Verwendung von VMware View Horizon Client für Windows

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-001179-02

vmware®

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

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
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

Inhalt

Verwendung von VMware Horizon View Client für Windows

Dieses Handbuch, *Verwendung von VMware Horizon View Client für Windows*, bietet Informationen über die Installation und Verwendung der VMware® Horizon View™-Software auf einem Microsoft Windows-Clientsystem zur Verbindungsherstellung mit einem View-Desktop im Rechenzentrum.

Die Informationen in diesem Dokument umfassen Systemanforderungen und Anweisungen zur Installation und Verwendung von Horizon View Client für Windows.

Diese Informationen sind für Administratoren bestimmt, die eine Bereitstellung von Horizon View mit Microsoft Windows-Clientsystemen ermöglichen müssen, so z. B. Desktops und Laptops. Die Informationen wurden für erfahrene Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen sowie mit Vorgängen in Rechenzentren vertraut sind.

Systemanforderungen und Setup von Windows-basierten View Clients

1

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

Systeme mit View Client auf Windows verwenden bei der Verbindungsherstellung mit dem View-Verbindungsserver Microsoft Internet Explorer-Einstellungen, z. B. Proxyeinstellungen. Stellen Sie sicher, dass Ihre Internet Explorer-Einstellungen richtig sind und Sie über Internet Explorer auf die URL für den View-Verbindungsserver zugreifen können.

Dieses Kapitel behandelt die folgenden Themen:

Systemanforderungen für Windows-Clients

Horizon View Client für Windows kann auf PCs oder Laptops installiert werden, die ein Microsoft Windows 8.x-, Windows 7-, Vista- oder XP-Betriebssystem verwenden.

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

Modell

Standardmäßiges x86-System oder x86-System mit 64-Bit-Kompatibilität für Desktop- oder Laptopcomputer

Arbeitsspeicher

Mindestens 1GB Arbeitsspeicher (RAM)

Betriebssysteme

Betriebssystem	Version	SP
Windows 8 oder 8.1	32 oder 64 Bit	–
Windows 7	32 oder 64 Bit	Ohne oder SP1
Windows XP	32 Bit	SP3
Windows Vista	32 Bit	SP1 oder SP2

Für Windows 7 und Windows Vista werden die folgenden Editionen unterstützt: Home, Enterprise, Professional/Business und Ultimate. Für Windows XP werden die Editionen Home und Professional unterstützt.

Für Windows 8 und 8.1 werden die folgenden Editionen unterstützt: Windows 8 oder 8.1 Pro - Desktop und Windows 8 oder 8.1 Enterprise – Desktop.

View-Verbindungsserver, Sicherheitsserver und View Agent

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 Sicherheitsservers. Mit einem Sicherheitsserver erfordern die Clientsysteme keine VPN-Verbindung.

Anzeigeprotokoll für Horizon View

PCoIP oder RDP

Hardwareanforderungen für PCoIP

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

  ```
  20 MB + (24 * (Anzahl der Monitore) * (Breite des Monitors) *
  (Höhe des Monitors))
  ```

  Als grobes Maß können Sie die folgenden Berechnungen verwenden:

  ```
  1 Monitor: 1600 x 1200: 64 MB
  2 Monitore: 1600 x 1200: 128MB
  3 Monitore: 1600 x 1200: 256MB
  ```

Hardwareanforderungen für RDP

- x86-basierter Prozessor mit SSE2-Erweiterungen, mit einer Prozessorgeschwindigkeit von 800 MHz oder höher.

- 128 MB RAM.

Softwareanforderungen für RDP

- Für Windows XP- und Windows XP Embedded-Systeme ist Microsoft RDP 6.1 zu verwenden.
- Windows Vista umfasst RDP 6.1; es wird jedoch RDP 7.1 empfohlen.
- Für Windows 7 ist RDP 7.1 oder 8.0 zu verwenden. Windows 7 umfasst RDP 7. Windows 7 SP1 umfasst RDP 7.1.
- Für Windows 8 ist RDP 8.0 zu verwenden. Für Windows 8.1 ist RDP 8.1 zu verwenden.
- Für virtuelle Windows XP-Maschinen müssen Sie die RDP-Patches installieren, die in den Knowledgebase-Artikeln 323497 und 884020 aufgeführt sind. Wenn Sie die RDP-Patches nicht installieren, wird möglicherweise ein Windows Socket-Fehler auf dem Client angezeigt.
- Das View Agent-Installationsprogramm konfiguriert die lokale Firewall-Regel für eingehende RDP-Verbindungen entsprechend dem aktuellen RDP-Port des Hostbetriebssystems (üblicherweise 3389). Wenn Sie die RDP-Portnummer ändern, müssen Sie die dazugehörigen Firewall-Regeln ändern.

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

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.

Horizon View-Remote-Desktop

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 *Installation und Verwaltung von VMware Horizon View Feature Pack* für VMware Horizon View-

Horizon View Client-Software

Horizon View Client 2.2 für Windows oder höher

Horizon View Client-Computer oder Clientzugriffsgerät

- Echtzeit-Audio/Video wird auf allen Betriebssystemen unterstützt, auf denen Horizon View Client für Windows ausgeführt wird. Weitere Informationen finden Sie unter „Systemanforderungen für Windows-Clients“, auf Seite 8.
- 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.

Anzeigeprotokoll für Horizon View

PCoIP

Echtzeit-Audio/Video wird in RDP-Desktop-Sitzungen nicht unterstützt.

Voraussetzungen für die Verwendung der Multimedia-Umleitung (MMR)

Die Multimedia-Umleitung (MMR) stellt den Multimedia-Stream direkt auf den Clientcomputern bereit.

Mit MMR wird der Multimediadatenstrom auf dem Clientsystem verarbeitet, d. h. entschlüsselt. Das Clientsystem gibt die Medieninhalte wieder und lagert so die Anforderung vom ESXi-Host aus.

Da MMR auf den verschiedenen Betriebssystemen unterschiedlich implementiert wird, unterscheiden sich die Systemanforderungen für Windows 7 von denen für Windows Vista und früheren Betriebssystemen.

WICHTIG Windows 8 View-Desktops unterstützen MMR nicht. Verwenden Sie für diese View-Agenten die Windows-Medienumleitung, die im Lieferumfang von RDP 7 und später enthalten ist.

MMR-Unterstützung und Anforderungen für Windows 7

Ihre Server, virtuellen Desktops und Clientcomputer müssen bestimmte Systemanforderungen erfüllen, um MMR auf View-Desktops mit Windows 7 und auf Clients mit Windows 7 oder Windows 8 verwenden zu können.

VMware-Softwareanforderungen

- Auf den Horizon View-Servern und -Desktops muss VMware Horizon View- 5.3 oder eine spätere Version installiert sein.
- Auf den virtuellen Desktops müssen Sie zudem den aktuellen Remote Experience Agent installieren. Siehe *Installation und Verwaltung von VMware Horizon View Feature Pack* für VMware Horizon View- 5.3 Feature Pack 1.
- Auf View Clients müssen Sie VMware Horizon View Client 2.2 oder später für Windows installieren.
- Informationen über andere erforderliche Konfigurationseinstellungen finden Sie im Dokument *Installation und Verwaltung von VMware Horizon View Feature Pack* für VMware Horizon View- 5.3 Feature Pack 1.

Horizon View-Desktop

- Auf den Desktops muss ein Windows 7-Betriebssystem mit 64 Bit oder 32 Bit ausgeführt werden.
- Für den Desktop-Pool muss das **3D-Rendering** aktiviert werden.
- Die virtuellen Desktop-Maschinen müssen virtuelle Hardware der Version 8 oder höher verwenden.
- Benutzer müssen Videos mit Windows Media Player 12 oder höher abspielen.

View Client-Computer oder Clientzugriffsgerät

- Auf den Clients muss ein Windows 7- oder Windows 8-Betriebssystem mit 64 Bit oder 32 Bit ausgeführt werden.
- Die Clients müssen über DVXA-kompatible (DirectX Video Acceleration) Grafikkarten verfügen, die die ausgewählten Videos decodieren können.

- Auf den Clients muss Windows Media Player 12 oder höher installiert sein, um eine Umleitung zur lokalen Hardware zu unterstützen.

Unterstützte Medienformate

Die Medienformate müssen dem H.264-Standard zur Videokomprimierung entsprechen. Die Dateiformate M4V, MP4 und MOV werden unterstützt. Ihre virtuellen Desktops müssen eines dieser Dateiformate verwenden, und auf den Clientsystemen müssen lokale Decoder für diese Formate vorhanden sein.

MMR-Unterstützung und Anforderungen für Windows Vista und Windows XP

Ihre Server, virtuellen Desktops und Clientcomputer müssen bestimmte Systemanforderungen erfüllen, um MMR auf View-Desktops und -Clients mit Windows Vista und Windows XP verwenden zu können.

VMware-Softwareanforderungen

- Sie müssen über VMware View-Server und -Desktops der Version 4.6.1 oder später verfügen.
- Auf View Clients müssen Sie View Client für Windows, Version 4.6.1 oder später, installieren.

Horizon View-Desktop

- Auf den Desktops muss die 32-Bit-Version von Windows Vista oder Windows XP ausgeführt werden.
- Benutzer müssen Videos mit Windows Media Player 10 oder höher abspielen.

View Client-Computer oder Clientzugriffsgerät

- Auf den Clients muss die 32-Bit-Version von Windows Vista, Windows XP oder Windows XP Embedded ausgeführt werden.
- Auf den Clients muss Windows Media Player 10 oder höher installiert sein, um eine Umleitung zur lokalen Hardware zu unterstützen.
- Die View Client-Hardware zur Videoanzeige muss Overlay-Unterstützung bieten, damit MMR ordnungsgemäß funktioniert.

Unterstützte Medienformate

Die MMR-Funktion unterstützt die Mediendateiformate, die das Clientsystem unterstützt, da auf dem Client lokale Decoder vorhanden sein müssen. Dateiformate sind unter anderem MPEG2-1, MPEG-2, MPEG-4 Part 2; WMV 7, 8 und 9; WMA; AVI; ACE; MP3 und WAV.

Hinweis Sie müssen den MMR-Port in Ihrer Firewall-Software als Ausnahme hinzufügen. Der standardmäßige Port für MMR lautet 9427.

Anforderungen zur Verwendung der Flash-URL-Umleitung

Durch das direkte Streaming von Flash-Inhalten von Adobe Media Server auf Clientendpunkte wird die Datenlast auf dem ESXi-Host im Rechenzentrum gesenkt, das zusätzliche Routing über das Rechenzentrum vermieden und die erforderliche Bandbreite zum simultanen Streaming von Live-Video-Ereignissen an mehrere Clientendpunkte verringert.

Die Flash-URL-Umleitung verwendet ein JavaScript, das durch den Webseitenadministrator in eine Webseite eingebettet wird. Immer dann, wenn ein Benutzer eines virtuellen Desktops aus einer Webseite auf den festgelegten URL-Link klickt, fängt das JavaScript die ShockWave-Datei (SWF) von der virtuellen Desktop-Sitzung ab und leitet sie an den Clientendpunkt um. Der Endpunkt kann anschließend außerhalb der virtuellen Desktop-Sitzung einen lokalen VMware Flash Projector öffnen und den Medienstream lokal abspielen.

Diese Funktion ist verfügbar, wenn sie zusammen mit der richtigen Version des VMware Horizon View-Feature Packs verwendet wird.

- Anforderungen für Multicast-Unterstützung: VMware Horizon View- 5.2 Feature Pack 2 oder später.
- Anforderungen für Unicast-Unterstützung: VMware Horizon View- 5.3 Feature Pack 1 oder später.

Um diese Funktion zu verwenden, müssen Sie Ihre Webseite und Ihre Clientgeräte einrichten. Die Clientsysteme müssen bestimmte Softwareanforderungen erfüllen:

- Für eine Multicast-Unterstützung müssen Sie die Clientsysteme Horizon View Client 5.4 oder 2.2 oder später verwenden. Für eine Unicast-Unterstützung müssen Sie die Clientsysteme Horizon View Client 2.2 oder später verwenden.
- Clientsysteme müssen über IP-Konnektivität mit dem Adobe Webserver verfügen, auf dem die Shock-Wave-Datei (SWF) zur Initiierung des Multicast- oder Unicast-Streaming gehostet wird. Falls erforderlich, müssen Sie in Ihrer Firewall die geeigneten Ports öffnen, um Clientgeräten den Zugriff auf diesen Server zu ermöglichen.
- Clientsysteme müssen über Adobe Flash Player 10.1 oder höher für Internet Explorer verfügen (dieser verwendet ActiveX).

Eine Liste der View-Desktop-Anforderungen für die Flash-URL-Umleitung sowie Anweisungen zum Konfigurieren einer Webseite zur Bereitstellung des Multicast- oder Unicast-Streaming finden Sie im Dokument *Installation und Verwaltung von VMware Horizon View Feature Pack*.

Voraussetzungen für die Verwendung von Microsoft Lync mit Horizon View Client

Sie können einen Microsoft Lync 2013-Client auf View-Desktops einsetzen, um an Unified Communications (UC) VoIP (Voice over IP) und Video-Chats mit Lync-zertifizierten USB-Audio- und -Videogeräten teilzunehmen. Ein spezielles IP-Telefon ist nicht länger erforderlich.

Für diese neue Architektur ist die Installation eines Microsoft Lync 2013-Clients auf dem View-Desktop und von einem Microsoft Lync VDI-Plug-In auf dem Clientendpunkt erforderlich. Kunden können den Microsoft Lync 2013-Client für Präsenz, Instant Messaging, Webkonferenz und Microsoft Office-Funktionen verwenden.

Sobald ein Lync VoIP-Anruf oder Video-Chat eintrifft, nimmt das Lync-VDI-Plug-In die gesamte Medienverarbeitung vom Rechenzentrumsserver auf den Clientendpunkt und codiert alle Medien in Lync-optimierten Audio- und Videocodecs. Diese optimierte Architektur ist äußerst skalierbar, was zu einer geringeren Nutzung der Netzwerkbandbreite führt und Unterstützung für qualitativ hochwertige VoIP- und Video-Übertragung von Punkt zu Punkt in Echtzeit bietet. Weitere Informationen finden Sie im Blogeintrag „End-User Computing Blog“ unter http://blogs.vmware.com/euc/2013/06/the-abcs-of-deploying-vmware-horizon-view-5-2-with-microsoft-lync-2013.html.

Hinweis Die Aufnahme von Audio wird noch nicht unterstützt. Diese Integration wird nur mit dem PCoIP-Anzeigeprotokoll unterstützt.

Für diese Funktion gelten die folgenden Anforderungen.

Betriebssystem

- Client-Betriebssystem: 32-Bit- oder 64-Bit-System mit Windows 7 SP1 oder Windows 8

- Betriebssystem der virtuellen Maschine (Agent): 32- oder 64-Bit-Windows 7 SP1

Software des Clientsystems

- Horizon View Client für Windows 5.3 oder später für Windows 7-Clientsysteme, Horizon View Client 5.4 oder später für Windows 8-Clientsysteme oder Horizon View Client für Windows 2.2 oder später.
- 32-Bit-Version des Microsoft Lync VDI-Plug-Ins

  WICHTIG Die 64-Bit-Version von Microsoft Office muss nicht auf dem Clientcomputer installiert werden. Das erforderliche 32-Bit-Microsoft Lync VDI-Plug-In ist nicht mit der 64-Bit-Version von Microsoft Office 2013 kompatibel.

- Das Sicherheitszertifikat, das während der Bereitstellung von Microsoft Lync Server 2013 erzeugt wird, muss in das Verzeichnis der vertrauenswürdigen Stammzertifizierungsstellen importiert werden.

Software für den View-Desktop (Agent)

- Horizon View Agent 5.2 oder später
- Microsoft Lync 2013-Client

  Die Bit-Version des Lync 2013-Clients sollte der Bit-Version des Betriebssystems der virtuellen Maschine entsprechen, wenn Sie einen Horizon View 5.2-Agenten verwenden. Wenn Sie den Horizon View 5.3-Agenten verwenden, muss die Bit-Version des Lync 2013-Clients nicht mit der Bit-Version des Betriebssystems der virtuellen Maschine übereinstimmen.

- Das Sicherheitszertifikat, das während der Bereitstellung von Microsoft Lync Server 2013 erzeugt wird, muss in das Verzeichnis der vertrauenswürdigen Stammzertifizierungsstellen importiert werden

Erforderliche Server

- Ein Server, auf dem View-Verbindungsserver 5.2 oder später ausgeführt wird
- Ein Server, auf dem Microsoft Lync Server 2013 ausgeführt wird
- Eine vSphere-Infrastruktur zur Aufnahme der virtuellen Maschinen

  Auf dem vCenter Server und den ESXi-Hosts muss vSphere 5.0 oder höher ausgeführt werden.

