Verwenden von VMware Horizon Client für Chrome OS

VMware Horizon Client for Chrome OS 4.5

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-002506-00

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

Verwenden von VMware Horizon Client für Chrome OS

Das Handbuch *Verwenden von VMware Horizon Client für Chrome OS* bietet Informationen zur Installation und Verwendung der VMware Horizon® Client™-Software für Chrome OS auf einem Chrome OS-Gerät zur Herstellung einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung im Datencenter.

Zu den Informationen in dieser Dokumentation gehören die Systemvoraussetzungen und Anweisungen zur Installation und Verwendung von Horizon Client für Chrome OS.

Diese Informationen sind für Administratoren gedacht, die bereits Erfahrung mit der Verwendung von Horizon und VMware vSphere haben. Als neuer Benutzer von Horizon benötigen Sie möglicherweise gelegentlich die schrittweisen Anleitungen für grundlegende Verfahren in den Dokumenten *View-Installation* und *Administration von View*.

Konfiguration und Installation 1

Zur Einrichtung einer Horizon-Bereitstellung für Chrome OS-Clients gehört die Verwendung bestimmter Konfigurationseinstellungen für den Verbindungsserver, die Sicherstellung der Systemanforderungen für Horizon Server und Chrome OS-Clients sowie das Herunterladen und Installieren von Horizon Client für Chrome OS.

Ab der Version Horizon Client 4.3 können Sie Horizon Client für Android auf bestimmten Chromebook-Modellen installieren. Weitere Informationen dazu finden Sie im Dokument *Verwenden von VMware Horizon Client für Android*.

Dieses Kapitel behandelt die folgenden Themen:

Systemanforderungen

Das Gerät, auf dem Sie Horizon Client installieren, muss bestimmte Systemanforderungen erfüllen.

Gerätemodelle	Chromebook
Betriebssysteme	Chrome OS, stabiler Kanal, ARC Version 41.4410.244.13 oder höher
CPU-Architektur	■ ARM ■ x86

Verbindungsserver, Sicherheitsserver und View Agent oder Horizon Agent	Die aktuelle Wartungsversion von 6.x und spätere Versionen. VMware empfiehlt, einen Sicherheitsserver oder die Unified Access Gateway-Appliance zu verwenden, damit Ihr Gerät keine VPN-Verbindung benötigt.
Anzeigeprotokolle	■ PCoIP ■ VMware Blast (erfordert Horizon Agent 7.0 oder höher)

Systemanforderungen für Echtzeit-Audio/Video

Echtzeit-Audio/Video arbeitet mit Standard-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-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

Wichtig Es wird nur die Audio-Eingangs-Funktion unterstützt. Die Video-Funktion wird nicht unterstützt.

Remote-Desktops	Auf den Desktops muss View Agent 5.3 oder später installiert sein. Für View Agent 5.3-Desktops muss auf den Desktops auch der entsprechende Remote Experience Agent installiert sein. Wenn beispielsweise View Agent 5.3 installiert ist, müssen Sie auch den Remote Experience Agent aus dem View 5.3 Feature Pack 1 installieren. Weitere Informationen finden Sie im Dokument *Installation und Administration von View Feature Pack*. Wenn Sie über View Agent 6.0 oder höher oder über Horizon Agent 7.0 oder höher verfügen, ist kein Feature Pack erforderlich. Um die Echtzeit-Audio-Video-Funktion mit RDS-Desktops und Remoteanwendungen zu verwenden, benötigen Sie Horizon Agent 7.0.2 oder höher.
Clientzugriffsgerät	Echtzeit-Audio/Video wird auf allen Chromebooks unterstützt, auf denen Horizon Client für Chrome OS ausgeführt wird.

