücklich ausgeschlossen haben, nicht automatisch ein. Sie müssen eine Filterrichtlinie wie z. B. <code>Include Vid/Pid Device (Vid/Pid-Gerät einschließen)</code> angeben, um diese Komponenten einzuschließen. Der Standardwert ist nicht definiert.
Allow Audio Input Devices (Audioeingabegeräte zulassen) Eigenschaft: AllowAudioIn	Lässt zu, dass Audioeingabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>true</b> ist.

**Tabelle 4-2.** Konfigurationseigenschaften für die USB-Umleitung (Fortsetzung)

Name und Eigenschaft der Richtlinie	Beschreibung
Allow Audio Output Devices (Audioausgabegeräte zulassen) Eigenschaft: AllowAudioOut	Lässt zu, dass Audioausgabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>false</b> ist.
HID zulassen Eigenschaft: AllowHID	Ermöglicht die Umleitung anderer Eingabegeräte neben Tastaturen und Mäusen. Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>true</b> ist.
Allow HIDBootable (HIDBootable zulassen) Eigenschaft: AllowHIDBootable	Ermöglicht die Umleitung anderer Eingabegeräte neben Tastaturen und Mäusen, die zur Startzeit verfügbar sind (auch bezeichnet als „startfähige Eingabegeräte“). Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>true</b> ist.
Ausfallsicherung der Dienstbeschreibung zulassen Eigenschaft: AllowDevDescFailsafe	Ermöglicht die Umleitung der Geräte, auch wenn Horizon View Client die Konfigurations-/Gerätebeschreibungen nicht abrufen kann. Um ein Gerät trotz Fehler in der Konfiguration/Beschreibung zuzulassen, muss dieses in den Filter „Include“ eingeschlossen werden, zum Beispiel in IncludeVidPid oder IncludePath. Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>false</b> ist.
Allow Keyboard and Mouse Devices (Tastatur- und Mausgeräte zulassen) Eigenschaft: AllowKeyboardMouse	Lässt zu, dass Tastaturen mit eingebauten Zeigegegeräten (Maus, Trackball oder Touchpad) umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>false</b> ist.
Allow Smart Cards (SmartCards zulassen) Eigenschaft: AllowSmartcard	Lässt zu, dass SmartCard-Geräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>false</b> ist.
Allow Video Devices (Videogeräte zulassen) Eigenschaft: AllowVideo	Lässt zu, dass Videogeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>true</b> ist.
Disable Remote Configuration Download (Remote-Konfigurations-Download deaktivieren) Eigenschaft: DisableRemoteConfig	Deaktiviert die Verwendung der View Agent-Einstellungen beim Durchführen der USB-Gerätefilterung. Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>false</b> ist.
Exclude All Devices (Alle Geräte ausschließen) Eigenschaft: ExcludeAllDevices	Schließt alle USB-Geräte von der Umleitung aus. Wenn für diese Einstellung <b>true</b> festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zuzulassen, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn für diese Einstellung <b>false</b> festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zu verhindern, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn Sie den Wert von Exclude All Devices in View Agent auf <b>true</b> setzen und diese Einstellung an Horizon View Client weitergegeben wird, überschreibt die View Agent-Einstellung die Horizon View Client-Einstellung. Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>false</b> ist.
Exclude Device Family (Gerätefamilie ausschließen) Eigenschaft: ExcludeFamily	Schließt Gerätefamilien von der Umleitung aus. Das Format der Einstellung ist <i>Familienname_1[;Familienname_2]</i> ... Beispiel: <b>bluetooth;smart-card</b> Der Standardwert ist nicht definiert. <b>HINWEIS</b> ((Horizon View Client 2.0 und höher) Wenn Sie die automatische Geräteaufschlüsselung aktiviert haben, prüft View die Gerätefamilie jeder Schnittstelle eines USB-Verbundgeräts, um zu entscheiden, welche Schnittstellen ausgeschlossen werden sollten. Wenn Sie das automatische Gerätesplitten deaktiviert haben, prüft View die Gerätefamilie des gesamten Composite USB-Gerätes.

**Tabelle 4-2.** Konfigurationseigenschaften für die USB-Umleitung (Fortsetzung)

Name und Eigenschaft der Richtlinie	Beschreibung
Exclude Vid/Pid Device (Vid/Pid-Gerät ausschließen) Eigenschaft: ExcludeVidPid	Schließt Geräte mit einer angegebenen Anbieter- oder Produkt-ID von der Umleitung aus. Das Format der Einstellung lautet <code>vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]</code> ... Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: <b>vid-0781_pid-****;vid-0561_pid-554c</b> Der Standardwert ist nicht definiert.
Exclude Path (Pfad ausschließen) Eigenschaft: ExcludePath	Schließt Geräte an angegebenen Hub- oder Portpfaden von der Umleitung aus. Das Format der Einstellung ist <code>bus-x1[/y1]..._port-z1[;bus-x2[/y2]..._port-z2]</code> ... Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden. Beispiel: <b>bus-1/2/3_port-02;bus-1/1/1/4_port-ff</b> Der Standardwert ist nicht definiert.
Include Device Family (Gerätefamilie einschließen) Eigenschaft: IncludeFamily	Bestimmt Gerätefamilien, die umgeleitet werden können. Das Format der Einstellung ist <code>Familienname_1[;Familienname_2]</code> ... Beispiel: <b>Speicher</b> Der Standardwert ist nicht definiert.
Include Path (Pfad einschließen) Eigenschaft: IncludePath	Schließt Geräte an angegebenen Hub- oder Portpfaden in die Umleitung ein. Das Format der Einstellung lautet <code>bus-x1[/y1]..._port-z1[;bus-x2[/y2]..._port-z2]</code> ... Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden. Beispiel: <b>bus-1/2_port-02;bus-1/7/1/4_port-0f</b> Der Standardwert ist nicht definiert.
Include Vid/Pid Device (Vid/Pid-Gerät einschließen) Eigenschaft: IncludeVidPid	Bestimmt Geräte mit einer angegebenen Anbieter- und Produkt-ID, die umgeleitet werden können. Das Format der Einstellung lautet <code>vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]</code> ... Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: <b>vid-0561_pid-554c</b> Der Standardwert ist nicht definiert.