Hardware

- Hardware, die alle der zuvor genannten erforderlichen Softwarekomponenten unterstützt
- Clientendpunkt: 1,5 GHz oder schnellere CPU und mindestens 2 GB RAM für das Microsoft Lync 2013-Plug-In

Anforderungen für die Smartcard-Authentifizierung

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

Für jedes Clientsystem, das zur Benutzerauthentifizierung eine Smartcard verwendet, gelten die folgenden Software- und Hardwareanforderungen:

- Horizon View Client
- Ein Windows-kompatibler Smartcard-Leser

- Smartcard-Middleware
- Produktspezifische Anwendungstreiber

Sie müssen auf den Remote-Desktops zusätzlich produktspezifische Anwendungstreiber installieren.

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

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

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

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

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

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

- Informationen zur Konfiguration von View Servern für die Nutzung von Smartcards finden Sie unter dem Thema „Konfigurieren der Smartcard-Authentifizierung“ im Dokument *Verwaltung von VMware Horizon View*.
- Informationen zu den Aufgaben, die Sie womöglich in Active Directory zur Implementierung der Smartcard-Authentifizierung durchführen müssen, finden Sie in den Hilfethemen zur Vorbereitung von Active Directory für die Smartcard-Authentifizierung im Dokument *Installation von VMware Horizon View*.

Clientbrowseranforderungen für View Portal

Von einem Clientsystem aus können Sie einen Browser öffnen und zu einer bestimmten View-Verbindungsserver-Instanz navigieren. Bei der angezeigten Webseite handelt es sich um ein Portal, das Links zum Herunterladen der Installationsdatei von Horizon View Client enthält.

Um über das Portal ein Horizon View Client-Installationsprogramm herunterzuladen, müssen Sie über einen der folgenden Webbrowser verfügen:

- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10 (von einem Windows 8-System im Desktop-Modus)
- Firefox 6 und höher
- Safari 5 (auf einem Mac)
- Chrome 14 oder höher

Wenn Ihr Administrator VMware Horizon View HTML Access auf dem Server installiert hat, wird unter Umständen auch ein Symbol für die Verbindung mit einem virtuellen Desktop über den Browser angezeigt, ohne dass eine Clientsoftware installiert werden muss. Für diese HTML-Zugriff-Funktion sind neuere Browserversionen erforderlich:

- Chrome 28 oder höher
- Internet Explorer 9 oder höher
- Safari 6 oder höher
- Mobile Safari auf iOS-Geräten mit iOS 6 oder höher
- Firefox 21 oder höher

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 Hilfethemen 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-*.

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 2.0 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 Clientsystems 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 *x.x.x-yyyyyy*, wobei *x.x.x* für die Client-Versionsnummer und *yyyyyy* für die Build-Nummer steht.
Client-Binärarchitektur	No (Nein)	Beispiele hierfür sind: ■ i386 ■ x86_64 ■ arm
Client-Build-Name	No (Nein)	Beispiele hierfür sind: ■ VMware-Horizon-View-Client-Win32-Windows ■ VMware-Horizon-View-Client-Linux ■ VMware-Horizon-View-Client-iOS ■ VMware-Horizon-View-Client-Mac ■ VMware-Horizon-View-Client-Android ■ VMware-Horizon-View-Client-WinStore
Host-Betriebssystem	No (Nein)	Beispiele hierfür sind: ■ Windows 8.1 ■ Windows 7, Service Pack 1 für 64 Bit (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 10.04.4 LTS ■ Mac OS X 10.7.5 (11G63)

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
Host-Betriebssystemkernel	No (Nein)	Beispiele hierfür sind: ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ unbekannt (für Windows Store)
Host-Betriebssystemarchitektur	No (Nein)	Beispiele hierfür sind: ■ x86_64 ■ i386 ■ armv71 ■ ARM
Hostsystem-Modell	No (Nein)	Beispiele hierfür sind: ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Hostsystem-CPU	No (Nein)	Beispiele hierfür sind: ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ unbekannt (für iPad)
Anzahl der Cores bzw. Kerne im Prozessor des Hostsystems	No (Nein)	Beispiel: 4
MB Arbeitsspeicher auf dem Hostsystem	No (Nein)	Beispiele hierfür sind: ■ 4096 ■ unbekannt (für Windows Store)

Installation von View Client für Windows 2

Sie können das Windows-basierte View Client-Installationsprogramm entweder von der VMware-Website oder über View Portal abrufen, einer Seite für den Webzugriff, die von View-Verbindungsserver bereitgestellt wird. Nach der Installation von View Client können Sie verschiedene Startoptionen für die Endbenutzer festlegen.

Dieses Kapitel behandelt die folgenden Themen:

Installieren von View Client für Windows

Endbenutzer öffnen View Client, um von einem Clientsystem aus eine Verbindung mit ihren virtuellen Desktops herzustellen. Sie können eine Windows-basierte Installationsdatei zum Installieren sämtlicher Komponenten von View Client ausführen.

Dieser Vorgang beschreibt die Installation von View Client über einen interaktiven Installationsassistenten. Wenn Sie stattdessen die Befehlszeilenoption bzw. die Option zur unbeaufsichtigten Installation des Microsoft Windows Installer (MSI) verwenden möchten, finden Sie weitere Informationen unter „Unbeaufsichtigte Installation von View Client“, auf Seite 23.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „Systemanforderungen für Windows-Clients“, auf Seite 8.
- 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 21. 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.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.

- Stellen Sie sicher, dass View Agent nicht installiert ist.
- Voraussetzungen für die USB-Umleitung:
  - Bestimmen Sie, ob der Benutzer des Clientgeräts von einem virtuellen Desktop auf lokal verbundene USB-Geräte zugreifen darf. Ist dies nicht der Fall, können Sie entweder die vom Assistenten vorgelegte Komponente **USB-Umleitung** deaktivieren oder die Komponente installieren, sie jedoch unter Verwendung von Gruppenrichtlinienobjekten deaktivieren.

    VMware empfiehlt, die Komponente **USB-Umleitung** immer zu installieren und Gruppenrichtlinienobjekte zur Steuerung des USB-Zugriffs zu verwenden. Auf diese Weise müssen Sie View Client nicht noch einmal neu installieren, wenn Sie die USB-Umleitung für einen Client zu einem späteren Zeitpunkt aktivieren möchten. Weitere Informationen finden Sie unter dem Thema „Einstellungen für die ADM-Vorlage der View Client-Konfiguration“ im Kapitel über die Konfigurationsrichtlinien im Dokument *Verwaltung von VMware Horizon View*.
  - Wenn Sie die Komponente **USB-Umleitung** installieren möchten, stellen Sie sicher, dass die Funktion für automatische Windows-Updates auf dem Clientcomputer nicht deaktiviert wurde.
- Bestimmen Sie, ob die Funktion verwendet werden soll, mit der Endbenutzer sich bei View Client und ihrem virtuellen Desktop als aktuell angemeldeter Benutzer anmelden können. Die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung am Clientsystem eingegeben hat, werden an die View-Verbindungsserver-Instanz und schließlich an den virtuellen Desktop übergeben. Einige Clientbetriebssysteme bieten keine Unterstützung für diese Funktion.
- Wenn Sie nicht möchten, dass die Endbenutzer den vollqualifizierten Domänennamen (FQDN) der View-Verbindungsserverinstanz eingeben müssen, ermitteln Sie den FQDN, um ihn während der Installation angeben zu können.

Vorgehensweise

1 Melden Sie sich als Benutzer mit Administratorberechtigungen am Clientsystem an.

2 Navigieren Sie auf dem Clientsystem zu der URL zum Herunterladen der Installationsdatei.

  Wählen Sie die entsprechende Installationsdatei aus, wobei *xxxxxx* die Build-Nummer und *y.y.y* die Versionsnummer ist.

Option	Aktion
View Client auf 64-Bit-Betriebssystemen	Wählen Sie `VMware-Horizon-View-Client-x86_64-y.y.y-xxxxxx.exe`, wobei *y.y.y* für die Versionsnummer und *xxxxxx* für die Buildnummer steht.
View Client auf 32-Bit-Betriebssystemen	Wählen Sie `VMware-Horizon-View-Client-x86-y.y.y-xxxxxx.exe`, wobei *y.y.y* für die Versionsnummer und *xxxxxx* für die Buildnummer steht.

3 Zum Starten des View Client-Installationsprogramms doppelklicken Sie auf die Installationsdatei.

4 Folgen Sie den Anweisungen zum Installieren der gewünschten Komponenten.

Der VMware View Client-Dienst wird auf dem Windows-Clientcomputer installiert.

Der Prozessname für View Client lautet `vmware-view`. Die Dienste für die USB-Komponenten lauten VMware USB Arbitration-Dienst (`VMUSBArbService`) und VMware View USB (`vmware-view-usbd`).

Weiter

Starten Sie View Client und stellen Sie sicher, dass Sie sich am richtigen virtuellen Desktop anmelden können. Siehe „Anmeldung an einem View-Desktop“, auf Seite 55.

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_7CD50CBABC614BCD976B2575FEDEF1F2">y.y.y-XXXX</varname>.exe#win
   link.win.1=https://<varname id="VARNAME_8243922EA8B44DC3A2E9A360C4DDC304">server-name</varname>/downloads/VMware-Horizon-View-Client-<varname id="VARNAME_9D2A6519E01D4ADA9B701FDB8785B141">y.y.y-XXXX</varname>.exe#win
   link.linux=https://<varname id="VARNAME_C62EA29FFF1047D1A350C57AD8006223">server-name</varname>/downloads/VMware-Horizon-View-Client-x86_64-<varname id="VARNAME_B664011E02154BBD9479411042551944">y.y.y-XXXX</varname>.rpm#linux
   link.linux.1=https://<varname id="VARNAME_C498001B66334F39A59E2610D499EAA8">server-name</varname>/downloads/VMware-Horizon-View-Client-<varname id="VARNAME_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 angegeben Stellen.

Unbeaufsichtigte Installation von View Client

Sie können eine unbeaufsichtigte Installation von View Client durchführen, indem Sie den Namen der Installationsdatei sowie die gewünschten Installationsoptionen an der Befehlszeile eingeben. Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Unbeaufsichtigte Installation von View Client

Sie können die MSI-Funktion (Microsoft Windows Installer) für die unbeaufsichtigte Installation verwenden, um den View Client auf mehreren Windows-Computern zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „Systemanforderungen für Windows-Clients“, auf Seite 8.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Stellen Sie sicher, dass View Agent nicht installiert ist.
- Bestimmen Sie, ob die Funktion verwendet werden soll, mit der Endbenutzer sich bei View Client und ihrem virtuellen Desktop als aktuell angemeldeter Benutzer anmelden können. Die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung am Clientsystem eingegeben hat, werden an die View-Verbindungsserver-Instanz und schließlich an den virtuellen Desktop übergeben. Einige Clientbetriebssysteme bieten keine Unterstützung für diese Funktion.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe „Befehlszeilenoptionen für Microsoft Windows Installer“, auf Seite 25.
- Machen Sie sich mit den verfügbaren MSI-Eigenschaften für die unbeaufsichtigte Installation von View Client vertraut. Siehe „Eigenschaften für die unbeaufsichtigte Installation von View Client“, auf Seite 24.
- Legen Sie fest, ob Sie Endbenutzern von ihren virtuellen Desktops aus den Zugriff auf lokal angeschlossene USB-Geräte gestatten möchten. Falls nicht, legen Sie über die MSI-Eigenschaft `ADDLOCAL` die Liste der relevanten Funktionen fest und lassen Sie die USB-Funktion aus. Weitere Informationen finden Sie unter „Eigenschaften für die unbeaufsichtigte Installation von View Client“, auf Seite 24.
- Wenn Sie nicht möchten, dass die Endbenutzer den vollqualifizierten Domänennamen (FQDN) der View-Verbindungsserverinstanz eingeben müssen, ermitteln Sie den FQDN, um ihn während der Installation angeben zu können.

Vorgehensweise

1 Laden Sie auf dem Clientsystem die View Client-Installationsdatei von der VMware-Produktseite unter http://www.vmware.com/go/viewclients herunter.

Wählen Sie die entsprechende Installationsdatei aus, wobei *xxxxxx* die Build-Nummer und *y.y.y* die Versionsnummer ist.

Option	Aktion
View Client auf 64-Bit-Betriebssystemen	Wählen Sie `VMware-Horizon-View-Client-x86_64-y.y.y-xxxxxx.exe`, wobei *y.y.y* für die Versionsnummer und *xxxxxx* für die Buildnummer steht.
View Client auf 32-Bit-Betriebssystemen	Wählen Sie `VMware-Horizon-View-Client-x86-y.y.y-xxxxxx.exe`, wobei *y.y.y* für die Versionsnummer und *xxxxxx* für die Buildnummer steht.

2 Öffnen Sie auf dem Windows-Clientcomputer eine Eingabeaufforderung.

3 Geben Sie den Installationsbefehl in einer Zeile ein.

In diesem Beispiel wird eine unbeaufsichtigte Installation von View Client durchgeführt: `VMware-Horizon-View-Client-x86-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core"`

Hinweis Die Funktion `Core` ist verbindlich.

Weiter

Starten Sie View Client und stellen Sie sicher, dass Sie sich am richtigen virtuellen Desktop anmelden können. Siehe „Anmeldung an einem View-Desktop“, auf Seite 55.

Eigenschaften für die unbeaufsichtigte Installation von View Client

Sie können spezifische Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation von View Client über die Befehlszeile durchführen. Sie müssen das Format *`EIGENSCHAFT=Wert`* verwenden, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

Im Abschnitt Tabelle 2-1 werden die Eigenschaften für die unbeaufsichtigte Installation von View Client gezeigt, die Sie an der Befehlszeile verwenden können.

Tabelle 2-1. MSI-Eigenschaften für die unbeaufsichtigte Installation von View Client

MSI-Eigenschaft	Beschreibung	Standardwert
INSTALLDIR	Pfad und Verzeichnis für die Installation der View Client-Software. Beispiel: `INSTALLDIR=""D:\abc\mein Ordner""` Die Paare doppelter Anführungszeichen, die den Pfad umschließen, ermöglichen es dem MSI Installer, das Leerzeichen als gültigen Teil des Pfades zu interpretieren. Diese MSI-Eigenschaft ist optional.	`%ProgramFiles%\VMware\VMware Horizon View Client`
VDM_SERVER	Der vollqualifizierte Domänennamen (FQDN) der View-Verbindungsserverinstanz, mit der sich View Client-Benutzer standardmäßig verbinden. Wenn Sie diese Eigenschaft konfigurieren, müssen View Client-Benutzer diesen FQDN nicht angeben. Beispiel: `VDM_SERVER=cs1.companydomain.com` Diese MSI-Eigenschaft ist optional.	Keine

Tabelle 2-1. MSI-Eigenschaften für die unbeaufsichtigte Installation von View Client (Fortsetzung)

MSI-Eigenschaft	Beschreibung	Standardwert
DESKTOP_SHORTCUT	Konfiguriert ein Desktop-Verknüpfungssymbol für View Client. Bei Verwendung des Werts 1 wird die Verknüpfung installiert. Bei Verwendung des Werts 0 wird die Verknüpfung nicht installiert. Diese MSI-Eigenschaft ist optional.	1
STARTMENU_SHORTCUT	Konfiguriert eine Verknüpfung für View Client im Startmenü. Bei Verwendung des Werts 1 wird die Verknüpfung installiert. Bei Verwendung des Werts 0 wird die Verknüpfung nicht installiert. Diese MSI-Eigenschaft ist optional.	1

In einem Befehl für die unbeaufsichtigte Installation können Sie die MSI-Eigenschaft `ADDLOCAL=` zum Festlegen von Funktionen verwenden, die das View Client-Installationsprogramm konfiguriert. Jede Funktion einer unbeaufsichtigten Installation entspricht einer Setupoption, die Sie während einer interaktiven Installation auswählen können.

Im Abschnitt Tabelle 2-2 werden die View Client-Funktionen gezeigt, die Sie an der Befehlszeile eingeben können. Es werden außerdem die zugehörigen Optionen bei einer interaktiven Installation aufgeführt.

Tabelle 2-2. View Client-Funktionen für die unbeaufsichtigte Installation und benutzerdefinierte Setupoptionen für die interaktive Installation

Funktion für die unbeaufsichtigte Installation	Benutzerdefinierte Setupoption in einer interaktiven Installation
Core Wenn Sie mit der MSI-Eigenschaft `ADDLOCAL=` einzelne Funktionen angeben, müssen Sie **`Core`** einschließen.	Keine. Während einer interaktiven Installation werden die View Client-Core-Funktionen standardmäßig installiert.
ThinPrint	Virtuelles Drucken
TSSO	Melden Sie sich als derzeit angemeldeter Windows-Domänenbenutzer an.
USB	USB-Umleitung

Befehlszeilenoptionen für Microsoft Windows Installer

Zur unbeaufsichtigten Installation von View-Komponenten müssen Sie die Befehlszeilenoptionen und Eigenschaften von Microsoft Windows Installer (MSI) verwenden. Die Installationsprogramme für View-Komponenten sind MSI-Programme und verwenden standardmäßige MSI-Funktionen. Sie können auch MSI-Befehlszeilenoptionen zum unbeaufsichtigten Deinstallieren von View-Komponenten verwenden.