Vorbereiten des Verbindungsservers für Horizon Client

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

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

- Wenn Sie Unified Access Gateway verwenden möchten, konfigurieren Sie den Verbindungsserver zur Zusammenarbeit mit Unified Access Gateway. Siehe das Dokument *Bereitstellen und Konfigurieren von Unified Access Gateway*. Unified Access Gateway-Appliances erfüllen dieselbe Rolle, die früher nur Sicherheitsserver übernommen hatten.
- Wenn Sie einen Sicherheitsserver verwenden, stellen Sie sicher, dass Sie die aktuellen Wartungsversionen für einen Verbindungsserver der Version 5.3.x und für einen Sicherheitsserver der Version 5.3.x oder höher verwenden. Weitere Informationen finden Sie im Dokument *View-Installation*.
- Wenn Sie eine sichere Tunnelverbindung für Clientgeräte verwenden möchten und die sichere Verbindung mit einem DNS-Hostnamen für den Verbindungsserver oder einen Sicherheitsserver konfiguriert ist, muss sichergestellt werden, dass das Clientgerät diesen DNS-Namen auflösen kann.

Wechseln Sie zur Aktivierung oder Deaktivierung der sicheren Tunnelverbindung in Horizon Administrator zum Dialogfeld Horizon-Verbindungsserver-Einstellungen bearbeiten und aktivieren Sie das Kontrollkästchen **Sichere Tunnelverbindung zum Desktop verwenden**.

- Vergewissern Sie sich, dass ein Desktop- oder Anwendungspool erstellt wurde und das Benutzerkonto, das Sie verwenden möchten, über die Rechte zum Zugriff auf diesen Pool verfügt. Informationen dazu finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.
- Für die Verwendung der zweistufigen Authentifizierung für Horizon Client, z. B. der RSA SecurID- oder RADIUS-Authentifizierung, müssen Sie diese Funktion auf dem Verbindungsserver aktivieren. Weitere Informationen finden Sie in den Themen zur zweistufigen Authentifizierung im Dokument *Administration von View*.
- Um Sicherheitsinformationen wie Server-URL-Informationen und das Dropdown-Menü **Domäne** in Horizon Client auszublenden, aktivieren Sie in Horizon Administrator die Einstellungen **Serverinformationen in der Kunden-Benutzeroberfläche ausblenden** und **Domänenliste in der Kunden-Benutzeroberfläche ausblenden**. Diese globalen Einstellungen sind in Horizon 7 Version 7.1 und höher verfügbar. Weitere Informationen zur Konfiguration globaler Einstellungen finden Sie im Dokument *Administration von View*.

  Um eine Authentifizierung bei ausgeblendetem Dropdown-Menü **Domäne** durchführen zu können, müssen Benutzer die Domäneninformationen durch Eingabe ihres Benutzernamens im Format ***Domäne**Benutzername*** oder ***Benutzername@Domäne*** in das Textfeld **Benutzername** zur Verfügung stellen.

  Wichtig Wenn Sie die Einstellungen **Serverinformationen in der Kunden-Benutzeroberfläche ausblenden** und **Domänenliste in der Kunden-Benutzeroberfläche ausblenden** aktivieren und die zweistufige Authentifizierung (RSA SecureID oder RADIUS) für die Verbindungsserver-Instanz auswählen, dürfen Sie nicht die Windows-Benutzernamenübereinstimmung erzwingen. Wenn die Windows-Benutzernamenübereinstimmung erzwungen wird, können Benutzer keine Domäneninformationen in das Textfeld „Benutzername“ eingeben und es ist keine Anmeldung mehr möglich. Weitere Informationen finden Sie in den Themen zur zweistufigen Authentifizierung im Dokument *Administration von View*.
- Um Benutzern einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen in Horizon Client zu ermöglichen, müssen Sie diese Funktion im Verbindungsserver aktivieren. Weitere Informationen finden Sie in den Themen zum nicht authentifizierten Zugriff im Dokument *Administration von View*.