## USB-Gerätefamilien

Beim Erstellen von USB-Filterregeln für Horizon View Client oder View Agent können Sie eine bestimmte Familie angeben.

**Tabelle 4-3.** USB-Gerätefamilien

Gerätefamilienname	Beschreibung
audio (Audio-wiedergabe)	Ein Audioeingabe- oder Audioausgabegerät beliebigen Typs.
audio-in (Audio-Eingabe)	Audioeingabegeräte, z. B. Mikrofone.
audio-out (Audio-Ausgabe)	Audioausgabegeräte, z. B. Lautsprecher und Kopfhörer.
bluetooth (Bluetooth)	Per Bluetooth verbundene Geräte.
comm	Kommunikationsgeräte wie Modems und kabelgebundene Netzwerkadapter.

**Tabelle 4-3.** USB-Gerätefamilien (Fortsetzung)

Gerätefamilienname	Beschreibung
hid (Eingabegeräte (Human Interface Devices))	Eingabegeräte (Human Interface Devices) außer Tastaturen und Zeigegeräten.
hid-bootable (Eingabegeräte startfähig)	Eingabegeräte (Human Interface Devices), die beim Start verfügbar sind, außer Tastaturen und Zeigegeräte.
imaging (Bildverarbeitung)	Bildverarbeitungsgeräte, z. B. Scanner.
keyboard (Tastatur)	Tastaturgerät.
mouse (Maus)	Zeigegerät, z. B. eine Maus.
Andere	Familie nicht angegeben.
pda (PDA)	PDA (Personal Digital Assistant)
physical (physisch)	Force-Feedback-Geräte, z. B. Force-Feedback-Joysticks.
printer (Drucker)	Druckergeräte.
security (Sicherheit)	Sicherheitsgeräte, z. B. Fingerabdruckleser.
smart-card (Smartcard)	SmartCard-Geräte.
Speicher	Massenspeichergeräte wie z. B. Flash-Laufwerke und externe Festplattenlaufwerke.
unknown (unbekannt)	Familie nicht bekannt.
vendor (Hersteller)	Geräte mit herstellerspezifischen Funktionen.
video (Video)	Videoeingabegeräte.
wireless (drahtlos)	Drahtlose Netzwerkadapter.
wusb	Drahtlose USB-Geräte.

## Aktivieren der Protokollierung für die USB-Umleitung

Zur Fehlerbehebung und Ermittlung der Produkt- und Hersteller-IDs verschiedener Geräte, die Sie an das Clientsystem anschließen, können Sie die USB-Protokolle verwenden.

Sie können die Ablaufprotokollierung entweder nur für die aktuelle Sitzung oder über mehrere Neustarts hinweg aktivieren. Zur Aktivierung der Protokollierung für die aktuelle Sitzung muss ein Shell-Befehl verwendet werden. Zur Aktivierung der Protokollierung über mehrere Neustarts hinweg muss der Shell-Befehl zur entsprechenden Profildatei hinzugefügt werden.

### Voraussetzungen

Wenn Sie beabsichtigen, die Ablaufprotokollierung auch nach einem Systemneustart beizubehalten, müssen Sie auf dem Clientsystem über Administrator- oder Stammberechtigungen verfügen. Diese Voraussetzung gilt nicht, wenn Sie planen, die Protokollierung nur für die aktuelle Sitzung zu aktivieren.

### Vorgehensweise

- Wenn Sie die Protokollierung nur für die aktuelle Sitzung aktivieren möchten, muss der Befehl `launchctl` verwendet werden.
  - a Beenden Sie Horizon View Client, sodass der USB-Dienst „daemon“ angehalten wird.
  - b Öffnen Sie eine Shell (`/Applications/Utilities/Terminal.app`) als der Benutzer, der Horizon View Client startet.
  - c Verwenden Sie den folgenden Befehl:
 

```
launchctl setenv VMWARE_VIEW_USBD_LOG_OPTIONS "-o log:trace"
```
  - d Starten Sie Horizon View Client neu.
- Zur Aktivierung der Protokollierung über mehrere Neustarts hinweg muss der Befehl `launchctl` zur entsprechenden Shell `rc` oder zur Profildatei für Ihre gewählte Shell hinzugefügt werden (z. B. `~/ .bash_profile` für die Standard-Mac OS X-Shell).

Im Folgenden sehen Sie ein Beispiel für den Hinzufügungs-Befehl `launchctl`:

```
setenv VMWARE_VIEW_USBD_LOG_OPTIONS "-o log:trace"
```

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

Mit der Echtzeit-Audio/Video-Funktion können Sie die Webcam oder das Mikrofon Ihres lokalen Computers auf Ihrem Remote-Desktop verwenden.

Diese Funktion steht bei Verwendung von VMware Horizon View- 5.2 Feature Pack 2 oder später zur Verfügung. Informationen über das Einrichten der Echtzeit-Audio/Video-Funktion und über das Konfigurieren der Frame-Rate und Bildauflösung in einem Remote-Desktop finden Sie im Handbuch *Installation und Verwaltung von VMware Horizon View Feature Pack*. Informationen zum Konfigurieren dieser Einstellungen auf Clientsystemen finden Sie im VMware KB-Artikel *Festlegen von Frame-Raten und Auflösung für Echtzeit-Audio/Video auf Horizon View Clients* unter <http://kb.vmware.com/kb/2053644>.