Einzelheiten zu MSI finden Sie auf der Website von Microsoft. Informationen zu MSI-Befehlszeilenoptionen finden Sie auf der Website der MSDN-Bibliothek (Microsoft Developer Network), wenn Sie nach MSI-Befehlszeilenoptionen suchen. Informationen zur Verwendung der MSI-Befehlszeile erhalten Sie, indem Sie auf dem Computer mit der View-Komponente eine Eingabeaufforderung öffnen und `msiexec /?` eingeben.

Für die unbeaufsichtigte Installation einer View-Komponente deaktivieren Sie zunächst das Bootstrap-Programm, mit dem das Installationsprogramm in ein temporäres Verzeichnis extrahiert und eine interaktive Installation gestartet wird.

Tabelle 2-3 zeigt die Befehlszeilenoptionen, die das Bootstrap-Programm des Installationsprogramms steuern.

Tabelle 2-3. Befehlszeilenoptionen für das Bootstrap-Programm einer View-Komponente

Option	Beschreibung
`/s`	Deaktiviert den Bootstrap-Splash-Bildschirm und das Dialogfeld für die Extraktion, wodurch die Anzeige interaktiver Dialogfelder unterbunden wird. Beispiel: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s` Die Option `/s` ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen. In den Beispielen steht *xxxxxx* für die Build-Nummer und *y.y.y* für die Versionsnummer.
`/v"MSI-Befehlszeilenoptionen"`	Weist den Installer an, die in doppelten Anführungszeichen eingeschlossene Zeichenfolge, die Sie an der Befehlszeile eingeben, als Befehlssatz zur Interpretation durch MSI zu übergeben. Sie müssen Ihre Befehlszeileneinträge in doppelte Anführungszeichen einschließen. Geben Sie ein doppeltes Anführungszeichen nach `/v` und am Ende der Befehlszeile ein. Beispiel: `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"Befehlszeilenoptionen"` Damit das MSI-Installationsprogramm eine Zeichenfolge mit Leerzeichen richtig auswertet, müssen Sie die Zeichenfolge in zwei Sätze doppelter Anführungszeichen einschließen. Angenommen, Sie möchten die View-Komponente in einem Pfad installieren, dessen Name Leerzeichen enthält. Beispiel: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"Befehlszeilenoptionen INSTALLDIR=""d:\abc\my folder"""` In diesem Beispiel übergibt das MSI-Installationsprogramm den Verzeichnispfad für die Installation und versucht nicht, die Zeichenfolge als Befehlszeilenoptionen auszuwerten. Beachten Sie die zweifach gesetzten doppelten Anführungszeichen, die die gesamte Befehlszeile umschließen. Die Option `/v"Befehlszeilenoptionen"` ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen.

Sie steuern die verbleibenden Schritte einer unbeaufsichtigten Installation, indem Sie Befehlszeilenoptionen und MSI-Eigenschaftenwerte an den MSI Installer, `msiexec.exe`, übergeben. Das MSI-Installationsprogramm umfasst den Installationscode der View-Komponente. Der Installer verwendet die in die Befehlszeile eingegebenen Werte und Optionen, um die Installationsauswahl und die für die View-Komponente spezifischen Setup-Optionen auszuwerten.

Tabelle 2-4 zeigt die Befehlszeilenoptionen und MSI-Eigenschaftenwerte, die an das MSI-Installationsprogramm übergeben werden.

Tabelle 2-4. MSI-Befehlszeilenoptionen und MSI-Eigenschaften

MSI-Option oder -Eigenschaft	Beschreibung
`/qn`	Weist den MSI Installer an, keine Seiten des Installations-Assistenten anzuzeigen. Angenommen, Sie möchten View Agent unbeaufsichtigt installieren und nur standardmäßige Setup-Optionen und Funktionen verwenden: `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"` In den Beispielen steht *xxxxxx* für die Build-Nummer und *y.y.y* für die Versionsnummer. Alternativ können Sie die Option `/qb` zur Anzeige der Assistentenseiten in einer nicht interaktiven, automatisierten Installation verwenden. Während die Installation durchgeführt wird, werden die Assistentenseiten angezeigt, Sie können jedoch keine Eingaben vornehmen. Die Option `/qn` oder `/qb` ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen.
`INSTALLDIR`	(Optional) Gibt einen alternativen Installationspfad für die View-Komponente an. Verwenden Sie das Format *INSTALLDIR=Pfad*, um den Installationspfad anzugeben. Sie können diese MSI-Eigenschaft ignorieren, wenn Sie die View-Komponente im Standardpfad installieren möchten.

Tabelle 2-4. MSI-Befehlszeilenoptionen und MSI-Eigenschaften (Fortsetzung)

MSI-Option oder -Eigenschaft	Beschreibung
ADDLOCAL	(Optional) Legt die komponentenspezifischen Funktionen fest, die installiert werden sollen. In einer interaktiven Installation zeigt das View-Installationsprogramm Auswahloptionen für das benutzerdefinierte Setup an. Mithilfe der MSI-Eigenschaft ADDLOCAL können Sie diese Setup-Optionen an der Befehlszeile angeben. Um alle verfügbaren Optionen für ein benutzerdefiniertes Setup zu installieren, geben Sie ADDLOCAL=ALL ein. Beispiel: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" Wenn Sie die MSI-Eigenschaft ADDLOCAL nicht verwenden, werden die standardmäßigen Setup-Optionen installiert. Zur Festlegung einzelner Setup-Optionen geben Sie eine Liste der Setup-Optionen ein. Trennen Sie hierbei die Namen der Optionen durch Kommata. Verwenden Sie zwischen den Namen keine Leerzeichen. Verwenden Sie das Format *ADDLOCAL=Wert,Wert,Wert...*. Angenommen, Sie möchten View Agent mit den View Composer Agent- und PCoIP-Funktionen in einem Gastbetriebssystem installieren: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP" **Hinweis** Die Funktion Core ist in View Agent erforderlich.
LOGINASCURRENTUSER_DISPLAY	(Optional) Legt fest, ob das Kontrollkästchen **Als aktueller Benutzer anmelden** im Dialogfeld für die Horizon View Client-Verbindung angezeigt wird. Gültige Werte sind 1 (aktiviert) und 0 (deaktiviert). Der Standardwert ist 1, womit das Kontrollkästchen sichtbar ist und die Benutzer dieses Kontrollkästchen aktivieren oder deaktivieren sowie den zugehörigen Standardwert außer Kraft setzen können. Wird das Kontrollkästchen ausgeblendet, können Benutzer den Standardwert im Dialogfeld für die Horizon View Client-Verbindung nicht ändern.
LOGINASCURRENTUSER_DEFAULT	(Optional) Bestimmt den Standardwert des Kontrollkästchens **Als aktueller Benutzer anmelden** im Dialogfeld für die Horizon View Client-Verbindung. Gültige Werte sind 1 (aktiviert) und 0 (deaktiviert). Es ist kein Standardwert festgelegt. Dies bedeutet, dass das Kontrollkästchen deaktiviert ist und die Benutzer Identitäts- und Anmeldeinformationen mehrere Male eingeben müssen, bevor sie auf einen Remote-Desktop zugreifen können. Wenn das Kontrollkästchen **Als aktueller Benutzer anmelden** aktiviert ist, werden die Identität und die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung am Clientsystem verwendet, an die View-Verbindungsserver-Instanz und schließlich an den Remote-Desktop übergeben. Verwenden Sie diese Option in Kombination mit der Option LOGINASCURRENTUSER_DISPLAY. Beispiel: LOGINASCURRENTUSER_DISPLAY=1 LOGINASCURRENTUSER_DEFAULT=1 Wenn ein Benutzer Horizon View Client über die Befehlszeile ausführt und die Option logInAsCurrentUser angibt, wird diese Einstellung durch den eingegebenen Wert überschrieben.

Tabelle 2-4. MSI-Befehlszeilenoptionen und MSI-Eigenschaften (Fortsetzung)

MSI-Option oder -Eigenschaft	Beschreibung
REBOOT	(Optional) Sie können die Option REBOOT=ReallySuppress verwenden, um die Ausführung von Systemkonfigurationsaufgaben zuzulassen, bevor das System neu gestartet wird.
/l*v *Protokolldatei*	(Optional) Schreibt Protokollinformationen in die angegebene Protokolldatei. Beispiel: /l*v ""%TEMP%\vmmsi.log"" In diesem Beispiel wird eine detaillierte Protokolldatei generiert, die dem Protokoll ähnelt, das während einer interaktiven Installation erstellt wird. Sie können diese Option dazu verwenden, benutzerdefinierte Funktionen aufzuzeichnen, die möglicherweise nur für Ihre Installation gelten. Sie können die aufgezeichneten Informationen dazu verwenden, Installationsfunktionen für unbeaufsichtigte Installationen anzugeben.

Beispiel: Installationsbeispiele

In den folgenden Beispielen steht *xxxxxx* für die Build-Nummer, *y.y.y* für die Versionsnummer, *install_folder* für den Pfad zum Installationsordner sowie view.mycompany.com für den Namen einer fiktiven View-Verbindungsserver-Instanz.

Standardinstallationsbeispiel:

```
VMware-Horizon-View-Client-x86_64-<varname id="varname_220C97F047DB49B58E53BC0BAAC63D17">y.y.y-xxxxxx</varname>.exe /s /v"/qn REBOOT=ReallySuppress INSTALLDIR=<varname id="varname_D2BE-ABF323394B30A00F658538C4D2EC">install_folder</varname> ADDLOCAL=ALL DESKTOP_SHORTCUT=1 STARTME-NU_SHORTCUT=1 VDM_SERVER=view.mycompany.com /l*v "%TEMP%\log.txt""
```

Installations- und Konfigurationsbeispiel für die Funktion „Als aktueller Benutzer anmelden“:

```
VMware-Horizon-View-Client-x86_64-<varname id="varname_DE1FCD32D49F4502AAF60F3A7CF4EB02">y.y.y-xxxxxx</varname>.exe /s /v"/qn REBOOT=ReallySuppress INSTALLDIR=<varname id="varna-me_51FF0C65A92A4EA990A78AA4A0FDF435">install_folder</varname> ADDLOCAL=TSSO LOGINASCURRENTU-SER_DISPLAY=1 LOGINASCURRENTUSER_DEFAULT=1 DESKTOP_SHORTCUT=1 STARTMENU_SHORTCUT=1 VDM_SER-VER=view.mycompany.com /l*v "%TEMP%\log.txt""
```

Konfigurieren von Horizon View Client für Endbenutzer

3

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

In der folgenden Tabelle werden einige Konfigurationseinstellungen beschrieben, die Sie auf verschiedene Weise festlegen können. Für viele andere Konfigurationseinstellungen müssen Sie einen ganz bestimmten Mechanismus verwenden. Beispielsweise müssen Sie für die Einstellung „Disable Toast Notifications“ (Toastnachrichten deaktivieren) eine Gruppenrichtlinieneinstellung verwenden.

Tabelle 3-1. Allgemeine Konfigurationseinstellungen

Einstellung	Konfigurationsmechanismen
Adresse des View-Verbindungsservers	URI, Gruppenrichtlinie, Befehlszeile, Windows-Registrierung
Active Directory-Benutzername	URI, Gruppenrichtlinie, Befehlszeile, Windows-Registrierung
Als aktueller Benutzer anmelden	Gruppenrichtlinie, Befehlszeile
Domänenname	URI, Gruppenrichtlinie, Befehlszeile, Windows-Registrierung
Desktopanzeigename	URI, Gruppenrichtlinie, Befehlszeile
Fenstergröße	URI, Gruppenrichtlinie, Befehlszeile
Anzeigeprotokoll	URI, Befehlszeile
Optionen zur Umleitung von USB-Geräten	URI, Gruppenrichtlinie, Befehlszeile
Konfigurieren der Zertifikatsprüfung	Gruppenrichtlinie, Windows-Registrierung
Konfigurieren von SSL-Protokollen und kryptografischen Algorithmen	Gruppenrichtlinie, Windows-Registrierung

Dieses Kapitel behandelt die folgenden Themen:

Verwenden von URIs zur Konfiguration von Horizon View Client

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
- RADIUS- oder RSA SecurID-Benutzername, falls dieser nicht mit dem Active Directory-Benutzernamen identisch ist
- Domänenname
- Desktopanzeigename
- Fenstergröße
- Desktop-Aktionen, darunter „Zurücksetzen“, „Abmelden“ und „Sitzung starten“
- Anzeigeprotokoll
- Optionen zur Umleitung von USB-Geräten

WICHTIG Um diese Funktion nutzen zu können, müssen Sie über Horizon View Client 2.0 oder höher verfügen.

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.

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 Clientbetriebssysteme 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-address</varname>:<varname id="VARNAME_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</varname>=<varname id="VARNAME_9B9916FF3D3540D4AA5622F9C828F072">value1</varname>[&<varname id="VARNAME_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 3-2. 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.
`start-session`	Startet den angegebenen Desktop. Wenn keine „action“-Abfrage bereitgestellt wird und der Desktopname angegeben wird, ist `start-session` die Standardaktion.
`zurücksetzen`	Fährt 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.

connectUSBOnInsert

Verbindet ein USB-Gerät beim Anschließen des Geräts mit dem im Vordergrund angezeigten Desktop. 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 **`yes`** und **`no`**. Ein Beispiel für die Syntax ist etwa **`connectUSBOnInsert=yes`**.

connectUSBOnStartup

Leitet alle aktuell mit dem Clientsystem 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 **`yes`** und **`no`**. Ein Beispiel für die Syntax ist etwa **`connectUSBOnStartup=yes`**.

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 3-3. Gültige Werte für desktopLayout-Abfrage

Wert	Beschreibung
`fullscreen`	Vollbild auf einem Monitor. Hierbei handelt es sich um die Standardeinstellung.
`multimonitor`	Vollbild auf allen Monitoren.
`windowLarge`	Großes Fenster.
`windowSmall`	Kleines Fenster.
*W*x*H*	Benutzerdefinierte Auflösung, bei der Sie die Breite mal Höhe in Pixel angeben. Ein Beispiel für die Syntax ist etwa **`desktopLayout=1280x800`**.

desktopProtocol

Gültige Werte sind **`RDP`** und **`PCoIP`**. Zur Angabe von PCoIP verwenden Sie beispielsweise die Syntax **`desktopProtocol=PCoIP`**.

domainName	Die Domäne, die mit dem Benutzer verknüpft ist, der eine Verbindung zum Remote-Desktop herstellt.
tokenUserName	Gibt den RSA- oder RADIUS-Benutzernamen an. Verwenden Sie diese Abfrage nur, wenn der RSA- oder RADIUS-Benutzername nicht mit dem Active Directory-Benutzernamen identisch ist. Wenn Sie diese Abfrage nicht angeben und die RSA- oder RADIUS-Authentifizierung erforderlich ist, wird der Windows-Benutzername verwendet. Die Syntax lautet `tokenUserName=`***`name`***.
unattended	Erstellt eine Serververbindung im Kioskmodus. Geben Sie keine Benutzerinformationen an, wenn Sie diese Abfrage verwenden.