Verwenden von eingebetteten RSA SecurID-Software-Token

Wenn Sie RSA SecurID-Software-Token erstellen und an Endbenutzer verteilen, müssen diese zum Authentifizieren lediglich ihre PIN und nicht die PIN plus den Token-Code eingeben.

Setup-Voraussetzungen

Sie können mithilfe von CTF (Compressed Token Format) oder der dynamischen Bereitstellung von Seed-Datensätzen, auch als CT-KIP (Cryptographic Token Key Initialization Protocol) bezeichnet, ein benutzerfreundliches RSA-Authentifizierungssystem einrichten. Mit diesem System generieren Sie eine URL, die Sie an die Endbenutzer senden. Um das Token zu installieren, fügen die Endbenutzer diese URL auf ihren Clientgeräten direkt in Horizon Client ein. Das Dialogfeld zum Einfügen dieser URL wird angezeigt, wenn die Endbenutzer mit Horizon Client eine Verbindung zum Verbindungsserver herstellen.

Nachdem das Software-Token installiert wurde, geben die Endbenutzer zur Authentifizierung eine PIN ein. Bei externen RSA-Token müssen die Endbenutzer eine PIN und den Token-Code eingeben, der von einem Hardware- oder Software-Authentifizierungstoken generiert wurde.

Die folgenden URL-Präfixe werden unterstützt, wenn bei einer Verbindung von Horizon Client mit einer Verbindungsserver-Instanz, auf der RSA aktiviert ist, die Endbenutzer die URL kopieren und in Horizon Client einfügen:

- `viewclient-securid://`
- `http://127.0.0.1/securid/`

Endbenutzer können das Token durch Antippen der URL installieren. Es werden beide Präfixe (`viewclient-securid://` und `http://127.0.0.1/securid/`) unterstützt. Beachten Sie, dass nicht alle Browser Hyperlinks unterstützen, die mit `http://127.0.0.1` beginnen. Zudem können manche Dateibrowser, so zum Beispiel die Datei-Manager-App auf dem ASUS Transformer Pad, die SDTID-Datei nicht mit Horizon Client verknüpfen.

Informationen zur dynamischen Bereitstellung von Seed-Datensätzen bzw. dateibasierten Bereitstellung (CTF) finden Sie auf der Webseite *RSA SecurID Software Token for iPhone Devices* unter http://www.rsa.com/node.aspx?id=3652 oder auf der Webseite *RSA SecurID Software Token for Android* unter http://www.rsa.com/node.aspx?id=3832.

Anweisungen für Endbenutzer

Wenn Sie eine CTFString-URL oder eine CT-KIP-URL erstellen, die an die Endbenutzer gesendet werden soll, können Sie eine URL mit oder ohne Kennwort bzw. Aktivierungscode generieren. Sie senden diese URL in einer E-Mail an die Endbenutzer. Diese E-Mail muss die folgenden Informationen enthalten:

- Anweisungen zur Navigation zum Dialogfeld „Software-Token installieren“.

  Weisen Sie die Endbenutzer an, im Horizon Client-Dialogfeld auf **Externes Token** zu tippen. Dadurch werden sie aufgefordert, ihre RSA SecurID-Anmeldedaten einzugeben, wenn sie eine Verbindung mit der Verbindungsserver-Instanz herstellen.

- CTFString-URL oder CT-KIP-URL als normaler Text.

  Wenn die URL formatiert ist, wird den Endbenutzern eine Fehlermeldung angezeigt, sofern sie versuchen, die URL in Horizon Client zu verwenden.

- Aktivierungscode, wenn die CT-KIP-URL, die Sie erstellen, nicht bereits den Aktivierungscode enthält.

  Endbenutzer müssen diesen Aktivierungscode in einem Textfeld des Dialogfelds eingeben.

- Wenn die CT-KIP-URL einen Aktivierungscode enthält, teilen Sie den Endbenutzern mit, dass im Textfeld **Kennwort oder Aktivierungscode** des Dialogfeldes „Software-Token installieren“ keine Eingabe erforderlich ist.