Auf der Website <http://labs.vmware.com/flings/real-time-audio-video-test-application> können Sie eine Testanwendung herunterladen, mit der überprüft wird, ob die Echtzeit-Audio/Video-Funktion ordnungsgemäß installiert ist und fehlerfrei arbeitet. Diese Testanwendung ist als VMware-Fling verfügbar, weshalb kein technischer Support besteht.

### In diesen Fällen können Sie Ihre Webcam verwenden

Wenn Ihr Horizon View-Administrator die Echtzeit-Audio/Video-Funktion konfiguriert hat und Sie das PCoIP-Anzeigeprotokoll verwenden, kann eine integrierte oder an Ihren lokalen Computer angeschlossene Webcam auf Ihrem Desktop verwendet werden. Sie können die Webcam in Konferenzanwendungen wie z. B. Skype, Webex oder Google Hangouts verwenden.

Während der Einrichtung von Anwendungen wie z. B. Skype, Webex oder Google Hangouts auf Ihrem Remote-Desktop können Sie VMware Virtual Microphone und VMware Virtual Webcam als Eingabegeräte und VMware Virtual Audio als Ausgabegerät in den Menüs der Anwendung auswählen. Bei vielen Anwendungen kann diese Funktion ohne die Auswahl eines Eingabegeräts genutzt werden.

Wenn die Webcam zurzeit von Ihrem lokalen Computer genutzt wird, kann sie gleichzeitig vom Remote-Desktop verwendet werden. Genauso kann die Webcam vom lokalen Computer verwendet werden, wenn sie zurzeit vom Remote-Desktop genutzt wird.

---

**HINWEIS** Wenn Sie eine USB-Webcam verwenden, verbinden Sie diese nicht über das Menü **Desktop > USB** in Horizon View Client. Dies würde dazu führen, dass die USB-Umleitung für das Gerät aktiviert wird und die Leistung für einen Videochat nicht ausreicht.

---

Wenn mehr als eine Webcam an Ihren lokalen Computer angeschlossen ist, kann Ihr Administrator eine bevorzugte Webcam konfigurieren, die auf Ihrem Remote-Desktop verwendet wird. Stimmen Sie sich mit Ihrem Horizon View-Administrator ab, wenn Sie sich bezüglich der Webcamauswahl nicht sicher sind.

## Auswählen eines Standardmikrofons auf einem Mac OS X-Clientsystem

Wenn Sie auf Ihrem Clientsystem über mehrere Mikrofone verfügen, wird nur eines davon auf Ihrem Remote-Desktop verwendet. Zur Festlegung, welches Mikrofon standardmäßig auf dem Remote-Desktop verwendet werden soll, können Sie die „Systemeinstellungen“ auf Ihrem Clientsystem verwenden.

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

Dieses Verfahren beschreibt die Auswahl eines Mikrofons über die Benutzeroberfläche des Clientsystems. Administratoren können auch über die Mac OS X-Standardwerte ein bevorzugtes Mikrofon konfigurieren. Siehe „[Konfigurieren einer bevorzugten Webcam oder eines bevorzugten Mikrofons auf einem Mac OS X-Clientsystem](#)“, auf Seite 41.

---

**WICHTIG** Wenn Sie ein USB-Mikrofon verwenden, verbinden Sie dieses nicht über das Menü **Desktop > USB** in Horizon View Client. In diesem Fall würde das Gerät über die USB-Umleitung umgeleitet, sodass die Echtzeit-Audio/Video-Funktion nicht genutzt werden kann.

---

### Voraussetzungen

- Stellen Sie sicher, dass ein USB-Mikrofon oder ein anderer Mikrofontyp auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren Remote-Desktop verwenden.

### Vorgehensweise

- 1 Wählen Sie auf Ihrem Clientsystem **Apple-Menü > Systemeinstellungen** und klicken Sie auf **Ton**.
- 2 Öffnen Sie den Eingabebereich der Toneinstellungen.
- 3 Wählen Sie das bevorzugte Mikrofon aus.

Wenn Sie das nächste Mal eine Verbindung zu einem Remote-Desktop herstellen und einen Anruf starten, verwendet der Desktop das von Ihnen auf dem Clientsystem ausgewählte Standardmikrofon.

## Konfigurieren von Echtzeit-Audio/Video auf einem Mac OS X-Client

Einstellungen für Echtzeit-Audio/Video können Sie mithilfe der Mac OS X-Standardwerte über die Befehlszeile konfigurieren. Mit den Standardwerten können Sie benutzerdefinierte Mac OS X-Standardwerte mithilfe von Terminal (`/Applications/Utilities/Terminal.app`) lesen, schreiben und löschen.

Mac OS X-Standardwerte gehören zu Domänen. Domänen entsprechen in der Regel einzelnen Anwendungen. Die Domäne für die Echtzeit-Audio/Video-Funktion lautet `com.vmware.rtav`.

### Syntax zur Konfiguration von Echtzeit-Audio/Video

Für die Konfiguration der Echtzeit-Audio/Video-Funktion können Sie die folgenden Befehle verwenden.