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

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

8 `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>
```

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 „Zertifikatsprüfungsmodi für Horizon View Client“, auf Seite 35.

Verwenden Sie die ADM-Vorlagendatei zur Client-Konfiguration, um den Überprüfungsmodus einzustellen. Die ADM-Vorlagendatei (`vdm_client.adm`) für die VMware Horizon View Client-Konfiguration ist im Verzeichnis *`Installationsverzeichnis`*`\VMware\VMware Horizon View Client\extras\` auf dem Clientsystem installiert. Das *`Installationsverzeichnis`* lautet standardmäßig `C:\Programme (x86)`. Informationen zum Festlegen der GPO-Einstellungen mithilfe dieser Vorlage finden Sie unter „Konfigurieren von VMware Horizon View Client für Windows mithilfe der Gruppenrichtlinienvorlage“, auf Seite 37.

Hinweis Mit der ADM-Vorlagendatei für die Client-Konfiguration können Sie auch die Verwendung bestimmter kryptografischer Algorithmen und Protokolle beschränken, bevor Sie eine verschlüsselte SSL-Verbindung herstellen. Weitere Informationen zu dieser Einstellung finden Sie unter „Sicherheitseinstellungen für Client-GPOs“, auf Seite 38.

Wenn Sie die Einstellung für die Zertifikatüberprüfung nicht als Gruppenrichtlinie konfigurieren möchten, können Sie die Zertifikatüberprüfung auch durch Hinzufügen des Wertnamens `CertCheckMode` zu einem der folgenden Registrierungsschlüssel auf dem Clientcomputer aktivieren:

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

Verwenden Sie die folgenden Werte im Registrierungsschlüssel:

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

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

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:

- Wurde das Zertifikat widerrufen?
- Ist das Zertifikat für einen anderen Zweck bestimmt als für die Überprüfung der Identität des Absenders und die Verschlüsselung der Serverkommunikation? Mit anderen Worten: Handelt es sich um den korrekten Zertifikattyp?
- Ist das Zertifikat abgelaufen oder erst zukünftig gültig? Mit anderen Worten: Ist das Zertifikat laut Computeruhr gültig?
- Stimmt der allgemeine Name auf dem Zertifikat mit dem Hostnamen des Servers überein, der es sendet? Zu einer fehlenden Übereinstimmung kann es kommen, wenn ein Lastenausgleich Horizon 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 unbekannten oder nicht als vertrauenswürdig eingestuften Zertifizierungsstelle (CA) signiert worden? Selbstsignierte Zertifikate sind ein Typ der nicht als vertrauenswürdig eingestuften CA.

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

Hinweis Anweisungen zur Verteilung eines selbstsignierten Stammzertifikats an alle Windows-Clientsysteme in einer Domäne finden Sie unter dem Thema „Stammzertifikat zu den vertrauenswürdigen Zertifizierungsstellen hinzufügen“ im Dokument *Installation von VMware Horizon View-*.

Wenn Ihr Administrator Ihnen die Verwendung von Horizon View Client bei der Anmeldung an einem Desktop ermöglicht hat, können Sie auf **SSL konfigurieren** klicken und den Zertifikatsprüfungsmodus einstellen. 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.

  Möglicherweise erhalten Sie auch eine Warnung, wenn das Zertifikat abgelaufen ist.
- **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.

Wichtig In früheren Versionen konfigurierten Sie die Clientsysteme Ihres Unternehmens so, dass sie über GPO ein bestimmtes Verschlüsselungsverfahren verwendeten, indem Sie als Gruppenrichtlinieneinstellung die Reihenfolge der SSL-Verschlüsselungssammlungen konfigurierten. Nun müssen Sie dafür eine Gruppenrichtlinien-Sicherheitseinstellung von Horizon View Client 2.3 verwenden, die in der ADM-Vorlagendatei für Horizon View enthalten ist. Siehe „Sicherheitseinstellungen für Client-GPOs“, auf Seite 38. Alternativ können Sie auch die Registrierungseinstellung `SSLCipherList` auf dem Client verwenden. Siehe „Konfigurieren des Horizon View Client mithilfe der Windows-Registrierung“, auf Seite 52.

Konfigurieren von VMware Horizon View Client für Windows mithilfe der Gruppenrichtlinienvorlage

VMware Horizon View Client enthält eine Gruppenrichtlinien-Verwaltungsvorlage (ADM-Datei) zum Konfigurieren von VMware Horizon View Client. Sie können Remote-Desktop-Verbindungen optimieren und schützen, indem Sie die Richtlinieneinstellungen in dieser ADM-Vorlagendatei zu einem neuen oder vorhandenen Gruppenrichtlinienobjekt (Group Policy Object, GPO) in Active Directory hinzufügen.

Die Horizon View-ADM-Vorlagendateien enthalten sowohl Gruppenrichtlinien für die Computerkonfiguration als auch Gruppenrichtlinien für die Benutzerkonfiguration.

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

Horizon View wendet Richtlinien beim Start eines Desktops und bei der Benutzeranmeldung an.

Die ADM-Vorlagendatei (`vdm_client.adm`) für die Horizon View Client-Konfiguration wird im Verzeichnis *`Installationsverzeichnis`*`\VMware\VMware Horizon View Client\extras\` auf dem Clientsystem installiert. Das *`Installationsverzeichnis`* lautet standardmäßig `C:\Programme (x86)` auf einem 64-Bit-System bzw. `C:\Programme` bei einem 32-Bit-System. Sie müssen diese Datei auf Ihren Active Directory-Server kopieren und diese Verwaltungsvorlage mithilfe des Gruppenrichtlinienverwaltungs-Editors hinzufügen. Anweisungen hierzu finden Sie unter dem Thema „Hinzufügen von View-ADM-Vorlagen zu einem GPO“ im Dokument *Verwaltung von VMware Horizon View Client*.

Einstellungen für die Skriptdefinition für Client-GPOs

Sie können Richtlinien für viele der Einstellungen festlegen, die beim Ausführen von VMware Horizon View Client über die Befehlszeile verwendet werden, wie beispielsweise die Desktop-Größe, den Namen oder den Domänennamen.

In der folgenden Tabelle werden die in der ADM-Vorlagendatei für die VMware Horizon View Client-Konfiguration enthaltenen Einstellungen für die Skriptdefinition beschrieben. Die Vorlage stellt für jede Skriptdefinition eine Version für die Computerkonfiguration und eine Version für die Benutzerkonfiguration bereit. Die Einstellung für die Benutzerkonfiguration setzt hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

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

Einstellung	Beschreibung
`Automatically connect if only one launch item is entitled`	(Horizon View Client 2.3 oder höher) Stellt automatisch eine Verbindung zum Desktop her, wenn der Benutzer nur Anspruch auf einen Desktop hat. Dem Benutzer wird dadurch die Auswahl des Desktops aus einer Liste mit nur einem Desktop erspart.
`Connect all USB devices to the desktop on launch`	Legt fest, ob alle der verfügbaren USB-Geräte auf dem Clientsystem mit dem Desktop verbunden werden, wenn dieser gestartet wird.
`Connect all USB devices to the desktop when they are plugged in`	Legt fest, ob USB-Geräte mit dem Desktop verbunden werden, wenn die Geräte an das Clientsystem angeschlossen werden.

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

Einstellung	Beschreibung
`DesktopLayout`	Legt das Layout des VMware Horizon View Client-Fensters fest, das einem Benutzer bei der Anmeldung an einem Remote-Desktop angezeigt wird. Es stehen folgende Optionen zur Auswahl: ■ `Vollbild` ■ `Mehrere Monitore` ■ `Fenster – groß` ■ `Fenster – klein` Diese Einstellung ist nur verfügbar, wenn die Einstellung `DesktopName to select` ebenfalls gesetzt ist.
`DesktopName to select`	Legt den von VMware Horizon View Client während der Anmeldung verwendeten Standard-Desktop fest.
`Disable 3rd-party Terminal Services plugins`	Legt fest, ob Terminaldienste-Plug-Ins von Drittanbietern, die als normale RDP-Plug-Ins installiert sind, von VMware Horizon View Client überprüft werden. Wenn Sie diese Einstellung nicht konfigurieren, überprüft VMware Horizon View Client standardmäßig Plug-Ins von Drittanbietern. Diese Einstellung hat keine Auswirkung auf Horizon View-spezifische Plug-Ins, wie beispielsweise die USB-Umleitung.
`Logon DomainName`	Legt die von Horizon View Client während der Anmeldung verwendete NetBIOS-Domäne fest.
`Logon Password`	Legt das von Horizon View Client während der Anmeldung verwendete Kennwort fest. Das Kennwort wird von Active Directory im Textformat gespeichert.
`Logon UserName`	Legt den von Horizon View Client während der Anmeldung verwendeten Benutzernamen fest.
`Server URL`	Legt die von Horizon View Client während der Anmeldung verwendete URL fest, z. B. `https://view1.beispiel.com`.
`Suppress error messages (nur bei Skriptverwendung)`	Legt fest, ob Horizon View Client Fehlermeldungen während der Anmeldung unterdrückt. Diese Einstellung ist nur anwendbar, wenn der Anmeldevorgang vollständig per Skript ausgeführt wird, z.B. wenn alle erforderlichen Anmeldeinformationen über eine Richtlinie vorausgefüllt werden. Wenn die Anmeldung aufgrund von falschen Anmeldeinformationen fehlschlägt, wird der Benutzer hierüber nicht benachrichtigt, und der Horizon View Client-Prozess wird beendet.

Sicherheitseinstellungen für Client-GPOs

Zu den Sicherheitseinstellungen zählen Optionen für das Sicherheitszertifikat, für Anmeldeinformationen und für die Single Sign-On-Funktion (SSO).

In der folgenden Tabelle werden die in der ADM-Vorlagendatei für die Horizon View Client-Konfiguration enthaltenen Sicherheitseinstellungen beschrieben. Diese Tabelle zeigt, ob die Einstellungen die Einstellungen „Computer Configuration (Computerkonfiguration)“ und User Configuration (Benutzerkonfiguration)“ enthalten oder nur die Einstellung „Computer Configuration (Computerkonfiguration)“. Bei den Sicherheitseinstellungen, die beide Typen einschließen, setzt die Einstellung für die Benutzerkonfiguration hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

Tabelle 3-5. Horizon View Client -Konfigurationsvorlage: Sicherheitseinstellungen

Einstellung	Beschreibung
`Allow command line credentials` (Einstellung für die Computerkonfiguration)	Legt fest, ob Benutzeranmeldeinformationen mit Horizon View Client-Befehlszeilenoptionen bereitgestellt werden können. Wenn diese Einstellung aktiviert ist, stehen die Optionen `smartCardPIN` und `password` nicht zur Verfügung, wenn Benutzer Horizon View Client über die Befehlszeile ausführen. Diese Einstellung ist standardmäßig aktiviert.
`Servers Trusted For Delegation (Vertrauenswürdige Server für die Delegierung)` (Einstellung für die Computerkonfiguration)	Gibt die View-Verbindungsserver-Instanzen an, welche die Benutzeridentitäts- und Anmeldeinformationen akzeptieren, die bei Aktivierung des Kontrollkästchens **Log in as current user (Anmelden als aktueller Benutzer)** übergeben werden. Wenn Sie keine View-Verbindungsserver-Instanzen angeben, akzeptieren alle View-Verbindungsserver-Instanzen diese Informationen. Verwenden Sie zum Hinzufügen einer View-Verbindungsserver-Instanz eines der folgenden Formate: ■ **`domain\system$`** ■ **`system$@domain.com`** ■ Service Principal Name (SPN) des View-Verbindungsserver-Dienstes

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

Einstellung	Beschreibung
`Certificate verification mode (Zertifikatüberprüfungsmodus)` (Einstellung für die Computerkonfiguration)	Konfiguriert die Ebene der Zertifikatsprüfung, die durch Horizon View Client durchgeführt wird. Es stehen folgende Modi zur Auswahl: ■ `No Security (Keine Sicherheit)`. Horizon View führt keine Zertifikatsprüfung durch. ■ `Warn But Allow (Warnen, aber zulassen)`. Wenn die folgenden Serverzertifikatprobleme auftreten, wird eine Warnung angezeigt, aber der Benutzer kann mit der Verbindungsherstellung mit View-Verbindungsserver fortfahren: ■ Von Horizon View wird ein selbstsigniertes Zertifikat bereitgestellt. In diesem Fall ist es akzeptabel, wenn der Zertifikatname nicht mit dem Namen des View-Verbindungsservers übereinstimmt, der in Horizon View Client vom Benutzer angegeben wurde. ■ Ein überprüfbares Zertifikat, das in Ihrer Bereitstellung konfiguriert wurde, ist abgelaufen oder noch nicht gültig. Wenn andere Zertifikatfehlerbedingungen vorliegen, zeigt Horizon View ein Fehlerdialogfeld an und verhindert, dass der Benutzer eine Verbindung zum View-Verbindungsserver herstellt. `Warn But Allow (Warnen, aber zulassen)` ist der Standardwert. ■ `Full Security (Volle Sicherheit)`. Wenn ein beliebiger Zertifikatfehler auftritt, kann der Benutzer keine Verbindung mit View-Verbindungsserver herstellen. Horizon View zeigt dem Benutzer die Zertifikatfehler an. Wenn diese Gruppenrichtlinieneinstellung konfiguriert ist, können die Benutzer den ausgewählten Modus für die Zertifikatsprüfung in Horizon View Client sehen, ihn aber nicht konfigurieren. Das Dialogfeld für die SSL-Konfiguration informiert die Benutzer darüber, dass der Administrator die Einstellung gesperrt hat. Wenn diese Einstellung nicht konfiguriert oder deaktiviert wurde, können Horizon View Client-Benutzer einen Zertifikatsprüfungsmodus auswählen. Damit ein Horizon View Server die von Horizon View Client bereitgestellten Zertifikate prüfen kann, muss der Client HTTPS-Verbindungen zum View-Verbindungsserver- oder Sicherheitsserver-Host herstellen. Die Zertifikatsüberprüfung wird nicht unterstützt, wenn Sie SSL auf ein Zwischengerät verlagern, welches HTTP-Verbindungen zum View-Verbindungsserver- oder Sicherheitsserver-Host herstellt. Wenn Sie diese Einstellung bei Windows-Clients nicht als Gruppenrichtlinie konfigurieren möchten, können Sie die Zertifikatüberprüfung auch durch Hinzufügen des Wertnamens `CertCheckMode` zu folgenden Registrierungsschlüsseln auf dem Clientcomputer aktivieren: ■ 32-Bit-Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security` ■ 64-Bit-Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security` Verwenden Sie die folgenden Werte im Registrierungsschlüssel: ■ **`0`** implementiert `No Security (Keine Sicherheit)`. ■ **`1`** implementiert `Warn But Allow (Warnen, aber zulassen)`. ■ **`2`** implementiert `Full Security (Volle Sicherheit)`. Wenn Sie sowohl die Gruppenrichtlinieneinstellung als auch die Einstellung `CertCheckMode` im Registrierungsschlüssel konfigurieren, hat die Gruppenrichtlinieneinstellung Vorrang vor der Registrierungsschlüsseleinstellung.

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

Einstellung	Beschreibung
`Default value of the 'Log in as current user' checkbox` (Einstellung für die Computer- und Benutzerkonfiguration)	Gibt den Standardwert des Kontrollkästchens **Als aktueller Benutzer anmelden** im Dialogfeld für die Horizon View Client-Verbindung an. Diese Einstellung setzt den Standardwert außer Kraft, der während der Horizon View Client-Installation angegeben wurde. Wenn ein Benutzer Horizon View Client über die Befehlszeile ausführt und die Option `logInAsCurrentUser` angibt, wird diese Einstellung durch den eingegebenen Wert überschrieben. Wenn das Kontrollkästchen **Als aktueller Benutzer anmelden** aktiviert ist, werden die Identität und die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung am Clientsystem verwendet, an die View-Verbindungsserver-Instanz und schließlich an den Remote-Desktop übergeben. Ist das Kontrollkästchen deaktiviert, müssen Benutzer Identitäts- und Anmeldeinformationen mehrere Male eingeben, bevor sie auf einen Remote-Desktop zugreifen können. Diese Einstellung ist standardmäßig deaktiviert.
`Display option to Log in as current user` (Einstellung für die Computer- und Benutzerkonfiguration)	Legt fest, ob das Kontrollkästchen **Als aktueller Benutzer anmelden** im Dialogfeld für die Horizon View Client-Verbindung angezeigt wird. Bei Anzeige des Kontrollkästchens können Benutzer die Option aktivieren oder deaktivieren oder den zugehörigen Standardwert außer Kraft setzen. Wird das Kontrollkästchen ausgeblendet, können Benutzer den Standardwert im Dialogfeld für die Horizon View Client-Verbindung nicht ändern. Sie können den Standardwert für **Log in as current user (Anmelden als aktueller Benutzer)** über die Richtlinieneinstellung `Default value of the 'Log in as current user' checkbox (Standardwert des Kontrollkästchens 'Anmelden als aktueller Benutzer')` festlegen. Diese Einstellung ist standardmäßig aktiviert.
`Enable jump list integration` (Einstellung für die Computerkonfiguration)	Legt fest, ob eine Sprungliste im Horizon View Client-Symbol in der Taskleiste von Windows 7 oder höheren Systemen angezeigt werden soll. Über die Sprungliste können Benutzer eine Verbindung zu zuletzt verwendeten View-Verbindungsserver-Instanzen und Remote-Desktops herstellen. Wenn Horizon View Client gemeinsam verwendet wird, sollen Benutzer möglicherweise nicht die Namen der zuletzt verwendeten Desktops sehen. Die Sprungliste können Sie deaktivieren, indem Sie diese Einstellung deaktivieren. Diese Einstellung ist standardmäßig aktiviert.
`Enable SSL encrypted framework channel (SSL-verschlüsselten Framework-Kanal aktivieren)` (Einstellung für die Computer- und Benutzerkonfiguration)	Legt fest, ob SSL für Horizon View 5.0 und ältere Desktops aktiviert wird. Vor Horizon View 5.0 wurden die über den Port TCP 32111 an den Desktop gesendeten Daten nicht verschlüsselt. ■ **Enable**: Aktiviert SSL, aber ermöglicht das Zurücksetzen auf die vorherige unverschlüsselte Verbindung, falls der Remote-Desktop SSL nicht unterstützt. Beispielsweise wird SSL von Horizon View 5.0 und älteren Desktops nicht unterstützt. **Enable** ist die Standardeinstellung. ■ **Disable**: Deaktiviert SSL. Diese Einstellung wird nicht empfohlen. Sie kann aber hilfreich sein für das Debugging oder wenn der Kanal nicht getunnelt wird und deshalb möglicherweise durch ein Produkt zur WAN-Beschleunigung optimiert werden könnte. ■ **Enforce**: Aktiviert SSL und verweigert das Herstellen einer Verbindung zu Desktops ohne SSL-Unterstützung.

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

Einstellung	Beschreibung
`Configures SSL protocols and cryptographic algorithms` (Einstellung für die Computer- und Benutzerkonfiguration)	Konfiguriert die Verschlüsselungsliste, um die Verwendung bestimmter kryptografischer Algorithmen und Protokolle zu beschränken, bevor Sie eine verschlüsselte SSL-Verbindung herstellen. Die Verschlüsselungsliste besteht aus einer oder mehreren Verschlüsselungszeichenfolgen, die durch Doppelpunkte voneinander getrennt werden. **Hinweis** Für alle Verschlüsselungszeichenfolgen wird die Groß-/Kleinschreibung berücksichtigt. Wenn diese Funktion aktiviert ist, lautet der Standardwert **SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH**. Dies bedeutet, dass SSL v3.0, TLS v1.0 und TLS v1.1 aktiviert sind. (SSL v2.0 und TLS v1.2 sind deaktiviert.) Verschlüsselungssammlungen verwenden 128- oder 256-Bit-AES, entfernen anonyme DH-Algorithmen und sortieren anschließend die aktuelle Verschlüsselungsliste nach der Schlüssellänge des Verschlüsselungsalgorithmus. Referenz-Link für die Konfiguration: http://www.openssl.org/docs/apps/ciphers.html
`Enable Single Sign-On for smart card authentication` (Einstellung für die Computerkonfiguration)	Legt fest, ob für die Smartcard-Authentifizierung das Single Sign-On (SSO) aktiviert ist. Ist SSO aktiviert, speichert Horizon View Client die verschlüsselte Smartcard-PIN im temporären Arbeitsspeicher, bevor sie an den View-Verbindungsserver gesendet wird. Ist SSO deaktiviert, zeigt Horizon View Client kein benutzerdefiniertes PIN-Dialogfeld an.
`Ignore bad SSL certificate date received from the server` (Einstellung für die Computerkonfiguration)	(Nur View 4.6 und frühere Versionen) Legt fest, ob Fehler in Zusammenhang mit ungültigen Datumswerten für das Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn ein Server ein abgelaufenes Zertifikat sendet.
`Ignore certificate revocation problems` (Einstellung für die Computerkonfiguration)	(Nur View 4.6 und frühere Versionen) Legt fest, ob Fehler in Zusammenhang mit einem gesperrten Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn der Server ein Zertifikat sendet, das gesperrt wurde, und der Client den Sperrstatus eines Zertifikats nicht überprüfen kann. Diese Einstellung ist standardmäßig deaktiviert.
`Ignore incorrect SSL certificate common name (host name field)` (Einstellung für die Computerkonfiguration)	(Nur View 4.6 und frühere Versionen) Legt fest, ob Fehler in Zusammenhang mit falschen allgemeinen Namen im Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn der allgemeine Name des Zertifikats nicht mit dem Hostnamen des Servers übereinstimmt, der das Zertifikat sendet.
`Ignore incorrect usage problems` (Einstellung für die Computerkonfiguration)	(Nur View 4.6 und frühere Versionen) Legt fest, ob Fehler in Zusammenhang mit einer falschen Verwendung des Serverzertifikats ignoriert werden. Diese Fehler treten auf, wenn das vom Server gesendete Zertifikat für einen anderen Zweck als die Überprüfung der Absenderidentität und zum Verschlüsseln der Serverkommunikation gedacht ist.