Konfigurieren erweiterter TLS-/SSL-Optionen

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

TLSv1.0, TLSv1.1 und TLSv1.2 sind standardmäßig aktiviert. SSL v2.0 und 3.0 werden nicht unterstützt. Die standardmäßige Verschlüsselungszeichenfolge lautet „!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA +AESGCM:kECDH+AES:ECDH+AES:RSA+AES“.

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

Informationen zum Konfigurieren der Sicherheitsprotokolle, die von Verbindungsserver-Instanzen akzeptiert werden, finden Sie im Dokument *View-Sicherheit*.

Vorgehensweise

1 Tippen Sie auf das Zahnradsymbol **Einstellungen** rechts oben im Horizon Client-Fenster und dann auf **Sicherheitsoptionen**.

2 Tippen Sie auf **Erweiterte SSL-Optionen**.

3 Stellen Sie sicher, dass **Standardeinstellungen verwenden** deaktiviert ist.

4 Zum Aktivieren oder Deaktivieren eines Sicherheitsprotokolls tippen Sie auf das Kontrollkästchen neben dem Namen des Sicherheitsprotokolls.

5 Um die Schlüsselsteuerzeichenfolge zu ändern, ersetzen Sie die Standardzeichenfolge.

6 (Optional) Falls Sie die Standardeinstellungen wiederherstellen müssen, tippen Sie, um **Standardeinstellungen verwenden** auszuwählen.

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

Die Änderungen werden wirksam, wenn Sie das nächste Mal eine Verbindung zum Server herstellen.

Unterstützte Desktop-Betriebssysteme

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

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

Installieren oder Aktualisieren von Horizon Client für Chrome OS

Horizon Client für Chrome OS ist eine Chrome OS-App, die Sie wie andere Chrome OS-Anwendungen installieren können.

Voraussetzungen

Wenn Sie das Chrome OS-Gerät noch nicht eingerichtet haben, so holen Sie dies nun nach. Siehe Bedienungsanleitung des Geräteherstellers.

Vorgehensweise

1 Melden Sie sich bei Ihrem Chromebook an.

2 Laden Sie die Horizon Client für Chrome OS-App vom Chrome Web Store herunter und installieren Sie diese.

3 Um festzustellen, ob die Installation erfolgreich war, überprüfen Sie, ob das **Horizon Client für Chrome OS**-App-Symbol im Chrome App Launcher angezeigt wird.

Konfigurieren der Decodierung für VMware Blast-Sitzungen

Sie können das Dekodieren für Remote-Desktop- und Remoteanwendungssitzungen konfigurieren, die das VMware Blast-Anzeigeprotokoll verwenden.

Voraussetzungen

Diese Funktion erfordert Horizon Agent 7.0 oder höher.

Vorgehensweise

1 Tippen Sie auf das Zahnradsymbol **Einstellungen** rechts oben im Horizon Client-Bildschirm und dann auf **VMware Blast**.

2 Aktivieren Sie das Kontrollkästchen **H.264**, um die H.264-Decodierung zuzulassen, oder deaktivieren Sie das Kontrollkästchen **H.264**, um die H.264-Decodierung auszuschalten.

   Wenn das Kontrollkästchen aktiviert ist, verwendet Horizon Client die H.264-Decodierung, sofern der Agent die H.264-Softwarecodierung unterstützt. Unterstützt der Agent die H.264-Softwarecodierung nicht, verwendet Horizon Client die JPG/PNG-Decodierung. Ist das Kontrollkästchen deaktiviert, verwendet Horizon Client immer die JPG/PNG-Dekodierung.

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

Konfigurieren der Horizon Client -Standardansicht

Sie können durch Konfiguration festlegen, ob zuletzt verwendete Desktops und Anwendungen oder Serververknüpfungen angezeigt werden, wenn Sie Horizon Client starten.