**Tabelle 4-4.** Befehlssyntax für die Konfiguration von Echtzeit-Audio/Video

Befehl	Beschreibung
<code>defaults write com.vmware.rtav srcWCamId "Webcam-Benutzer-ID"</code>	Legt die bevorzugte Webcam für die Verwendung auf Remote-Desktops fest. Wenn dieser Wert nicht festgelegt ist, wird die Webcam automatisch durch die Systemauflistung ausgewählt. Sie können jede Webcam angeben, die an das Clientsystem angeschlossen (oder in dieses integriert) ist.
<code>defaults write com.vmware.rtav srcAudioInId "Audiogerät-Benutzer-ID"</code>	Legt das bevorzugte Mikrofon (Audioeingabegerät) für die Verwendung auf Remote-Desktops fest. Wenn dieser Wert nicht festgelegt ist, verwenden Remote-Desktops das Standard-Aufzeichnungsgerät auf dem Clientsystem. Sie können jedes Mikrofon angeben, das an das Clientsystem angeschlossen (oder in dieses integriert) ist.
<code>defaults write com.vmware.rtav srcWCamFrameWidthPixel</code>	Legt die Bildbreite fest. Hierfür wird standardmäßig ein hartcodierter Wert von 320 Pixeln verwendet. Die Bildbreite können Sie auf jeden Pixelwert ändern.
<code>defaults write com.vmware.rtav srcWCamFrameHeightPixel</code>	Legt die Bildhöhe fest. Hierfür wird standardmäßig ein hartcodierter Wert von 240 Pixeln verwendet. Die Bildhöhe können Sie auf jeden Pixelwert ändern.
<code>defaults write com.vmware.rtav srcWCamFrameRateF/s</code>	Legt die Framerate fest. Standardmäßig wird der Wert 15 F/s verwendet. Die Framerate können Sie auf jeden Wert ändern.
<code>defaults write com.vmware.rtav LogLevel "Ebene"</code>	Legt die Protokollierungsebene für die Echtzeit-Audio/Video-Protokolldatei fest ( <code>/Library/Logs/VMware/vmware-RTAV-pid.log</code> ). Als Protokollierungsebene können Sie „trace“ oder „debug“ festlegen.
<code>defaults write com.vmware.rtav IsDisabledWert</code>	Bestimmt, ob Echtzeit-Audio/Video aktiviert oder deaktiviert ist. Echtzeit-Audio/Video ist standardmäßig aktiviert. (Dieser Wert ist nicht aktiv.) Legen Sie „true“ fest, um Echtzeit-Audio/Video auf dem Client zu deaktivieren.
<code>defaults read com.vmware.rtav</code>	Zeigt Einstellungen für die Konfiguration von Echtzeit-Audio/Video an.
<code>defaults delete com.vmware.rtavEinstellung</code>	Löscht eine Einstellung für die Konfiguration von Echtzeit-Audio/Video. Beispiel: <code>defaults delete com.vmware.rtav srcWCamFrameWidth</code>

**HINWEIS** Sie können für die Framerate einen Wert zwischen 1 F/s und maximal 25 F/s sowie eine Auflösung von maximal 1920x1080 einstellen. Eine hohe Auflösung in Kombination mit einer schnellen Framerate wird möglicherweise nicht auf allen Geräten oder in allen Umgebungen unterstützt.

## Konfigurieren einer bevorzugten Webcam oder eines bevorzugten Mikrofons auf einem Mac OS X-Clientsystem

Wenn Sie die Echtzeit-Audio/Video-Funktion einsetzen und auf Ihrem Clientsystem über mehrere Webcams oder Mikrofone verfügen, kann nur eine Webcam oder ein Mikrofon auf Ihrem Remote-Desktop verwendet werden. Die bevorzugte Webcam und das bevorzugte Mikrofon legen Sie mithilfe der Mac OS X-Standardwerte über die Befehlszeile fest.

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

In den meisten Umgebungen muss kein bevorzugtes Mikrofon bzw. keine bevorzugte Webcam konfiguriert werden. Wenn Sie kein bevorzugtes Mikrofon festlegen, verwenden Remote-Desktops das standardmäßige Audiogerät, das in den Systemeinstellungen des Clientsystems festgelegt ist. Siehe „[Auswählen eines Standardmikrofons auf einem Mac OS X-Clientsystem](#)“, auf Seite 40. Wenn Sie keine bevorzugte Webcam konfigurieren, wählt der Remote-Desktop die Webcam anhand der Auflistung aus.

### Voraussetzungen

- Stellen Sie beim Konfigurieren einer bevorzugten USB-Webcam sicher, dass die Webcam auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Stellen Sie beim Konfigurieren eines bevorzugten USB-Mikrofons oder eines sonstigen Mikrofontyps sicher, dass das Mikrofon auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren Remote-Desktop verwenden.

### Vorgehensweise

- 1 Starten Sie auf Ihrem Mac OS X-Clientsystem eine Webcam- oder Mikrofonanwendung, um eine Auflistung der Kamera- oder Audiogeräte in der Echtzeit-Audio/Video-Protokolldatei auszulösen.
  - a Schließen Sie die Webcam oder das Audiogerät an.
  - b Doppelklicken Sie im Ordner **Anwendungen** auf **VMware Horizon View Client**, um Horizon View Client zu starten.
  - c Starten Sie einen Anruf und beenden Sie ihn dann.
- 2 Suchen Sie in der Echtzeit-Audio/Video-Protokolldatei nach Protokolleinträgen für die Webcam oder das Mikrofon.
  - a Öffnen Sie die Echtzeit-Audio/Video-Protokolldatei in einem Text-Editor.  
Die Echtzeit-Audio/Video-Protokolldatei heißt `/Library/Logs/VMware/vmware-RTAV-pid.log`, wobei `pid` für die Prozess-ID der aktuellen Sitzung steht.
  - b Suchen Sie in der Echtzeit-Audio/Video-Protokolldatei nach Einträgen für die angeschlossenen Webcams oder Mikrofone.