`Ignore unknown certificate authority problems` (Einstellung für die Computerkonfiguration)	(Nur View 4.6 und frühere Versionen) Legt fest, ob bestimmte Fehler in Zusammenhang mit einer unbekannten Zertifizierungsstelle im Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn das vom Server gesendete Zertifikat durch eine nicht vertrauenswürdige Drittanbieter-Zertifizierungsstelle signiert wurde.

RDP-Einstellungen für Client-GPOs

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

In der folgenden Tabelle werden die in der ADM-Vorlagendatei für die Horizon View Client-Konfiguration enthaltenen RDP-Einstellungen (Remote Desktop Protocol) beschrieben. Alle RDP-Einstellungen sind Einstellungen für die Benutzerkonfiguration.

Tabelle 3-6. ADM-Vorlage für Horizon View Client -Konfiguration: RDP-Einstellungen

Einstellung	Beschreibung
`Audio redirection`	Legt fest, ob auf dem Remote-Desktop wiedergegebene Audioinformationen umgeleitet werden. Es stehen folgende Einstellungen zur Auswahl: ■ **Disable Audio**: Die Audiowiedergabe ist deaktiviert. ■ **Play VM (erforderlich für VoIP USB-Unterstützung)**: Audiodaten werden im Remote-Desktop wiedergegeben. Diese Einstellung erfordert ein gemeinsam genutztes USB-Audiogerät zur Wiedergabe von Sound auf dem Client. ■ **Redirect to client**: Audiodaten werden an den Client umgeleitet. Dies ist der Standardmodus. Diese Eigenschaft gilt nur für RDP-Audio. Über MMR umgeleitete Audiodaten werden im Client wiedergegeben.
`Audio capture redirection`	Legt fest, ob das standardmäßige Audioeingabegerät vom Client an die Remote-Sitzung umgeleitet wird. Wenn diese Einstellung aktiviert ist, wird das Audioaufzeichnungsgerät des Clients im Remote-Desktop angezeigt und kann zur Aufzeichnung von Audioeingabedaten verwendet werden. Diese Einstellung ist standardmäßig deaktiviert.
`Bitmap cache file size in` *unit* `for` *number* `bpp bitmaps`	Gibt die Größe des Bitmapcaches (in KB oder MB) für die Zwischenspeicherung von Bitmaps mit einer bestimmten Farbeinstellung (Bits pro Pixel, bpp) an. Für die verschiedenen Kombinationen aus Einheit und Bits pro Pixel stehen unterschiedliche Versionen zur Verfügung: ■ KB/8bpp ■ MB/8bpp ■ MB/16bpp ■ MB/24bpp ■ MB/32bpp
`Bitmap caching/cache persistence active (Bitmap-Cache/Dauerhafte Zwischenspeicherung aktiv)`	Legt fest, ob für Bitmaps eine dauerhafte Zwischenspeicherung durchgeführt wird (aktiv ist). Eine dauerhafte Zwischenspeicherung für Bitmaps kann die Leistung verbessern, erfordert jedoch zusätzlichen Speicherplatz.
`Color Depth`	Legt die Farbtiefe für den Remote-Desktop fest. Es stehen folgende Einstellungen zur Auswahl: ■ 8 Bit ■ 15 Bit ■ 16 Bit ■ 24 Bit ■ 32 Bit Für Windows XP-Systeme mit 24 Bit müssen Sie die Richtlinie `Limit Maximum Color Depth` in **Computer Configuration > Administrative Templates > Windows Components > Terminal Services** aktivieren und auf 24 Bit festlegen.
`Cursor shadow`	Legt fest, ob auf dem Remote-Desktop unter dem Cursor ein Schatten angezeigt wird.
`Desktop Background`	Legt fest, ob der Desktop-Hintergrund angezeigt wird, wenn Clients eine Verbindung zu einem Remote-Desktop herstellen.
`Desktop composition`	(Windows Vista oder höher) Legt fest, ob die Desktop-Gestaltung auf dem Remote-Desktop aktiviert ist. Wenn die Desktop-Gestaltung aktiviert ist, werden einzelne Fenster nicht länger direkt auf dem Bildschirm oder dem primären Anzeigegerät dargestellt, wie dies in früheren Versionen von Microsoft Windows der Fall war. Stattdessen werden die Bilddaten zunächst in den nicht sichtbaren Offscreen-Bereich des Videospeichers umgeleitet und anschließend zur Darstellung auf dem Anzeigegerät in ein Desktop-Bild gerendert.
`Enable compression`	Legt fest, ob RDP-Daten komprimiert werden. Diese Einstellung ist standardmäßig aktiviert.

Tabelle 3-6. ADM-Vorlage für Horizon View Client -Konfiguration: RDP-Einstellungen (Fortsetzung)

Einstellung	Beschreibung
`Enable Credential Security Service Provider`	Gibt an, ob die Remote-Desktop-Verbindung die Authentifizierung auf Netzwerkebene (Network Level Authentication, NLA) verwendet. In Windows Vista erfordern Remote-Desktop-Verbindungen standardmäßig NLA. Wenn das Gastbetriebssystem für Remote-Desktop-Verbindungen NLA erfordert, müssen Sie diese Einstellung aktivieren. Andernfalls kann Horizon View Client keine Verbindung zum Desktop herstellen. Zusätzlich zur Aktivierung dieser Einstellung müssen Sie sicherstellen, dass die folgenden Bedingungen erfüllt sind: ■ Sowohl das Client- als auch das Gastbetriebssystem unterstützen NLA. ■ Für die View-Verbindungsserver-Instanz sind direkte Clientverbindungen aktiviert. Tunnelverbindungen werden mit NLA nicht unterstützt.
`Enable RDP Auto-Reconnect`	Legt fest, ob die RDP-Clientkomponente versucht, erneut eine Verbindung mit einem Remote-Desktop herzustellen, nachdem ein RDP-Verbindungsfehler aufgetreten ist. Diese Einstellung hat keine Auswirkung, wenn die Option **Use secure tunnel connection to desktop (Sichere Tunnelverbindung zum Desktop verwenden)** in View Administrator aktiviert wurde. Diese Einstellung ist standardmäßig deaktiviert. **Hinweis** Die automatische erneute RDP-Verbindung wird für Desktops mit View Agent 4.5 oder einer höheren Version unterstützt. Wenn ein Desktop eine frühere Version von View Agent verwendet, können einige Funktionen nicht verwendet werden.
`Font smoothing`	(Windows Vista oder höher) Legt fest, ob Anti-Aliasing auf die Schriftarten auf dem Remote-Desktop angewendet wird.
`Menu and window animation`	Legt fest, ob die Animation für Menüs und Fenster aktiviert ist, wenn Clients eine Verbindung zu einem Remote-Desktop herstellen.
`Redirect clipboard`	Legt fest, ob die Informationen in der lokalen Zwischenablage umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen.
`Redirect drives`	Legt fest, ob lokale Festplattenlaufwerke umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen. Lokale Laufwerke werden standardmäßig umgeleitet. Durch Aktivieren oder Nichtkonfigurieren dieser Einstellung können Daten auf dem umgeleiteten Laufwerk des Remote-Desktops auf das Laufwerk des Clientcomputers kopiert werden. Deaktivieren Sie diese Einstellung, wenn das Übertragen von Daten vom Remote-Desktop zu den Clientcomputern des Benutzers ein mögliches Sicherheitsrisiko für Ihre Bereitstellung darstellt. Alternativ können Sie auch die Ordnerumleitung in der virtuellen Maschine des Remote-Desktops deaktivieren, indem Sie die Microsoft Windows-Gruppenrichtlinieneinstellung `Do not allow drive redirection (Laufwerkumleitung nicht zulassen)` aktivieren. Die Einstellung `Redirect drives (Laufwerke umleiten)` wirkt sich nur auf RDP aus.
`Redirect printers`	Legt fest, ob lokale Drucker umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen.
`Redirect serial ports`	Legt fest, ob lokale COM-Ports umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen.
`Redirect smart cards`	Legt fest, ob lokale Smartcards umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen. **Hinweis** Diese Einstellung gilt sowohl für RDP- als auch für PCoIP-Verbindungen.
`Redirect supported plug-and-play devices`	Legt fest, ob lokale Plug & Play- sowie POS-Geräte (Point of Sale) umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen. Dieses Verhalten unterscheidet sich dahingehend von der Umleitung, dass es durch die Horizon View Agent-Komponente für die USB-Umleitung verwaltet wird.
`Shadow bitmaps`	Legt fest, ob Schattenbitmaps verwendet werden. Diese Einstellung hat im Vollbildmodus keine Auswirkung.

Tabelle 3-6. ADM-Vorlage für Horizon View Client -Konfiguration: RDP-Einstellungen (Fortsetzung)

Einstellung	Beschreibung
`Show contents of window while dragging`	Legt fest, ob Ordnerinhalte angezeigt werden, wenn der Benutzer einen Ordner an einen neuen Speicherort zieht.
`Themes`	Legt fest, ob Designs angezeigt werden, wenn Clients eine Verbindung zu einem Remote-Desktop herstellen.
`Windows key combination redirection`	Legt fest, wo Windows-Tastenkombinationen angewendet werden. Mit dieser Einstellung können Sie Tastenkombinationen an die virtuelle Remote-Maschine senden oder lokal Tastenkombinationen anwenden. Wenn diese Einstellung nicht konfiguriert ist, werden Tastenkombinationen lokal angewandt.

Allgemeine Einstellungen für Client-GPOs

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

Allgemeine Einstellungen

In der folgenden Tabelle werden die in der ADM-Vorlagendatei für die Horizon View Client-Konfiguration enthaltenen allgemeinen Einstellungen beschrieben. Zu den allgemeinen Einstellungen gehören sowohl Einstellungen für die Computerkonfiguration als auch Einstellungen für die Benutzerkonfiguration. Die Einstellung für die Benutzerkonfiguration setzt hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

Tabelle 3-7. Horizon View Client -Konfigurationsvorlage: Allgemeine Einstellungen

Einstellung	Beschreibung
`Always on top` (Einstellung für die Benutzerkonfiguration)	Legt fest, ob das Horizon View Client-Fenster immer im Vordergrund angezeigt wird. Durch Aktivierung dieser Einstellung wird verhindert, dass die Windows-Taskleiste ein Horizon View Client-Fenster im Vollbildmodus überlappt. Diese Einstellung ist standardmäßig aktiviert.
`Determines if the VMware View Client should use proxy.pac file` (Einstellung für die Computerkonfiguration)	(Nur View 4.6 und frühere Versionen) Legt fest, ob Horizon View Client eine PAC-Datei (Proxy Automatic Configuration) verwendet. Wenn diese Einstellung aktiviert ist, verwendet Horizon View Client eine PAC-Datei. Eine PAC-Datei (häufig als `proxy.pac` bezeichnet) hilft Webbrowsern und anderen Agenten, den geeigneten Proxy-Server für eine bestimmte URL oder Website-Anforderung zu finden. Wenn Sie diese Einstellung auf einer Maschine mit mehreren Kernen aktivieren, stürzt möglicherweise die WinINet-Anwendung ab, die Horizon View Client für die Suche nach Proxy-Server-Informationen verwendet. Deaktivieren Sie diese Einstellung, wenn dieses Problem auf Ihrer Maschine auftritt. Diese Einstellung ist standardmäßig deaktiviert. **Hinweis** Diese Einstellung gilt nur für direkte Verbindungen. Auf Tunnelverbindungen hat die Einstellung keine Auswirkung.
`Disable Time Zone Forwarding` (Einstellung für die Computerkonfiguration)	Legt fest, ob die Zeitzonensynchronisierung des Remote-Desktops mit der des verbundenen Clients deaktiviert ist.
`Disable toast notifications (Toastnachrichten deaktivieren)` (Einstellung für die Computer- und Benutzerkonfiguration)	Hierdurch wird festgelegt, ob Toastnachrichten von Horizon View Client deaktiviert werden sollen. Aktivieren Sie diese Einstellung, wenn Sie nicht möchten, dass dem Benutzer Toastnachrichten in der Ecke des Bildschirms angezeigt werden. **Hinweis** Wenn Sie diese Einstellung aktivieren, wird dem Benutzer bei Aktivierung der Funktion „Sitzungszeitüberschreitung“ keine 5-Minuten-Warnung eingeblendet.

Tabelle 3-7. Horizon View Client -Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Beschreibung
`Don't check monitor alignment on spanning` (Einstellung für die Benutzerkonfiguration)	Standardmäßig wird der Client-Desktop nicht in den Mehrfachmonitor-Modus geschaltet, wenn die Bildschirme in Kombination kein exaktes Rechteck bilden (d.h. identische Höhe bei horizontaler Anordnung oder identische Breite bei vertikaler Anordnung). Aktivieren Sie diese Einstellung, um den Standardwert außer Kraft zu setzen. Diese Einstellung ist standardmäßig deaktiviert.
`Enable multi-media acceleration` (Einstellung für die Benutzerkonfiguration)	Legt fest, ob die Multimedia-Umleitung (Multimedia Redirection, MMR) auf dem Client aktiviert ist. MMR arbeitet nicht ordnungsgemäß, wenn die Horizon View Client-Hardware zur Videoanzeige keine Overlay-Unterstützung bietet.
`Relative Maus aktivieren` (Einstellung für die Computer- und Benutzerkonfiguration)	(Nur Horizon View 5.2 und höhere Versionen) Aktiviert die relative Maus bei Verwendung des PCoIP-Anzeigeprotokolls. Der Modus für relative Maus optimiert das Mausverhalten für bestimmte Grafikanwendungen und Spiele. Falls der Modus für relative Maus nicht vom Remote-Desktop unterstützt wird, wird diese Einstellung nicht verwendet. Diese Einstellung ist standardmäßig deaktiviert.
`Enable the shade` (Einstellung für die Benutzerkonfiguration)	Legt fest, ob die Schatten-Menüleiste im oberen Bereich des Horizon View Client-Fensters sichtbar ist. Diese Einstellung ist standardmäßig aktiviert. **Hinweis** Die Schatten-Menüleiste im oberen Bereich ist für den Kiosk-Modus standardmäßig deaktiviert.
`Tunnel proxy bypass address list` (Einstellung für die Computerkonfiguration)	Gibt eine Liste von Tunneladressen an. Der Proxy-Server wird für diese Adressen nicht verwendet. Verwenden Sie ein Semikolon (;) zum Trennen mehrerer Einträge.
`URL for View Client online help` (Einstellung für die Computerkonfiguration)	Gibt eine alternative URL an, von der Horizon View Client Hilfeseiten abrufen kann. Diese Einstellung ist zur Verwendung in Umgebungen gedacht, die das remote verwaltete Hilfesystem nicht abrufen können, da kein Internetzugriff verfügbar ist.
`Pin the Shade` (Einstellung für die Benutzerkonfiguration)	Legt fest, ob die Fixierung der Menüleiste im oberen Bereich des Horizon View Client-Fensters aktiviert ist, sodass die Menüleiste nicht automatisch ausgeblendet wird. Diese Einstellung hat keine Auswirkung, wenn die Menüleiste deaktiviert wurde. Diese Einstellung ist standardmäßig aktiviert.
`Meldungen zum Trennen von Desktops deaktivieren` (Einstellung für die Computer- und Benutzerkonfiguration)	Legt fest, ob Meldungen, die normalerweise beim Trennen von Desktops angezeigt werden, deaktiviert werden sollen. Diese Meldungen werden standardmäßig angezeigt.

USB-Einstellungen für Client-GPOs

Sie können USB-Richtlinieneinstellungen sowohl für Horizon View Agent als auch für Horizon View Client für Windows definieren. Nach dem Herstellen der Verbindung lädt Horizon View Client die USB-Richtlinieneinstellungen von Horizon View Agent herunter und verwendet diese zusammen mit den Horizon View Client-USB-Richtlinieneinstellungen, um zu entscheiden, welche Geräte vom Hostcomputer umgeleitet werden dürfen.

In der folgenden Tabelle werden die Richtlinieneinstellungen zum Splitten von USB-Verbundgeräten in der ADM-Vorlagendatei für die Horizon View Client-Konfiguration beschrieben. Die Einstellungen gelten auf Computerebene. Horizon View Client liest die Einstellungen vorzugsweise aus dem GPO auf der Computerebene, andernfalls aus der Registrierung unter `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`. Eine Beschreibung, wie Horizon View die Richtlinien zum Splitten von USB-Verbundgeräten anwendet, finden Sie in den Themen über die Verwendung von Richtlinien zur Steuerung der USB-Umleitung im Dokument *Verwaltung von VMware Horizon View*-.

Tabelle 3-8. Horizon View Client -Konfigurationsvorlage: USB-Splittingeinstellungen

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

In der folgenden Tabelle werden die Richtlinieneinstellungen zum Filtern von USB-Verbundgeräten in der ADM-Vorlagendatei für die Horizon View Client-Konfiguration beschrieben. Die Einstellungen gelten auf Computerebene. Horizon View Client liest die Einstellungen vorzugsweise aus dem GPO auf der Computerebene, andernfalls aus der Registrierung unter `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`. Eine Beschreibung, wie Horizon View die Richtlinien zum Filtern von USB-Geräten anwendet, finden Sie in den Themen über die Konfiguration von Filterrichtlinieneinstellungen für die USB-Umleitung im Dokument *Verwaltung von VMware Horizon View-*.

Tabelle 3-9. Horizon View Client -Konfigurationsvorlage: USB-Filtereinstellungen

Einstellung	Eigenschaften
`Allow Audio Input Devices (Audioeingabegeräte zulassen)`	Lässt zu, dass Audioeingabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist.
`Allow Audio Output Devices (Audioausgabegeräte zulassen)`	Lässt zu, dass Audioausgabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
`Allow HIDBootable (HIDBootable zulassen)`	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 **`true`** ist.
`Verhalten auch dann zulassen, wenn Gerätebeschreibungen nicht abgerufen werden können`	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 **`false`** ist.
`Andere Eingabegeräte zulassen`	Lässt zu, dass Eingabegeräte außer HID-startfähigen Geräten oder Tastaturen mit integrierten Zeigegeräten umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist.

Tabelle 3-9. Horizon View Client -Konfigurationsvorlage: USB-Filtereinstellungen (Fortsetzung)

Einstellung	Eigenschaften
`Allow Keyboard and Mouse Devices (Tastatur- und Mausgeräte zulassen)`	Lässt zu, dass Tastaturen mit eingebauten Zeigegeräten (Maus, Trackball oder Touchpad) umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
`Allow Smart Cards (SmartCards zulassen)`	Lässt zu, dass SmartCard-Geräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
`Allow Video Devices (Videogeräte zulassen)`	Lässt zu, dass Videogeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist.
`Remote-Konfiguration deaktivieren`	Deaktiviert die Verwendung der View Agent-Einstellungen beim Durchführen der USB-Gerätefilterung. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
`Exclude All Devices (Alle Geräte ausschließen)`	Schließt alle USB-Geräte von der Umleitung aus. Wenn für diese Einstellung **`true`** festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zuzulassen, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn für diese Einstellung **`false`** festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zu verhindern, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn Sie den Wert von `Exclude All Devices` in View Agent auf **`true`** 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 **`false`** ist.
`Exclude Device Family (Gerätefamilie ausschließen)`	Schließt Gerätefamilien von der Umleitung aus. Das Format der Einstellung ist *Familienname_1*`[;`*Familienname_2*`]`... Beispiel: **`bluetooth;smart-card`** Wenn Sie das automatische Gerätesplitten aktiviert haben, prüft Horizon View die Gerätefamilie jeder Schnittstelle eines USB-Verbundgeräts, um zu entscheiden, welche Schnittstellen ausgeschlossen werden sollten. Wenn Sie das automatische Gerätesplitten deaktiviert haben, prüft Horizon View die Gerätefamilie des gesamten USB-Verbundgeräts. Der Standardwert ist nicht definiert.
`Exclude Vid/Pid Device (Vid/Pid-Gerät ausschließen)`	Schließt Geräte mit einer angegebenen Anbieter- oder Produkt-ID von der Umleitung aus. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]`... Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (**`*`**) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid-0781_pid-****;vid-0561_pid-554c`** Der Standardwert ist nicht definiert.
`Exclude Path (Pfad ausschließen)`	Schließt Geräte an angegebenen Hub- oder Portpfaden von der Umleitung aus. Das Format der Einstellung ist `bus-`*x1*`[/`*y1*`]`.../`port-`*z1*`[;bus-`*x2*`[/`*y2*`]`.../`port-`*z2*`]`... Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden. Beispiel: **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** Der Standardwert ist nicht definiert.
`Include Device Family (Gerätefamilie einschließen)`	Bestimmt Gerätefamilien, die umgeleitet werden können. Das Format der Einstellung ist *Familienname_1*`[;`*Familienname_2*`]`... Beispiel: **`Speicher`** Der Standardwert ist nicht definiert.

Tabelle 3-9. Horizon View Client -Konfigurationsvorlage: USB-Filtereinstellungen (Fortsetzung)

Einstellung	Eigenschaften
`Include Path (Pfad einschließen)`	Schließt Geräte an angegebenen Hub- oder Portpfaden in die Umleitung ein. Das Format der Einstellung ist `bus-`*x1*`[/`*y1*`].../port-`*z1*`[;bus-`*x2*`[/`*y2*`]...port-`*z2*`]...` Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden. Beispiel: **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** Der Standardwert ist nicht definiert.
`Include Vid/Pid Device (Vid/Pid-Gerät einschließen)`	Bestimmt Geräte mit einer angegebenen Anbieter- und Produkt-ID, die umgeleitet werden können. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (`*`) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid-0561_pid-554c`** Der Standardwert ist nicht definiert.

Ausführen von View Client aus der Befehlszeile

Sie können View Client für Windows von der Befehlszeile aus oder über Skripts ausführen. Dies kann erwünscht sein, wenn Sie eine kioskbasierte Anwendung implementieren, die Endbenutzern Zugriff auf Desktop-Anwendungen gewährt.

Sie verwenden den Befehl `vmware-view.exe`, um View Client für Windows von der Befehlszeile auszuführen. Der Befehl umfasst Optionen, die Sie angeben können, um das Verhalten von View Client zu ändern.

Verwenden von Horizon View Client -Befehlen

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

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