Vorgehensweise

1 Tippen Sie auf das Zahnradsymbol **Einstellungen** in der oberen rechten Ecke des Horizon Client-Fensters und tippen Sie dann auf **Anzeige**.

2 Tippen Sie auf **Standardstartansicht**.

Die ausgewählte Standardansicht wird sofort wirksam.

Aktivieren der Funktion für mehrere Monitore für Horizon Client

Mit der Funktion für mehrere Monitore können Sie einen Remote-Desktop auf einen externen Monitor erweitern.

Um die Funktion für mehrere Monitore für Horizon Client zu aktivieren, installieren Sie eine Helper-Erweiterung und aktivieren Sie den Unified Desktop-Modus auf Ihrem Chromebook.

Sie müssen die Helper-Erweiterung installieren, damit das Remote-Desktop-Fenster korrekt auf dem externen Monitor angezeigt wird, wenn die Chromebook- und die externe Anzeige ein unterschiedliches Breite-Länge-Verhältnis aufweisen.

Vorgehensweise

1 Melden Sie sich bei Ihrem Chromebook an.

2 Laden Sie die VMware Horizon Client-Helper-Erweiterung aus dem Chrome Web Store herunter und installieren Sie diese.

3 Öffnen Sie ein Browserfenster auf Ihrem Chromebook und geben Sie in der URL-Leiste `chrome://flags` ein.

4 Führen Sie einen Bildlauf nach unten bis **Unified Desktop-Modus** durch und klicken Sie auf **Aktivieren**.

5 Klicken Sie auf **Jetzt neu starten**, um Ihr Chromebook neu zu starten und die Änderungen wirksam werden zu lassen.

Weiter

Nach dem Neustart des Chromebook können Sie die Chromebook-Einstellungen öffnen und durch Klicken auf **Anzeigeeinstellungen** die Anzeigeoptionen für Unified Desktop konfigurieren.

Um ein Remote-Desktop-Fenster auf den externen Monitor zu erweitern, klicken Sie auf die Schaltfläche **Maximieren**. Sie können durch Klicken auf die Schaltfläche **Wiederherstellen** das Remote-Desktop-Fenster wieder auf dem Chromebook-Monitor anzeigen lassen.

Konfigurieren einer standardmäßigen Verbindungsserver-URL

Ein Chrome-Administrator hat die Möglichkeit, eine standardmäßige Verbindungsserver-URL für Horizon Client auf registrierten Chromebooks zu konfigurieren. Wenn eine standardmäßige Verbindungsserver-URL konfiguriert ist, wird Horizon Client immer mit dem Standardserver verbunden.

Anforderungen und Voraussetzungen

Für die Funktion der standardmäßigen Verbindungsserver-URL gelten die im Folgenden aufgeführten Anforderungen und Voraussetzungen.

- Die Funktion wird nur auf registrierten Chromebooks unterstützt, die mit dem G Suite-Administrator verwaltet werden.
- Ein Chrome-Administrator muss die Horizon Client für Chrome OS-App und die VMware Horizon Client-Helper-Erweiterung über die Chrome-Geräteverwaltung installieren. Die App und die Erweiterung sind im Chrome Web Store verfügbar.

Wenn eine standardmäßige Verbindungsserver-URL festgelegt ist, wird das Zahnradsymbol **Einstellungen** in Horizon Client nicht angezeigt, solange sich kein Benutzer bei einer Remotesitzung angemeldet hat, und bestimmte Optionen wie z. B. **VMware Blast** und **Nicht authentifizierter Zugriff** können nicht geändert werden.

Erstellen einer JSON-Konfigurationsdatei

Ein Chrome-Administrator muss die standardmäßige Verbindungsserver-URL in einer JSON-Konfigurationsdatei angeben. Beispielsweise legt die folgende JSON-Konfigurationsdatei die standardmäßige Verbindungsserver-URL auf `connection-server.mycompany.com` fest.

```
{
    "Default Server URL":{
    "Value":"connection-server.mycompany.com"
   }
}
```

Es werden die im Folgenden aufgeführten URL-Formate unterstützt.