Das folgende Beispiel veranschaulicht Webcam-Einträge in der Echtzeit-Audio/Video-Protokolldatei:

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
1 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=FaceTime HD Camera (Built-in)  UserId=FaceTime HD Camera (Built-
in)#0xfa20000005ac8509  SystemId=0xfa20000005ac8509
```

Das folgende Beispiel veranschaulicht Mikrofon-Einträge in der Echtzeit-Audio/Video-Protokolldatei:

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: int AVCaptureEnumerateAudioDevi-
ces(MMDev::DeviceList&) -
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- 2 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- Index=255  Name=Built-in Microphone  UserId=Built-in Microphone#AppleHDAEngineInput:1B,
0,1,0:1  SystemId=AppleHDAEngineInput:1B,0,1,0:1
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- Index=255  Name=Built-in Input  UserId=Built-in Input#AppleHDAEngineInput:1B,0,1,1:2
SystemId=AppleHDAEngineInput:1B,0,1,1:2
```

- 3 Suchen Sie in der Echtzeit-Audio/Video-Protokolldatei nach der bevorzugten Webcam oder dem bevorzugten Mikrofon und notieren Sie sich die zugehörige Benutzer-ID.

Die Benutzer-ID wird in der Protokolldatei nach der Zeichenfolge „UserId=“ aufgeführt. Beispielsweise lautet die Benutzer-ID der internen FaceTime-Kamera „FaceTime HD Camera (Built-in)“, und die Benutzer-ID des internen Mikrofons lautet „Built-in Microphone“.

- 4 Legen Sie in Terminal (/Applications/Utilities/Terminal.app) mithilfe des Befehls `defaults write` die bevorzugte Webcam bzw. das bevorzugte Mikrofon fest.

Option	Aktion
<b>Bevorzugte Webcam festlegen</b>	Geben Sie <code>defaults write com.vmware.rtav srcWCamId "Webcam-Benutzer-ID"</code> ein, wobei <i>Webcam-Benutzer-ID</i> für die Benutzer-ID der bevorzugten Webcam steht, die Sie anhand der Echtzeit-Audio/Video-Protokolldatei ermittelt haben. Beispiel: <code>defaults write com.vmware.rtav srcWCamId "HD Webcam C525"</code>
<b>Bevorzugtes Mikrofon festlegen</b>	Geben Sie <code>defaults write com.vmware.rtav srcAudioInId "Audiogerät-Benutzer-ID"</code> ein, wobei <i>Audiogerät-Benutzer-ID</i> für die Benutzer-ID des bevorzugten Mikrofons steht, die Sie anhand der Echtzeit-Audio/Video-Protokolldatei ermittelt haben. Beispiel: <code>defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"</code>

- 5 (Optional) Überprüfen Sie mithilfe des Befehls `defaults read` Ihre Änderungen an der Echtzeit-Audio/Video-Funktion.

Beispiel: `defaults read com.vmware.rtav`

Mit diesem Befehl werden alle Einstellungen für Echtzeit-Audio/Video aufgeführt.

Wenn Sie das nächste Mal eine Verbindung zu einem Remote-Desktop herstellen und einen Anruf starten, verwendet der Desktop soweit verfügbar die bevorzugte Webcam bzw. das bevorzugte Mikrofon, die bzw. das Sie konfiguriert haben. Falls die bevorzugte Webcam oder das bevorzugte Mikrofon nicht verfügbar ist, kann der Remote-Desktop eine andere verfügbare Webcam oder ein anderes verfügbares Mikrofon verwenden.

## Kopieren und Einfügen von Text und Bildern

Sie können standardmäßig Text von Ihrem Clientsystem auf einen Remote-Desktop kopieren und einfügen. Wenn Ihr Administrator die Funktion aktiviert, können Sie auch Text zwischen einem Remote-Desktop und Ihrem Clientsystem oder zwischen zwei Remote-Desktops kopieren und einfügen. Hierfür gelten allerdings einige Einschränkungen.

Wenn Sie das PCoIP-Anzeigeprotokoll sowie einen Horizon View-Remote-Desktop vom Typ 5.x oder eine neuere Version verwenden, kann Ihr View-Administrator diese Funktion so einstellen, dass Kopier- und Einfügevorgänge nur von Ihrem Clientsystem auf einen Remote-Desktop oder nur von einem Remote-Desktop zu Ihrem Clientsystem oder beide Vorgänge zugelassen werden bzw. keiner der beiden Vorgänge zugelassen wird.

Die Administratoren konfigurieren die Möglichkeit zum Kopieren/Einfügen durch die Verwendung von Gruppenrichtlinienobjekten (GPOs), die View Agent auf den Remote-Desktops zugeordnet sind. Weitere Informationen finden Sie unter dem Thema über allgemeine Sitzungsvariablen von View PCoIP im Dokument *Verwaltung von VMware Horizon View*- im Kapitel über die Konfigurationsrichtlinien.

Zu den unterstützten Dateiformaten gehören Text, Bilder und RTF (Rich Text Format). In der Zwischenablage können bis zu 1 MB an Daten für Kopier- und Einfügevorgänge gespeichert werden. Wenn Sie formatierten Text kopieren, handelt es sich bei den Daten teilweise um Text und teilweise um Formatierungsinformationen. Ein Dokument mit einer Größe von 800 KB kann beim Kopieren eine Datenmenge von mehr als 1 MB besitzen, da mehr als 200 KB an RTF-Daten in der Zwischenablage gespeichert werden.

Wenn Sie daher eine große Menge an formatiertem Text oder Text und ein Bild kopieren, kann es beim Einfügen dazu kommen, dass Sie den Text ganz oder teilweise sehen, nicht aber die Formatierung oder das Bild. Dies liegt daran, dass die drei Arten von Daten separat gespeichert werden können. Je nach Art des Dokuments, von dem aus Sie kopieren, können Bilder möglicherweise als Bilder oder als RTF-Daten gespeichert werden.

Beträgt die Gesamtmenge von Text und RTF weniger als 1 MB, wird der formatierte Text eingefügt. Es ist häufig der Fall, dass die RTF-Daten nicht gekürzt werden können, sodass die RTF-Daten verworfen und nur der reine Text eingefügt wird, sollten Text und Formatierung zusammen mehr als 1 MB umfassen.