```
<cmdname id="CMDNAME_6B817C59FA9D4EA7BC789DC30C022258">vmware-view</cmdname> [<varname id="VARNA-
ME_DE8697255C5D4E68B4ED9BA9BF3DAE0D">command_line_option</varname> [<varname id="VARNA-
ME_8BE22B262785472C982FBF41DCA364E7">argument</varname>]] ...
```

Der Standardpfad zur ausführbaren Datei des Befehls `vmware-view` ist vom System abhängig.

- Auf 32-Bit-Systemen lautet der Pfad `C:\Programme\VMware\VMware Horizon View Client\`.
- Auf 64-Bit-Systemen lautet der Pfad `C:\Programme (x86)\VMware\VMware Horizon View Client\`.

Zur Vereinfachung fügen Sie diesen Pfad zu Ihrer Umgebungsvariable *PATH* hinzu.

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

Tabelle 3-10. Horizon View Client -Befehlszeilenoptionen

Option	Beschreibung
`/?`	Zeigt die Liste der Befehlsoptionen an.
`-connectUSBOnStartup`	Wenn hier `true` angegeben ist, werden alle gegenwärtig mit dem Host verbundenen USB-Geräte an den Desktop umgeleitet. Diese Option wird bei Angabe der Option `-unattended` implizit festgelegt. Die Standardeinstellung ist `false`.
`-connectUSBOnInsert`	Wenn hier `true` angegeben ist, wird ein USB-Gerät mit dem Desktop im Vordergrund verbunden, wenn Sie das Gerät anschließen. Diese Option wird bei Angabe der Option `-unattended` implizit festgelegt. Die Standardeinstellung ist `false`.

Tabelle 3-10. Horizon View Client -Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung
`–desktopLayout` *Fenstergröße*	Gibt an, wie das Desktop-Fenster angezeigt wird: **`fullscreen`** Anzeige im Vollbildmodus **`multimonitor`** Anzeige auf mehreren Monitoren **`windowLarge`** Großes Fenster **`windowSmall`** Kleines Fenster
`–desktopName` *Desktop-Name*	Gibt den Namen des Desktops an, der im Dialogfeld zur Desktop-Auswahl angezeigt wird. Dies ist der Anzeigename des Desktops im Dialogfeld zur Desktop-Auswahl.
`–desktopProtocol` *Protokoll*	Gibt den Namen des zu verwendenden Protokolls an, der im Dialogfeld zur Desktop-Auswahl angezeigt wird. Das Protokoll kann PCOIP oder RDP sein.
`–domainName` *Domänenname*	Gibt die Domäne an, die der Endbenutzer zur Anmeldung an Horizon View Client verwendet.
`–file` *Dateipfad*	Gibt den Pfad einer Konfigurationsdatei mit zusätzlichen Befehlsoptionen und -argumenten an. Siehe „View Client-Konfigurationsdatei“, auf Seite 51.
`–h`	Zeigt Hilfeoptionen an.
`–languageId` *Gebietsschema-ID*	Bietet Lokalisierungsunterstützung für verschiedene Sprachen in Horizon View Client. Wenn eine Ressourcenbibliothek verfügbar ist, geben Sie die zu verwendende Gebietsschema-ID (Locale ID, LCID) an. Für Englisch (USA) geben Sie 0x409 ein.
`–logInAsCurrentUser`	Wenn hier `true` angegeben ist, werden die Anmeldeinformationen des Endbenutzers, die dieser zur Anmeldung am Clientsystem eingegeben hat, an die View-Verbindungsserver-Instanz und schließlich an den View-Desktop übergeben. Die Standardeinstellung ist `false`.
`–nonInteractive`	Unterdrückt Fehlermeldungen beim Starten von Horizon View Client über ein Skript. Diese Option wird bei Angabe der Option `–unattended` implizit festgelegt.
`–noVMwareAddins`	Verhindert das Laden von VMware-spezifischen virtuellen Kanälen, wie z. B. für den virtuellen Druck.
`–password` *Kennwort*	Gibt das Kennwort an, das der Endbenutzer zur Anmeldung an Horizon View Client verwendet. Diese Option muss für Clients im Kiosk-Modus nicht angegeben werden, wenn das Kennwort automatisch generiert wird.
`–printEnvironmentInfo`	Zeigt die IP-Adresse, die MAC-Adresse und den Maschinennamen des Clientgeräts an.
`–serverURL` *Verbindungsserver*	Gibt die URL, die IP-Adresse oder den FQDN der View-Verbindungsserver-Instanz an.
`–SingleAutoConnect`	(Horizon View Client 2.3 oder höher) Wenn ein Benutzer nur Anspruch auf einen Remote-Desktop hat, wird mit dieser Einstellung nach der Authentifizierung des Benutzers beim Server automatisch eine Verbindung mit dem Desktop hergestellt und der Benutzer wird angemeldet. Dem Benutzer wird dadurch die Auswahl des Desktops aus einer Liste mit nur einem Desktop erspart.
`–smartCardPIN` *PIN*	Gibt die PIN an, wenn ein Endbenutzer eine Smartcard zur Anmeldung einführt.

Tabelle 3-10. Horizon View Client -Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung
`–standalone`	Unterstützt zur Bereitstellung von Abwärtskompatibilität. Dies ist das Standardverhalten für diesen Client. Die Angabe von `–standalone` ist nicht erforderlich. Startet eine zweite Instanz von Horizon View Client, die eine Verbindung mit demselben oder einem anderen View-Verbindungsserver herstellen kann. Für mehrere Desktopverbindungen zum selben oder einem anderen Server wird keine sichere Tunnelverbindung unterstützt. **Hinweis** Die zweite Desktopverbindung hat möglicherweise keinen Zugriff auf die lokale Hardware, wie USB-Geräte, Smartcards, Drucker und mehrere Monitore.
`–unattended`	Führt Horizon View Client im nicht interaktiven Modus aus, der sich für Clients im Kiosk-Modus eignet. Zusätzlich müssen folgende Informationen angegeben werden: ■ Der Kontoname des Clients, wenn dieser nicht über die MAC-Adresse des Clientgeräts generiert wurde. Der Name muss mit der Zeichenfolge „custom-“ oder einem alternativen Präfix beginnen, das Sie in ADAM konfiguriert haben. ■ Das Kennwort des Clients, wenn dieses nicht automatisch beim Einrichten des Clientkontos generiert wurde. Über die Option `–unattended` werden implizit die Optionen `–nonInteractive`, `–connectUSBOnStartup`, `–connectUSBOnInsert` und `–desktopLayout multimonitor` festgelegt.
`–userName` *Benutzername*	Gibt den Kontonamen an, den der Endbenutzer zur Anmeldung an Horizon View Client verwendet. Diese Option muss für Clients im Kiosk-Modus nicht angegeben werden, wenn der Kontoname über die MAC-Adresse des Clientgeräts generiert wird.

Über die Befehlszeile oder in der Konfigurationsdatei angegebene Optionen haben Vorrang vor globalen Systemrichtlinien, die wiederum Benutzerrichtlinien außer Kraft setzen.

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

View Client-Konfigurationsdatei

Sie können Befehlszeileninformationen für View Client aus einer Konfigurationsdatei auslesen.

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

Beispiel: Beispiel einer Konfigurationsdatei für eine nicht interaktive Anwendung

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

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

Beispiel: Beispiel einer Konfigurationsdatei für einen Client im Kioskmodus

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