Format	Beispiel
Nur Domänenname	`connection-server.mycompanycom`
Domänenname und -port	`connection-server.mycompany.com:443`
HTTPS-Schema und Domänenname	`https://connection-server.mycompany.com`
HTTPS-Schema, Domänenname und Portnummer	`https://connection-server.mycompany.com:443`

Erstellen Sie eine Richtlinie, um die standardmäßige Verbindungsserver-URL festzulegen.

Um die Verbindungsserver-URL für Horizon Client-Benutzer festzulegen, muss ein Chrome-Administrator eine Richtlinie erstellen. Um die Richtlinie erstellen zu können, muss sich der Chrome-Administrator bei der Google Admin-Konsole anmelden, die VMware Horizon Client-Helper-Erweiterung sowie **Benutzereinstellungen** auswählen und dann die JSON-Konfigurationsdatei, die die standardmäßige Verbindungsserver-URL festlegt, hochladen.

Ausführliche Informationen zur Anwendung der Google Admin-Konsole finden Sie in der Hilfe zum G Suite-Administrator.

Durch VMware gesammelte Horizon Client -Daten

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

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 Client-Informationen werden erst an den Verbindungsserver und dann an VMware gesendet, zusammen mit den Daten der Verbindungsserver-Instanzen, Desktop-Pools und Remote-Desktops.

Der Administrator, der die Installation des Verbindungsservers durchführt, kann während der Ausführung des Installations-Assistenten für den Verbindungsserver entscheiden, ob am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit teilgenommen wird. Nach der Installation kann ein Administrator eine entsprechende Option in Horizon Administrator festlegen.

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

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Unternehmen, das die Horizon Client-Anwendung hergestellt hat	Nein	VMware
Produktname	Nein	VMware Horizon Client
Client-Produktversion	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	Nein	Beispiele hierfür sind: ■ i386 ■ x86_64 ■ arm
Client-Build-Name	Nein	Beispiele hierfür sind: ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore
Host-Betriebssystem	Nein	Beispiele hierfür sind: ■ Windows 8.1 ■ Windows 7, Service Pack 1 für 64 Bit (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
Host-Betriebssystemkernel	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)

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

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Host-Betriebssystemarchitektur	Nein	Beispiele hierfür sind: ■ x86_64 ■ i386 ■ armv71 ■ ARM
Hostsystem-Modell	Nein	Beispiele hierfür sind: ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Hostsystem-CPU	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	Nein	Beispiel: 4
MB Arbeitsspeicher auf dem Hostsystem	Nein	Beispiele hierfür sind: ■ 4096 ■ unbekannt (für Windows Store)
Anzahl der angeschlossenen USB-Geräte	Nein	2 (Die Umleitung von USB-Geräten wird nur für Linux-, Windows- und Mac-Clients unterstützt.)
Maximale Anzahl gleichzeitiger USB-Geräteverbindungen	Nein	2
Hersteller-ID des USB-Geräts	Nein	Beispiele hierfür sind: ■ Kingston ■ NEC ■ Nokia ■ Wacom
Produkt-ID des USB-Geräts	Nein	Beispiele hierfür sind: ■ DataTraveler ■ Gamepad ■ Speicherlaufwerk ■ Kabellose Maus
USB-Gerätefamilie	Nein	Beispiele hierfür sind: ■ Sicherheit ■ Eingabegeräte ■ Bildverarbeitung
Nutzungszähler für das USB-Gerät	Nein	(Gibt an, wie oft das Gerät gemeinsam genutzt wurde)

Verwalten der Remote-Desktop- und Anwendungsverbindungen 2

Mit Horizon Client können Sie eine Verbindung zu einem Server herstellen, die Liste der Server, mit denen Sie sich verbinden können, bearbeiten, sich bei Remote-Desktops an- oder abmelden sowie Remoteanwendungen verwenden. Zur Fehlerbehebung können Sie auch Remote-Desktops und -Anwendungen 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:

Festlegen des Zertifikatsprüfungsmodus für Horizon 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 dem Verbindungsserver und Horizon Client durchgeführt. Die Zertifikatsüberprüfung umfasst die folgenden Checks:

- Ist das Zertifikat für einen anderen Zweck bestimmt als für die Überprüfung der Identität des Absenders und die Verschlüsselung der Serverkommunikation? Mit anderen Worten: Handelt es sich um den korrekten Zertifikattyp?
- Ist das Zertifikat abgelaufen oder erst zukünftig gültig? Mit anderen Worten: Ist das Zertifikat laut Computeruhr gültig?

- Stimmt der allgemeine Name auf dem Zertifikat mit dem Hostnamen des Servers überein, der es sendet? Zu einer fehlenden Übereinstimmung kann es kommen, wenn ein Lastenausgleich Horizon Client an einen Server mit einem Zertifikat umleitet, das nicht mit dem in Horizon Client eingegebenen Hostnamen übereinstimmt. Ein weiterer möglicher Grund für eine fehlende Übereinstimmung ist die Eingabe einer IP-Adresse statt eines Hostnamens im Client.
- Ist das Zertifikat von einer unbekannten oder nicht als vertrauenswürdig eingestuften Zertifizierungsstelle (CA) signiert worden? Selbstsignierte Zertifikate sind ein Typ der nicht als vertrauenswürdig eingestuften CA.

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

Hinweis Informationen zur Verteilung eines selbstsignierten Stammzertifikats, das die Benutzer auf ihren Chrome OS-Geräten installieren können, sowie Anweisungen zur Installation eines Zertifikats auf einem Chrome OS-Gerät finden Sie in der Dokumentation auf der Google-Website.

Zum Festlegen des Sicherheitsmodus tippen Sie auf das Zahnradsymbol **Einstellungen** in der oberen rechten Ecke des Horizon Client-Fensters, dann auf **Sicherheitsoptionen** und schließlich auf **Sicherheitsmodus**. 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 Servernamen übereinstimmen, den Sie in Horizon Client eingegeben haben.
- **Server-Identitätszertifikate nicht überprüfen**. Mit dieser Einstellung werden Zertifikate nicht überprüft.

Ist der Zertifikatsprüfungsmodus auf **Warnen** gesetzt, können Sie immer noch eine Verbindung mit einer Verbindungsserver-Instanz 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.

Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung

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

Voraussetzungen

- Besorgen Sie sich die Anmeldedaten, etwa einen Active Directory-Benutzernamen und das zugehörige Kennwort, den RSA SecurID-Benutzernamen und -Passcode oder den RADIUS-Authentifizierungsbenutzernamen oder -Passcode.
- Führen Sie die unter „Vorbereiten des Verbindungsservers für Horizon Client“, auf Seite 8 beschriebenen administrativen Aufgaben aus.

- Wenn Sie sich außerhalb des Firmennetzwerks befinden und für den Zugriff auf den Remote-Desktop oder auf die Remoteanwendung keinen Sicherheitsserver verwenden, müssen Sie sicherstellen, dass Ihr Clientgerät für die Verwendung einer VPN-Verbindung konfiguriert ist. Aktivieren Sie diese Verbindung.

  Wichtig In den meisten Fällen ist es empfehlenswert, einen Sicherheitsserver anstelle eines VPN zu verwenden.