Sollten Sie nicht in der Lage sein, den gesamten formatierten Text und die von Ihnen ausgewählten Bilder einzufügen, versuchen Sie geringere Teilmengen zu speichern und einzufügen.

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

## Drucken von einem Remote-Desktop aus

Sie können von einem Remote-Desktop aus Dokumente auf einem virtuellen Drucker oder einem USB-Drucker ausdrucken, der mit Ihrem Clientcomputer verbunden ist. Die virtuelle Druckfunktion und das Drucken mit USB-Umleitung können ohne Konflikte gemeinsam eingesetzt werden.

### Aktivieren des virtuellen Drucks auf dem Mac OS X-Client

Mit Horizon View Client 2.1 oder höher können Sie, wenn Sie das PCoIP-Anzeigeprotokoll verwenden, für Ihren lokalen Computer konfigurierte Drucker von Ihrer virtuellen Maschine aus verwenden, ohne Druckertreiber auf der virtuellen Maschine installieren zu müssen.

Die virtuelle Druckfunktion steht zur Verfügung, ohne dass eine Treiberinstallation erforderlich ist.

Wenn die Funktion für den virtuellen Druck aktiviert ist, zeigt das Menü **Desktop** den Eintrag **Druckfunktion aktiviert**.

Sie können den virtuellen Druck beim ersten Start von Horizon View Client aktivieren. Klicken Sie auf **Weiter**, wenn Horizon View Client Sie zum Starten der USB- und Druckdienste für Remote-Desktops auffordert, und geben Sie Ihre Systemanmeldeinformationen ein.

Wenn Sie den virtuellen Druck nicht beim ersten Start von Horizon View Client aktivieren, können Sie das Menü **Desktop** dazu verwenden, die Funktion für den virtuellen Druck später zu aktivieren.

- Zum Aktivieren der virtuellen Druckfunktion vor der Verbindungsherstellung mit einem Desktop wählen Sie im Menü **VMware Horizon View Client** die Option **Desktop > Druckdienste starten** aus. Klicken Sie im Dialogfeld Druckdienste für Remote-Desktop starten auf **Fortfahren** und geben Sie Ihre Systemanmeldeinformationen ein.
- Zum Aktivieren der virtuellen Druckfunktion nach der Verbindungsherstellung mit einem Desktop wählen Sie im Menü **VMware Horizon View Client** die Option **Desktop > Druckdienste starten** aus. Klicken Sie auf **Fortfahren**, geben Sie Ihre Systemanmeldeinformationen ein und stellen Sie erneut eine Verbindung mit dem Desktop her. Wenn Sie die Desktop-Verbindung abbrechen, können Sie auf **Desktop > Druckfunktion aktivieren** klicken. Horizon View Client fordert Sie daraufhin zur erneuten Verbindungsherstellung mit dem Desktop auf.

## Festlegen von Druckeinstellungen für die virtuelle Druckfunktion

Die virtuelle Druckfunktion ermöglicht Endbenutzern das Verwenden von lokalen oder Netzwerkdruckern auf einem Remote-Desktop, ohne dass im Remote-Desktop zusätzliche Druckertreiber installiert werden müssen. Für jeden Drucker, der über diese Funktion zur Verfügung steht, können Sie Voreinstellungen für Datenkomprimierung, Druckqualität, doppelseitigen Druck, Farbe usw. festlegen.

Nachdem dem lokalen Computer ein Drucker hinzugefügt wurde, fügt Horizon View Client diesen Drucker der Liste der verfügbaren Drucker auf dem Remote-Desktop hinzu. Keine weitere Konfiguration ist erforderlich. Benutzer mit Administratorrechten können weiterhin Druckertreiber auf dem Remote-Desktop installieren, ohne einen Konflikt mit der virtuellen Druckfunktion zu verursachen.

---

**WICHTIG** Diese Funktion steht für die folgenden Druckertypen nicht zur Verfügung:

- USB-Drucker, die die USB-Umleitungsfunktion zur Verbindung mit einem virtuellen USB-Port im Remote-Desktop verwenden
 

Sie müssen den USB-Drucker im Remote-Desktop trennen, um die virtuelle Druckfunktion verwenden zu können.
  - Die Windows-Funktion für die Ausgabe in einer Datei
 

Das Kontrollkästchen **Ausgabe in Datei** im Dialogfeld **Drucken** kann nicht ausgewählt werden. Ein Druckertreiber, über den eine Datei erstellt wird, kann verwendet werden. Beispielsweise können Sie einen PDF-Writer zum Drucken einer PDF-Datei verwenden.
- 

Dieses Verfahren beschreibt die Schritte auf einem Remote-Desktop mit einem Windows 7- oder Windows 8.x-Betriebssystem (Desktop). Die Vorgehensweise ähnelt der für Windows XP und Windows Vista, ist aber nicht vollständig gleich.

### Voraussetzungen

Stellen Sie sicher, dass die virtuelle Druckfunktion von View Agent auf dem Remote-Desktop installiert ist. Die Treiber befinden sich im Remote-Desktop-Dateisystem unter `C:\Programme\Gemeinsame Dateien\VMware\Drivers\Virtual Printer`.

Die Installation von View Agent ist eine der Aufgaben, die im Rahmen der Vorbereitung einer virtuellen Maschine auf die Verwendung als Remote-Desktop durchgeführt werden muss. Weitere Informationen finden Sie im Dokument *Verwaltung von VMware Horizon View*.

### Vorgehensweise

- 1 Klicken Sie auf einem Remote-Desktop mit Windows 7 oder Windows 8.x auf **Start > Geräte und Drucker**.
- 2 Klicken Sie im Fenster „Geräte und Drucker“ mit der rechten Maustaste auf den Standarddrucker und wählen Sie aus dem Kontextmenü **Druckereigenschaften** und dann den Drucker aus.
 