```
–serverURL 145.124.24.100
–unattended
```

Konfigurieren des Horizon View Client mithilfe der Windows-Registrierung

Sie können Standardeinstellungen für den Horizon View Client in der Windows-Registrierung definieren, anstatt diese Einstellungen über die Befehlszeile anzugeben. Richtlinieneinträge haben Priorität vor den Windows-Registrierungseinstellungen, und Befehlszeileneinstellungen haben Priorität vor Richtlinieneinträgen.

Tabelle 3-11 zeigt die Registrierungseinstellungen für die Anmeldung bei Horizon View Client. Diese Einstellungen befinden sich in der Registrierung unter „HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client\“. Dieser Speicherort ist spezifisch für einen bestimmten Benutzer, wohingegen die Einstellungen „HKEY_LOCAL_MACHINE“, die in der nächsten Tabelle beschrieben werden, computerweite Einstellungen sind, die für alle lokalen Benutzer und alle Domänenbenutzer in einer Windows-Domänenumgebung gelten, die über die Berechtigung verfügen, sich am Computer anzumelden.

Tabelle 3-11. Horizon View Client Registrierungseinstellungen für Anmeldeinformationen

Registrierungs-einstellung	Beschreibung
Kennwort	Bestimmt das Standardkennwort.
UserName	Bestimmt den standardmäßigen Benutzernamen.

Tabelle 3-12 zeigt die Registrierungseinstellungen für Horizon View Client, die nicht die Anmeldeinformationen beinhalten. Der Speicherort dieser Einstellungen hängt vom Systemtyp ab:

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

Tabelle 3-12. Horizon View Client -Registrierungseinstellungen

Registrierungs-einstellung	Beschreibung
DomainName	Bestimmt den standardmäßigen Domänennamen.
EnableShade	Bestimmt, ob die Menüleiste (Shade) am oberen Rand des Horizon View Client-Fensters aktiviert ist. Die Menüleiste ist standardmäßig aktiviert, mit Ausnahme bei Clients im Kioskmodus. Mit dem Wert „false“ wird die Menüleiste deaktiviert.
ServerURL	Bestimmt die standardmäßige View-Verbindungsserverinstanz anhand der URL, IP-Adresse oder des FQDN.

In der folgenden Tabelle werden Sicherheitseinstellungen beschrieben, die Sie hinzufügen können. Der Speicherort dieser Einstellungen hängt vom Systemtyp ab:

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

Tabelle 3-13. Sicherheitseinstellungen

Registrierungseinstellung	Beschreibung und gültige Werte
`CertCheckMode`	Legt den Zertifikatsprüfungsmodus fest. ■ **`0`** implementiert `Server-Identitätszertifikate nicht überprüfen`. ■ **`1`** implementiert `Warnung vor Verbindung mit nicht vertrauenswürdigen Servern ausgeben`. ■ **`2`** implementiert `Nie mit nicht vertrauenswürdigen Servern verbinden`.
`SSLCipherList`	Konfiguriert die Verschlüsselungsliste, um die Verwendung bestimmter kryptografischer Algorithmen und Protokolle zu beschränken, bevor Sie eine verschlüsselte SSL-Verbindung herstellen. Die Verschlüsselungsliste besteht aus einer oder mehreren Verschlüsselungszeichenfolgen, die durch Doppelpunkte voneinander getrennt werden. **HINWEIS** Für alle Verschlüsselungszeichenfolgen wird die Groß-/Kleinschreibung berücksichtigt. Wenn diese Funktion aktiviert ist, lautet der Standardwert **SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH**. Dies bedeutet, dass SSL v3.0, TLS v1.0 und TLS v1.1 aktiviert sind. (SSL v2.0 und TLS v1.2 sind deaktiviert.) Verschlüsselungssammlungen verwenden 128- oder 256-Bit-AES, entfernen anonyme DH-Algorithmen und sortieren anschließend die aktuelle Verschlüsselungsliste nach der Schlüssellänge des Verschlüsselungsalgorithmus. Referenz-Link für die Konfiguration: http://www.openssl.org/docs/apps/ciphers.html

Verwaltung der Serververbindungen und Desktops 4

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 zugewiesen 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:

Anmeldung an einem View-Desktop

Bevor Sie den Endbenutzern Zugriff auf ihre virtuellen Desktops gewähren, sollten Sie sicherstellen, dass Sie sich von einem Clientgerät aus an einem virtuellen Desktop anmelden können. Sie können View Client über das Menü **Start** oder eine Desktop-Verknüpfung auf dem Clientsystem starten.

In Umgebungen, in denen eine Netzwerkverbindung verfügbar ist, wird die Benutzersitzung von View-Verbindungsserver authentifiziert.

Voraussetzungen

- Besorgen Sie sich die zur Anmeldung benötigten Informationen, so etwa den Benutzernamen und das Kennwort, den RSA SecurID-Benutzernamen und das Kennwort, den RADIUS-Authentifizierungsbenutzernamen oder -Passcode oder die Smartcard-PIN.
- Besorgen Sie sich den Domänennamen für die Anmeldung.
- Führen Sie die unter „Vorbereiten des View-Verbindungsservers für Horizon View Client“, auf Seite 15 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-Verbindungsserver vorgelegte SSL-Zertifikat konfigurieren.

  Informationen zur Bestimmung des zu verwendenden Modus finden Sie unter „Zertifikatsprüfungsmodi für Horizon View Client“, auf Seite 35.

Vorgehensweise

1 Doppelklicken Sie auf die Desktop-Verknüpfung **VMware Horizon View Client** oder klicken Sie auf **Start > Programme > VMware > VMware Horizon View Client**.

2 (Optional) Zur Festlegung des Zertifikatsprüfungsmodus klicken Sie auf die Schaltfläche **Optionen** in der oberen linken Ecke des Fensters und wählen Sie **SSL konfigurieren**.

  Wie in den Voraussetzungen für dieses Verfahren beschrieben, können Sie diese Option nur dann konfigurieren, wenn Ihr Administrator dies gestattet.

3 (Optional) Um sich als derzeit angemeldeter Windows-Domänenbenutzer anzumelden, klicken Sie in der oberen linken Ecke des Fensters auf die Schaltfläche **Optionen** und wählen Sie **Anmelden als aktueller Benutzer**.

  Diese Option steht zur Verfügung, wenn das Modul **Anmelden als aktueller Benutzer** auf Ihrem Clientsystem installiert ist und wenn der Administrator die globale Einstellung für diese Funktion aktiviert hat. Einige Unternehmen entschließen sich, die Funktion nicht zu aktivieren.

4 Klicken Sie auf die Schaltfläche **+ Server hinzufügen**, geben Sie den Namen des View-Verbindungsservers oder eines Sicherheitsservers ein, und klicken Sie auf **Verbinden**.

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

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

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 die Anmeldeinformationen eines Benutzers ein, der für die Verwendung von mindestens einem Desktop-Pool berechtigt ist, wählen Sie die Domäne aus und klicken Sie auf **Anmelden**.

  Wenn Sie den Benutzernamen mit dem Format **`Benutzer@Domaene`** eingeben, wird er aufgrund des At-Zeichens (@) als Benutzerprinzipalname (User Principal Name, UPN) behandelt, und das Dropdown-Menü für die Domäne wird abgeblendet dargestellt.

  Informationen zur Erstellung von Desktop-Pools und zum Zuweisen von Benutzerberechtigungen für Pools finden Sie im Dokument *Verwaltung von VMware Horizon View*-.

7 (Optional) Zum Konfigurieren von Anzeigeeinstellungen klicken Sie entweder mit der rechten Maustaste auf ein Desktop-Symbol oder Sie wählen ein Desktop-Symbol aus und klicken auf die Schaltfläche **Einstellungen** in der oberen rechten Bildschirmecke.

Option	Beschreibung
Anzeigeprotokoll	Wenn Ihr Administrator dies gestattet, können Sie anhand der Liste **Verbinden über** zwischen den Anzeigeprotokollen PCoIP und Microsoft RDP auswählen. PCoIP bietet ein optimiertes PC-Benutzererlebnis bei der Bereitstellung von Bildern sowie Audio- und Videoinhalten im LAN oder WAN.
Anzeigelayout	Verwenden Sie die Liste **Anzeige**, um eine Fenstergröße auszuwählen oder mehrere Monitore zu verwenden.

8 Doppelklicken Sie auf ein Remote-Desktop-Symbol, um die Verbindung herzustellen.

Nachdem die Verbindung hergestellt wurde, wird das View-Desktopfenster angezeigt. Wenn Sie aus mehreren Desktop-Symbolen auswählen konnten, bleibt das Fenster zur Desktop-Auswahl geöffnet, sodass Sie sich mit mehreren Desktops gleichzeitig verbinden können.

Wenn keine Authentifizierung gegenüber View-Verbindungsserver möglich ist oder View Client keine Verbindung mit einem Desktop herstellen kann, führen Sie die folgenden Aufgaben aus:

- Legen Sie fest, ob der View-Verbindungsserver dahingehend konfiguriert werden soll, SSL nicht zu verwenden. 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 den View-Verbindungsserver sicher. Wenn dies nicht zutrifft, wird in View Administrator möglicherweise angezeigt, dass View Agent in Desktops nicht erreichbar ist, und über den Übertragungsserver-Status wird angezeigt, dass die Komponente nicht bereit ist. Dies sind Hinweise auf zusätzliche Verbindungsprobleme, die durch Zertifikatprobleme verursacht werden.
- 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 View-Desktop verwenden, müssen Sie bestätigen, dass der Clientcomputer Remote-Desktop-Verbindungen zulässt.

Weiter

Konfigurieren Sie Startoptionen. Wenn Sie nicht möchten, dass Endbenutzer den Hostnamen von View-Verbindungsserver eingeben müssen, oder wenn Sie andere Startoptionen konfigurieren möchten, verwenden Sie die View Client-Befehlszeilenoptionen, um eine Desktop-Verknüpfung zu erstellen. Siehe „Ausführen von View Client aus der Befehlszeile“, auf Seite 49.

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
Einen Remote-Desktop auf demselben Server auswählen	Führen Sie einen der folgenden Schritte aus: ■ Wählen Sie in der Horizon View Client-Menüleiste **Optionen > Zu einem anderen Desktop wechseln** und wählen Sie den Desktop aus, der angezeigt werden soll. ■ Doppelklicken Sie im Fenster für die Desktop-Auswahl auf das Symbol für einen anderen Desktop-Pool. Der Desktop wird in einem neuen Fenster geöffnet, sodass mehrere Desktops geöffnet sind und Sie zwischen diesen wechseln können.
Einen Remote-Desktop auf einem anderen Server auswählen	Wenn Sie zur Verwendung mehrerer Desktops berechtigt sind und deshalb das Fenster zur Desktop-Auswahl geöffnet ist, wechseln Sie zum Fenster für die Desktop-Auswahl, klicken Sie auf **Optionen** in der oberen linken Ecke des Fensters und wählen Sie **Verbindung trennen**. Sie werden vom aktuellen Server und allen offenen Desktop-Sitzungen abgemeldet. Sie können anschließend eine Verbindung mit einem anderen Server herstellen. Wenn Sie nur zur Verwendung eines Desktops berechtigt sind, wird das Fenster zur Desktop-Auswahl nicht geöffnet. Sie müssen Horizon View Client beenden und neu starten, um eine Verbindung mit einem anderen Server herzustellen.

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 in den meisten Fällen auch die Tastenkombination Strg+Alt+Einfg betätigen. Wenn Sie auf Windows 8.1-Desktops das Microsoft RDP-Anzeigeprotokoll verwenden, kann diese Tastenkombination nicht verwendet werden.

Vorgehensweise

- Trennen Sie die Verbindung, ohne sich abzumelden.

Option	Aktion
Vom Remote-Desktop-Fenster aus	Führen Sie einen der folgenden Schritte aus: ■ Klicken Sie auf die Schaltfläche **Schließen** in der Ecke des Desktop-Fensters. ■ Wählen Sie in der Menüleiste des Desktop-Fensters **Optionen > Verbindung trennen** aus.
Im Fenster zur Desktop-Auswahl	Das Fenster zur Desktop-Auswahl ist geöffnet, wenn Sie über Berechtigungen für mehrere Desktops auf dem Server verfügen. Führen Sie einen der folgenden Schritte aus: ■ Klicken Sie auf die Schaltfläche **Schließen** in der Ecke des Fensters zur Desktop-Auswahl, und klicken Sie im Warnungsfenster auf **Ja**. ■ Klicken Sie auf das Optionssymbol in der oberen linken Ecke des Fensters zur Desktop-Auswahl, wählen Sie **Verbindung trennen** und klicken Sie im Warnungsfenster auf **Ja**.

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
Aus dem Desktop-Betriebssystem heraus	Melden Sie sich über das Windows-**Start**-Menü ab.
Über die Menüleiste	Wählen Sie **Optionen > Trennen und Abmelden**. 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.

  a Starten Sie Horizon View Client, stellen Sie eine Verbindung mit der View-Verbindungsserver-Instanz her, die Zugriff auf den Remote-Desktop bietet, und geben Sie Ihre Anmeldeinformationen für die Authentifizierung an.

  b Klicken Sie mit der rechten Maustaste auf das Desktop-Symbol und wählen Sie **Abmelden**.

Arbeiten auf einem View-Desktop 5

Horizon View bietet die vertraute, individuell angepasste Desktop-Umgebung, die Benutzer erwarten. Benutzer können auf an ihren lokalen Computer angeschlossene USB- und andere Geräte zugreifen, Dokumente an beliebige Drucker senden, die von ihrem lokalen Computer erkannt werden, eine Authentifizierung mithilfe von Smartcards durchführen und mehrere Anzeigemonitore verwenden.

Dieses Kapitel behandelt die folgenden Themen:

Funktionsunterstützungs-Matrix

Viele Funktionen, so zum Beispiel die RSA SecurID-Authentifizierung, das standortbasierte Drucken und das PCoIP-Protokoll, werden auf den meisten Clientbetriebssystemen unterstützt. Dabei muss jedoch auch berücksichtigt werden, ob die Funktion auf dem Betriebssystem des View-Desktops unterstützt wird.

Verwenden Sie bei der Planung und Bereitstellung des Anzeigeprotokolls und der Funktionen, die für Ihre Endbenutzer verfügbar sein sollen, die folgenden Informationen, um zu ermitteln, welche Clientbetriebssysteme und Agent-Betriebssysteme (View-Desktop) die Funktion unterstützen.

Tabelle 5-1. Auf Windows-basierten View Clients unterstützte Funktionen

Funktion	Windows XP-Desktop	Windows Vista-Desktop	Windows 7-Desktop	Windows 8-Desktop	Windows Server 2008 R2-Desktop
USB-Zugriff	X	X	X	X	X
Echtzeit-Audio/Video (RTAV)	X	X	X	X	X
RDP-Anzeigeprotokoll	X	X	X	X	X

Tabelle 5-1. Auf Windows-basierten View Clients unterstützte Funktionen (Fortsetzung)

Funktion	Windows XP-Desktop	Windows Vista-Desktop	Windows 7-Desktop	Windows 8-Desktop	Windows Server 2008 R2-Desktop
PCoIP-Anzeigeprotokoll	X	X	X	X	X
Persona-Verwaltung	X	X	X	X	
Wyse MMR	X	X			
Windows 7 MMR			X		
Standortbasiertes Drucken	X	X	X	X	
Virtuelles Drucken	X	X	X	X	
Smartcards	X	X	X	X	X
RSA SecurID oder RADIUS	X	X	X	X	X
Einmaliges Anmelden	X	X	X	X	X
Mehrere Monitore	X	X	X	X	X

Informationen darüber, welche Editionen bzw. Service Packs der einzelnen Clientbetriebssysteme unterstützt werden, finden Sie im Abschnitt „Systemanforderungen“.

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

- Windows 8-Desktops werden nur unterstützt, wenn Sie über Server und Desktops mit Horizon View 5.2 oder später verfügen.
- Die Echtzeit-Audio/Video-Funktion wird nur unterstützt, wenn Sie über Horizon View 5.2 mit Feature Pack 2 oder später verfügen.
- Windows 2008 R2-Desktops werden nur unterstützt, wenn Sie über Server und Desktops mit Horizon View 5.3 oder später verfügen.

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

Internationalisierung

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

Verwendung mehrerer Monitore

Unabhängig vom Anzeigeprotokoll können Sie mit einem View-Desktop mehrere Monitore verwenden.

Wenn Sie PCoIP verwenden, das Anzeigeprotokoll von VMware, können Sie die Anzeigeauflösung und die Drehung für jeden Monitor separat anpassen. PCoIP ermöglicht eine echte Sitzung mit mehreren Monitoren, anstelle von einer Erweiterungsmodussitzung.

Eine Erweiterungsmodus-Remote-Sitzung ist im Grunde eine Sitzung mit einem Monitor. Die Monitore müssen die gleiche Größe und Auflösung haben und das Monitorlayout muss in einen Begrenzungsrahmen passen. Wenn Sie ein Anwendungsfenster maximieren, füllt das Fenster alle Monitore aus. Microsoft RDP 6 verwendet den Erweiterungsmodus.

In einer echten Sitzung mit mehreren Monitoren, können die Monitore unterschiedliche Auflösungen und Größen haben, und ein Monitor kann geschwenkt sein. Wenn Sie ein Anwendungsfenster maximieren, wird das Fenster auf das Vollbild des Monitors erweitert, in dem es angezeigt wird.

Für diese Funktion gelten die folgenden Einschränkungen:

- Wenn Sie PCoIP verwenden, können Sie maximal 4 Monitore verwenden, um einen View-Desktop anzuzeigen, und zwar mit einer Auflösung von 2560 x 1600. Die maximale Anzahl Monitore, die übereinander gestapelt werden können, beträgt 2. Wenn die 3D-Funktion aktiviert ist, werden bis zu 2 Monitore mit einer Auflösung von 1920 x 1200 unterstützt.
- Wenn Sie Microsoft RDP 7 verwenden, beträgt die maximale Anzahl Monitore, die Sie zur Anzeige eines View-Desktops verwenden können, 16.
- Wenn Sie das Microsoft RDP-Anzeigeprotokoll verwenden, muss Microsoft Remote Desktop Connection (RDC) 6.0 oder später auf dem View-Desktop installiert sein.

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 Zeigegeräte. 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 über das Menü **USB-Gerät verbinden** nicht unterstützt. Zur Verwendung einer Webcam oder eines Audioeingabegeräts müssen Sie die Echtzeit-Audio/Video-Funktion verwenden. Diese Funktion steht bei Verwendung von VMware Horizon View- 5.2 Feature Pack 2 oder später zur Verfügung. Siehe „Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone“, auf Seite 66.

- Die Umleitung von USB-Audiogeräten ist vom Netzwerkstatus abhängig und daher nicht zuverlässig. Manche Geräte erfordern auch im Ruhezustand einen hohen Datendurchsatz. Wenn Sie die in VMware Horizon View- 5.2 Feature Pack 2 oder höher enthaltene Echtzeit-Audio/Video-Funktion verwenden, arbeiten Audioeingabe- und Audioausgabegeräte ordnungsgemäß, und die Verwendung der USB-Umleitung ist für diese Geräte nicht erforderlich.

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

Hinweis Leiten Sie keine USB-Geräte wie USB-Ethernet-Geräte und Touchscreen-Geräte an den Remote-Desktop um. Wenn Sie ein USB-Ethernet-Gerät umleiten, verliert Ihr lokales Clientsystem die Verbindung zum Netzwerk. Wenn Sie ein Touchscreen-Gerät umleiten, empfängt der Remote-Desktop Eingaben vom Touchscreen und nicht von der Tastatur. Wenn Sie Ihren virtuellen Desktop zur automatischen Verbindung von USB-Geräten konfiguriert haben, können Sie Richtlinien konfigurieren, um bestimmte Geräte auszuschließen. Siehe Thema „Konfiguration der Filterrichtlinieneinstellungen für USB-Geräte“ im Dokument *Verwaltung von VMware Horizon View-*.

Wichtig In diesem Verfahren wird die Verwendung des VMware Horizon View Client-Menüelements zur Konfiguration der automatischen Verbindung von USB-Geräten mit dem Remote-Desktop erläutert. Sie können die automatische Verbindung auch konfigurieren, indem Sie die Horizon View Client-Befehlszeilenschnittstelle verwenden oder eine Gruppenrichtlinie erstellen.

Weitere Informationen über die Befehlszeilenschnittstelle finden Sie unter „Ausführen von View Client aus der Befehlszeile“, auf Seite 49. Weitere Informationen zur Erstellung von Gruppenrichtlinien finden Sie im Dokument *Verwaltung von VMware Horizon View-*.

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 in den Abschnitten „USB-Einstellungen für View Agent“, „USB-Einstellungen für View Client“, „Konfiguration der Geräteaufschlüsselungs-Richtlinieneinstellungen für USB-Verbundgeräte“ und „Konfiguration der Filterrichtlinieneinstellungen für USB-Geräte“ im Dokument *Verwaltung von VMware Horizon View-*.

- Bei der Installation von Horizon View Client muss die Komponente **USB-Umleitung** mit installiert werden. Wenn Sie diese Komponente nicht in die Installation eingeschlossen haben, sollten Sie das Installationsprogramm erneut ausführen, die Komponenten ändern und die Komponente **USB-Umleitung** einschließen.

Vorgehensweise

- Verbinden Sie das USB-Gerät manuell mit einem Remote-Desktop.

  a Schließen Sie das USB-Gerät an Ihr lokales Clientsystem an.

  b Klicken Sie in der VMware Horizon View Client-Menüleiste auf **USB-Gerät verbinden**.

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

  c 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 Klicken Sie in der VMware Horizon View Client-Menüleiste auf **USB-Geräte verbinden > USB-Geräte bei Start automatisch verbinden**.

  b 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 von Clients zur erneuten Verbindung beim Neustart der USB-Geräte

Wenn Sie View Client nicht zur automatischen Verbindung der USB-Geräte mit Ihrem View-Desktop konfigurieren, können Sie immer noch festlegen, dass View Client mit bestimmten Geräten, die gelegentlich neu starten, wieder eine Verbindung herstellt. Wenn anderenfalls ein Gerät während eines Upgrade-Vorgangs neu startet, stellt es eine Verbindung zum lokalen System, anstatt zum View-Desktop her.

Wenn Sie als USB-Gerät zum Beispiel ein Smartphone oder ein Tablet verbinden möchten, welches bei Betriebssystem-Upgrades automatisch neu gestartet wird, können Sie View Client dazu anweisen, das bestimmte Gerät erneut mit dem View-Desktop zu verbinden. Zum Durchführen dieser Aufgabe muss die Konfigurationsdatei auf dem Client bearbeitet werden.

Wenn Sie die Option **Nach Einführung automatisch verbinden** in View Client verwenden, werden alle Geräte, die Sie am Clientsystem anschließen, an den View-Desktop umgeleitet. Wenn Sie nicht möchten, dass alle Geräte verbunden werden, sollten Sie die folgende Vorgehensweise zur Konfiguration von View Client anwenden, sodass nur bestimmte USB-Geräte automatisch neu verbunden werden.

Voraussetzungen

Ermitteln Sie das hexadezimale Format der Hersteller-ID (VID) und der Produkt-ID (PID) des Geräts. Anweisungen hierzu finden Sie im VMware KB-Artikel http://kb.vmware.com/kb/1011600.

Vorgehensweise

1 Öffnen Sie die Datei `config.ini` in einem Text-Editor auf dem Client.

Betriebssystemversion	Dateipfad
Windows 7	`C:\ProgramData\VMware\VMware USB Arbitration Service\config.ini`
Windows XP	`C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware USB Arbitration Service\config.ini`

2 Legen Sie die Eigenschaft `slow-reconnect` für das bestimmte Gerät oder die Geräte fest.