Auf dem Remote-Desktop werden virtuelle Drucker als `<Druckername>#:<Nummer>` angezeigt.
- 3 Klicken Sie im Fenster mit den Druckereigenschaften auf die Registerkarte **Geräteeinstellungen** und geben Sie die zu verwendenden Einstellungen an.
- 4 Klicken Sie auf der Registerkarte **Allgemein** auf **Einstellungen** und geben Sie die zu verwendenden Einstellungen an.
- 5 Klicken Sie im Dialogfeld mit den Druckereinstellungen auf die verschiedenen Registerkarten und geben Sie an, welche Einstellungen verwendet werden sollen.
 

Für die erweiterte Einstellung **Seitenanpassung** empfiehlt VMware, die Standardeinstellungen beizubehalten.

- 6 Klicken Sie auf **OK**.

## Verwenden von USB-Druckern

In einer Horizon View-Umgebung können virtuelle Drucker und umgeleitete USB-Drucker ohne Konflikte miteinander verwendet werden.

Ein USB-Drucker ist ein Drucker, der an einen USB-Port auf dem lokalen Clientsystem angeschlossen ist. Zum Senden von Druckaufträgen an einen USB-Drucker können Sie entweder die USB-Umleitungsfunktion oder die virtuelle Druckfunktion verwenden. Der USB-Druck ist gelegentlich schneller als der virtuelle Druck, abhängig von den Netzwerkbedingungen.

- Sie können die USB-Umleitungsfunktion zum Anschließen eines USB-Druckers an einen virtuellen USB-Port auf dem Remote-Desktop verwenden, sofern die erforderlichen Treiber auf dem Remote-Desktop installiert sind.

Wenn Sie diese Umleitungsfunktion verwenden, ist der Drucker nicht länger logisch an den physischen USB-Port auf dem Client angeschlossen. Aus diesem Grund wird der USB-Drucker nicht mehr in der Liste der lokalen Drucker angezeigt. Dies bedeutet auch, dass Sie über den USB-Drucker auf dem Remote-Desktop drucken können, nicht jedoch über die lokale Clientmaschine.

Auf dem Remote-Desktop werden umgeleitete USB-Drucker als *<Druckername>* angezeigt.

Informationen zur Verbindungsherstellung mit einem USB-Drucker finden Sie unter „[Verbinden von USB-Geräten](#)“, auf Seite 31.

- Auf einigen Clients können Sie alternativ die virtuelle Druckfunktion nutzen, um Druckaufträge an einen USB-Drucker zu senden. Wenn Sie die virtuelle Druckfunktion verwenden, können Sie sowohl über den Remote-Desktop als auch über den lokalen Client auf dem USB-Drucker drucken, und es ist nicht erforderlich, Druckertreiber auf dem Remote-Desktop zu installieren.

## PCoIP-Client-Bildcache

Bei der PCoIP-Client-Bildzwischenspeicherung wird der Bildinhalt auf dem Client gespeichert, um erneute Übertragungen zu vermeiden. Durch diese Funktion wird die Bandbreitenauslastung reduziert.

---

**WICHTIG** Diese Funktion ist nur verfügbar, wenn View Agent und der View-Verbindungsserver über die View-Version 5.0 oder höher verfügen.

---

Der PCoIP-Bildcache erfasst die räumliche sowie zeitliche Redundanz. Wenn Sie beispielsweise in einem PDF-Dokument einen Bildlauf nach unten durchführen, wird unten im Fenster neuer Inhalt angezeigt, während oben im Fenster der älteste Inhalt nicht mehr angezeigt wird. Der restliche Inhalt bleibt unverändert und wird nach oben verschoben. Der PCoIP-Bildcache kann räumliche und zeitliche Redundanz erkennen.

Da es sich während des Bildlaufs bei den an das Client-Gerät gesendeten Anzeigeeinformationen in erster Linie um eine Abfolge von Cache-Indizes handelt, lassen sich durch die Verwendung eines Bildcaches deutliche Bandbreiteneinsparungen erzielen. Dieser effiziente Bildlauf hat sowohl bei LAN- als auch WAN-Verbindungen Vorteile.

- Bei LAN-Verbindungen mit relativ uneingeschränkter Bandbreite führt die clientseitige Bildzwischenspeicherung zu deutlichen Bandbreiteneinsparungen.
- Um bei WAN-Verbindungen innerhalb der Bandbreiteneinschränkungen zu bleiben, nimmt die Bildlaufleistung ohne clientseitige Zwischenspeicherung ab. Bei WAN-Verbindungen führt die clientseitige Zwischenspeicherung zu einer Einsparung von Bandbreite und stellt einen reibungslosen, äußerst schnellen Bildlauf sicher.

Mithilfe der clientseitigen Zwischenspeicherung speichert der Client Teile der Anzeige, die zuvor übertragen wurden. Die Cachegröße beträgt 250 MB.

Bei Horizon View Client 2.0 und höheren Versionen und der Verwendung von Horizon View 5.2-Servern und -Desktops liefert ein 90-MB-Client-Cache die gleiche Leistung wie ein 250-MB-Cache bei früheren Versionen.





# Fehlerbehebung für Horizon View Client

# 5

Sie können die meisten Probleme mit Horizon View Client lösen, indem Sie den Desktop zurücksetzen oder die VMware Horizon View Client-Anwendung neu installieren.

Dieses Kapitel behandelt die folgenden Themen:

- „Zurücksetzen eines Desktops“, auf Seite 49
- „Deinstallieren von Horizon View Client“, auf Seite 50

## Zurücksetzen eines Desktops

Eventuell muss der Desktop zurückgesetzt werden, wenn das Desktop-Betriebssystem nicht mehr reagiert. Beim Zurücksetzen wird der Desktop heruntergefahren und neu gestartet. Nicht gespeicherte Daten gehen verloren.

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 ohne vorheriges Speichern geschlossen.