```
usb.quirks.device0 = "vid:pid slow-reconnect"
```

Hier stehen *vid*:*pid* jeweils für die Hersteller- und die Produkt-ID (im hexadezimalen Format) des Geräts. Die folgenden Zeilen legen diese Eigenschaft beispielsweise für zwei USB-Geräte fest:

```
usb.quirks.device0 = "0x0529:0x0001 slow-reconnect"
usb.quirks.device1 = "0x0601:0x0009 slow-reconnect"
```

Geben Sie die Geräteeigenschaften `usb.quirks.deviceN` in der richtigen Reihenfolge, beginnend bei 0, an. Folgt auf die Zeile `usb.quirks.device0` zum Beispiel nicht eine Zeile mit `usb.quirks.device1`, sondern eine Zeile mit `usb.quirks.device2`, wird nur die erste Zeile gelesen.

Wenn nun für Geräte wie Smartphones oder Tablets ein Upgrade der Firmware oder des Betriebssystems durchgeführt wird, verläuft das Upgrade erfolgreich, da das Gerät neu startet und die Verbindung zu dem View-Desktop herstellt, welcher das Gerät verwaltet.

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

Wichtig Wenn Sie eine USB-Webcam verwenden, verbinden Sie diese nicht über das Menü **USB-Gerät verbinden** 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 einer bevorzugten Webcam auf einem Windows-Clientsystem

Wenn Sie die Echtzeit-Audio/Video-Funktion einsetzen und auf Ihrem Clientsystem über mehrere Webcams verfügen, wird nur eine davon auf Ihrem View-Desktop verwendet. Zur Festlegung einer bevorzugten Webcam können Sie einen Registrierungsschlüsselwert festlegen.

Die bevorzugte Webcam wird auf dem Remote-Desktop verwendet, sofern sie verfügbar ist. Andernfalls wird eine andere Webcam verwendet.

Voraussetzungen

- Stellen Sie sicher, dass auf Ihrem Clientsystem eine USB-Webcam installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren Remote-Desktop verwenden.

Vorgehensweise

1 Schließen Sie die Webcam an, die Sie verwenden möchten.

2 Starten Sie einen Anruf, und stoppen Sie den Anruf.

Auf diese Weise wird eine Protokolldatei erstellt.

3 Öffnen Sie die Debug-Protokolldatei mit einem Texteditor.

Betriebssystem	Protokolldatei, Speicherort
Windows XP	`C:\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Anwendungsdaten\VMware\VDM\Logs\debug-20`*`JJ-MM-TT-XXXXXX`*`.txt`
Windows 7 oder Windows 8	`C:\Benutzer\%username%\AppData\Local\VMware\VDM\Logs\debug-20`*`JJ-MM-TT-XXXXXX`*`.txt`

Das Format der Protokolldatei lautet `debug-20`*`JJ-MM-TT-XXXXXX`*`.txt`, wobei 20*JJ* für das Jahr, *MM* für den Monat, *TT* für den Tag und *XXXXXX* für eine Nummer steht.

4 Durchsuchen Sie die Protokolldatei nach `[ViewMMDevRedir] VideoInputBase::LogDevEnum`, um die Protokolldateieinträge zu finden, in denen die angeschlossenen Webcams referenziert werden.

Nachfolgend sehen Sie einen Auszug aus der Protokolldatei zur Identifikation der Microsoft Lifecam HD-5000-Webcam:

```
[ViewMMDevRedir] VideoInputBase::LogDevEnum - 2 Device(s) found

[ViewMMDevRedir] VideoInputBase::LogDevEnum - Index=0 Name=Integrated Webcam   UserId=vid_1bcf&pid_2b83&mi_00#7&1b2e878b&0&0000   SystemId=\\?\usb#vid_1bcf&pid_2b83&mi_00#

[ViewMMDevRedir] VideoInputBase::LogDevEnum - Index=1 Name=Microsoft LifeCam HD-5000  UserId=vid_045e&pid_076d&mi_00#8&11811f49&0&0000  SystemId=\\?\usb#vid_045e&pid_076d&mi_00#
```

5 Kopieren Sie die Benutzer-ID der bevorzugten Webcam.

Beispiel: Kopieren Sie `vid_045e`, um die Microsoft LifeCam HD-5000 als Standardwebcam festzulegen.

6 Starten Sie den Registrierungs-Editor (`regedit.exe`) und navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RTAV`.

7 Fügen Sie den ID-Bestandteil der Zeichenfolgen in den REG_SZ-Wert **srcWCamId** ein.

Beispiel: Fügen Sie `vid_045e` in **srcWCamId** ein.

8 Speichern Sie Ihre Änderungen und beenden Sie die Registrierung.

9 Starten Sie einen neuen Anruf.

Auswählen eines Standardmikrofons auf einem Windows-Clientsystem

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

Wichtig Wenn Sie ein USB-Mikrofon verwenden, verbinden Sie dieses nicht über das Menü **USB-Gerät verbinden** 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 Wenn Sie gerade einen Anruf tätigen, beenden Sie das Gespräch.

2 Klicken Sie mit der rechten Maustaste auf das Lautsprechersymbol in der Systemleiste und wählen Sie **Aufnahmegeräte**.

Alternativ können Sie die Option „Sound“ in der Systemsteuerung öffnen und auf die Registerkarte **Aufnahme** klicken.

3 Klicken Sie im Dialogfeld **Sound** auf der Registerkarte **Aufnahme** mit der rechten Maustaste auf das Mikrofon, das Sie verwenden möchten.

4 Wählen Sie **Als Standardgerät auswählen** und klicken Sie auf **OK**.

5 Starten Sie über View-Desktop einen neuen Anruf.

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.

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 Druckeinstellungen 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 63.

- 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.

Steuern der Anzeige von Adobe Flash

Der View-Administrator kann den Adobe Flash-Inhalt so einrichten, dass er auf Ihrem View-Desktop auf einer Stufe angezeigt wird, die möglichst wenig Rechenressourcen in Anspruch nimmt. Manchmal können diese Einstellungen zu einer schlechten Wiedergabequalität beitragen. Wenn Sie mit dem Mauszeiger auf den Adobe Flash-Inhalt zeigen, können Sie die Adobe Flash-Einstellungen überschreiben, die Ihr View-Administrator festgelegt hat.

Die Adobe Flash-Anzeigesteuerung steht nur in Internet Explorer-Sitzungen unter Windows zur Verfügung sowie nur bei den Adobe Flash-Versionen 9 und 10. Zur Steuerung der Adobe Flash-Anzeigequalität darf Adobe Flash nicht im Vollbildmodus ausgeführt werden.

Vorgehensweise

1 Navigieren Sie im Internet Explorer im View-Desktop zu dem entsprechenden Adobe Flash-Inhalt und starten Sie ihn, falls erforderlich.

Je nach Konfiguration der Adobe Flash-Einstellungen durch Ihren View-Administrator werden Ihnen „Dropped Frames“, d. h. ausgelassene Videoframes, oder eine geringere Wiedergabequalität auffallen.

2 Bewegen Sie den Mauszeiger während der Wiedergabe auf den Adobe Flash-Inhalt.

Die Anzeigequalität verbessert sich, solange der Cursor auf dem Adobe Flash-Inhalt bleibt.

3 Um die Qualitätsverbesserung beizubehalten, doppelklicken Sie auf den Adobe Flash-Inhalt.

Verwenden der Funktion der relativen Mausbewegung für CAD- und 3D-Anwendungen

Wenn Sie das PCoIP-Anzeigeprotokoll bei CAD- oder 3D-Anwendungen in einem Horizon View 5.2-Desktop oder höher verwenden, können Sie die Mausleistung durch Aktivierung der Funktion für die relative Mausbewegung verbessern.

In den meisten Fällen, wenn Sie Anwendungen verwenden, die kein 3D-Rendering erfordern, überträgt View Client Informationen über die Mauszeigerbewegungen mithilfe von absoluten Koordinaten. Bei der Verwendung von absoluten Koordinaten rendert der Client die Mausbewegungen lokal, wodurch die Leistung insbesondere dann verbessert wird, wenn Sie sich außerhalb des Firmennetzwerks befinden.

Bei der Arbeit mit grafikintensiven Anwendungen wie AutoCAD oder bei 3D-Videospielen können Sie die Mausleistung verbessern, indem Sie die Funktion für die relative Mausbewegung aktivieren. Diese Funktion verwendet relative statt absoluter Koordinaten. Um diese Funktion zu verwenden, wählen Sie **Optionen > Relative Maus aktivieren** in der View Client-Menüleiste.

Hinweis Wenn Sie View Client im Fenstermodus und nicht im Vollbildmodus verwenden und die Funktion der relativen Mausbewegung aktiviert ist, können Sie möglicherweise den Mauszeiger nicht auf die View Client-Menüoptionen oder aus dem View Client-Fenster hinaus bewegen. Um diese Situation zu beheben, drücken Sie Strg+Alt.

Wenn die Funktion der relativen Mausbewegung aktiviert ist, kann die Performance langsam sein, wenn Sie sich außerhalb des Firmennetzwerks in einem WAN befinden.

Wichtig Für diese Funktion wird ein Horizon View 5.2-Desktop oder höher benötigt, und Sie müssen das 3D-Rendering für den Desktop-Pool einschalten. Weitere Informationen zu Pool-Einstellungen und den Optionen für 3D-Rendering finden Sie im Dokument *Verwaltung von VMware Horizon View-*.

Fehlerbehebung für Horizon View Client 6

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:

Vorgehensweise, wenn View Client unerwartet beendet wird

View Client wird möglicherweise beendet, selbst wenn Sie die Anwendung nicht schließen.

Problem

View Client wird möglicherweise unerwartet beendet. Abhängig von Ihrer View-Verbindungsserver-Konfiguration kann eine Meldung wie die folgende angezeigt werden: `Es besteht keine sichere Verbindung mit View-Verbindungsserver`. In manchen Fällen wird jedoch keine Meldung angezeigt.

Ursache

Dieses Problem tritt auf, wenn die Verbindung zu View-Verbindungsserver getrennt wird.

Lösung

- Starten Sie View Client neu. Sobald View-Verbindungsserver wieder ausgeführt wird, können Sie erfolgreich eine Verbindung herstellen. Sollten weiterhin Probleme mit der Verbindung bestehen, wenden Sie sich an Ihren View-Administrator.

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 **Desktop zurücksetzen**-Befehl.

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Wählen Sie **Optionen > Desktop zurücksetzen** aus der Menüleiste.
In der Desktop-Auswahlliste	a Starten Sie Horizon View Client, stellen Sie eine Verbindung mit der View-Verbindungsserver-Instanz her, die Zugriff auf den Remote-Desktop bietet, und geben Sie Ihre Anmeldeinformationen für die Authentifizierung an. b Wechseln Sie zum Fenster für die Desktop-Auswahl, klicken Sie mit der rechten Maustaste auf das Desktop-Symbol und wählen Sie **Desktop zurücksetzen**.

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.

Verwenden Sie beispielsweise das Applet **Software** Ihres Windows-Betriebssystems, um die VMware Horizon View Client-Anwendung zu entfernen.

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

Siehe Kapitel 2, „Installation von View Client für Windows“, auf Seite 19.

Index