Sie können den Desktop nur zurücksetzen, wenn Ihr View-Administrator diese Funktion aktiviert hat.

### Vorgehensweise

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

Option	Aktion
<b>Aus dem Desktop-Betriebssystem heraus</b>	Wählen Sie in der Menüleiste <b>Desktop &gt; Zurücksetzen</b> .
<b>Vom Startbildschirm aus (mit Serversymbolen)</b>	<ol style="list-style-type: none"><li>Doppelklicken Sie auf das Serversymbol und geben Sie die Anmeldeinformationen an.  Dazu zählen möglicherweise die RSA SecurID-Anmeldeinformationen und die Anmeldeinformationen zur Anmeldung am Desktop.</li><li>Wählen Sie zuerst den Desktop und anschließend <b>Desktop &gt; Zurücksetzen</b> aus der Menüleiste aus.</li></ol>
<b>Vom Startbildschirm aus (mit Desktop-Symbolen)</b>	Wählen Sie zuerst den Desktop und anschließend <b>Desktop &gt; Zurücksetzen</b> aus der Menüleiste aus.

Das Betriebssystem im Remote-Desktop wird neu gestartet. Horizon View Client wird vom Desktop getrennt.

### Weiter

Warten Sie eine Weile, bis das System gestartet wurde, und versuchen Sie anschließend, eine Verbindung zum Remote-Desktop herzustellen.

## Deinstallieren von Horizon View Client

Manchmal können Sie Probleme mit Horizon View Client einfach dadurch beheben, dass Sie die Horizon View Client-Anwendung deinstallieren und anschließend neu installieren.

Die Vorgehensweise beim Deinstallieren von Horizon View Client entspricht der Vorgehensweise bei der Deinstallation anderer Anwendungen.

Ziehen Sie die **VMware Horizon View Client**-Anwendung vom Ordner **Anwendungen** zum **Papierkorb** und leeren Sie diesen.

Nachdem Sie die Deinstallation durchgeführt haben, können Sie die Anwendung von neuem installieren.

Siehe [„Installieren von Horizon View Client auf Mac OS X“](#), auf Seite 11.

# Index

## A

- Abmeldung **25**
- automatische Verbindung von USB-Geräten **31**

## B

- Betriebssystem-, Unterstützung auf View Agent **9**
- Bildcache, Client **46**
- Bilder, kopieren **43**

## C

- Client-Bildcache **46**

## D

- Deinstallieren von View Client **50**
- Desktop
  - Abmelden **25**
  - Rollback **27**
  - wechseln **25**
  - zurücksetzen **49**
- Desktop zurücksetzen **49**
- Dock **12**
- Drucken über einen Desktop **44**
- Drucker, einrichten **45**

## E

- Echtzeit-Audio/Video, Systemanforderungen **8**
- erneute Anmeldung an einem Remote-Desktop **21**

## F

- Funktionsunterstützungs-Matrix, für Mac OS X **29**

## G

- Geräte, USB **38**
- Gerätefamilien **37**
- Geräten
  - USB **33**
  - Verbinden von USB- **31**

## H

- Hardwareanforderungen, Mac **7**
- Horizon View Client
  - Download über View Portal **9**
  - Fehlerbehebung **49**
  - Installieren unter Mac OS X **11**

- Konfiguration für Mac-Clients **7**
- starten **21**
- Systemanforderungen für Mac OS X **7**
- Trennen der Verbindung mit einem Desktop **25**

## M

- Mac OS X
  - Installieren von Horizon View Client auf View Client-Installation **11**
- mehrere Monitore **30**
- Menübefehl Strg+Alt+Entf senden **25**
- Mikrofon **40**

## N

- Neuanordnen von Verknüpfungen **27**

## O

- OS X, Installieren von Horizon View Client **11**

## P

- PCoIP-Client-Bildcache **46**
- Programm zur Verbesserung der Benutzerfreundlichkeit, Desktop-Pool-Daten **13**
- Protokollieren, für USB-Geräte **38**

## R

- Remote-Desktop, Rollback **27**
- Retina-Display **30**
- Rollback eines Remote-Desktops **27**

## S

- Server-Verknüpfung **26**
- Serververbindungen **21**
- Sicherheitsserver **9**
- SSL-Zertifikate, Überprüfen **12**
- Strg+Alt+Entf **25**
- Suchen nach Remote-Desktops **24**
- Systemanforderungen, für Mac OS X **7**

## T

- Text, kopieren **43**
- Text und Bilder einfügen **43**
- Text und Bilder kopieren **43**
- ThinPrint-Einrichtung **45**

Trennen der Verbindung mit einem Remote-  
Desktop **25**

## **U**

Überprüfung des Serverzertifikats **12**

Überprüfungsmodi für die Zertifikatsprüfung **12**

Umleitung

Eigenschaften für USB-Geräte **35**

USB **33, 38**

UPNs, Horizon View Client **21**

URI-Beispiele **18**

URI-Syntax für View Clients **16**

URIs (Uniform Resource Identifier) **15**

USB-Drucker **44, 46**

USB-Geräte **31**

USB-Gerätefamilien **37**

USB-Umleitung **33, 38**

## **V**

Verbinden, USB-Geräte **31**

Verknüpfung für View-Verbindungsserver **26**

View Agent, Installationsanforderungen **9**

View Portal **9**

View-Verbindungsserver, Verknüpfung für **26**

virtuelle Drucker **44**

virtuelle Druckfunktion **45**

Virtuelles Drucken **44**

Voraussetzungen für Clientgeräte **9**

## **W**

Webcam **39, 41**

Wechseln zwischen Desktops **25**

Weiterleiten von USB-Geräten **33**

## **Z**

Zertifikate, Ignorieren von Problemen **12, 23**

Zwischenspeicherung, Clientseitiges Bild **46**