- Stellen Sie sicher, dass Sie über den vollqualifizierten Domänennamen (FQDN) des Servers verfügen, der Zugriff auf den Remote-Desktop oder die Remoteanwendung gewährt. Unterstriche (_) werden in Servernamen nicht unterstützt. Wenn es sich nicht um Port 443 handelt, benötigen Sie auch die Portnummer.
- Wenn Sie planen, eingebettete RSA SecurID-Software zu verwenden, stellen Sie sicher, dass Sie die richtige CT-KIP-URL und den richtigen Aktivierungscode haben. Siehe „Verwenden von eingebetteten RSA SecurID-Software-Token“, auf Seite 9.
- Konfigurieren Sie den Zertifikatsprüfungsmodus für das SSL-Zertifikat, das vom Verbindungsserver präsentiert wird. Siehe „Festlegen des Zertifikatsprüfungsmodus für Horizon Client“, auf Seite 17.

Vorgehensweise

1 Sollte eine VPN-Verbindung erforderlich sein, müssen Sie das VPN aktivieren.

2 Auf Ihrem Chrome OS-Gerät tippen Sie auf das Symbol **Chrome App Launcher** in der Taskleiste und dann auf die App **Horizon Client für Chrome OS**.

Das Horizon Client-Fenster wird geöffnet.

3 Stellen Sie eine Verbindung mit einem Server her.

Option	Aktion
Verbindung mit einem neuen Server herstellen	Geben Sie den Namen eines Servers und optional eine Beschreibung ein und tippen Sie auf **Verbinden**.
Verbindung mit einem vorhandenen Server herstellen	Tippen Sie auf der Registerkarte **Server** auf die Serververknüpfung.

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

4 Wenn Sie zur Eingabe von RSA SecurID- oder RADIUS-Authentifizierungs-Anmeldedaten aufgefordert werden, geben Sie entweder Ihre Anmeldedaten ein oder installieren Sie ein eingebettetes RSA SecurID-Token, falls Sie beabsichtigen, ein solches zu verwenden.

Option	Aktion
Vorhandenes Token	Wenn Sie ein Hardware-Authentifizierungstoken oder ein Software-Authentifizierungstoken auf einem Smartphone verwenden, geben Sie Ihren Benutzernamen und Ihren Passcode ein. Der Passcode kann möglicherweise sowohl aus einer PIN als auch einer zum Token generierten Nummer bestehen.
Software-Token installieren	Klicken Sie auf **Externes Token**. Fügen Sie im Dialogfeld Install Software Token (Software-Token installieren) die CT-KIP- oder die CTFString-URL aus der E-Mail von Ihrem Administrator ein. Wenn die URL einen Aktivierungscode enthält, brauchen Sie im Textfeld **Kennwort oder Aktivierungscode** nichts einzugeben.

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

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

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

6 Geben Sie im Anmeldedialogfeld Ihren Benutzernamen und Ihr Kennwort ein, wählen Sie eine Domäne aus und tippen Sie dann auf **Anmelden**.

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

7 (Optional) Tippen Sie auf das Symbol der Einstellungen für das Anzeigeprotokoll rechts oben im Bildschirm, um das gewünschte Anzeigeprotokoll auszuwählen.

   VMware Blast stellt eine verbesserte Akkulaufzeit zur Verfügung und bietet das beste Protokoll für Benutzer von High-End-3D- und mobilen Geräten. Das Standardanzeigeprotokoll ist **PCoIP**.

8 Tippen Sie zum Herstellen einer Verbindung mit einem Remote-Desktop oder mit einer Remoteanwendung auf das Symbol des Desktops bzw. der Anwendung.

Nachdem Sie sich zum ersten Mal bei einem Remote-Desktop oder einer Remoteanwendung angemeldet haben, wird im Register **Zuletzt verwendet** eine Verknüpfung für den Desktop oder die Anwendung gespeichert. Wenn Sie das nächste Mal eine Verbindung mit dem Remote-Desktop oder mit der Remoteanwendung herstellen möchten, können Sie einfach auf diese Verknüpfung tippen.

Wenn Horizon Client keine Verbindung mit dem Remote-Desktop herstellen kann, führen Sie die folgenden Aufgaben aus:

- Legen Sie fest, ob der Verbindungsserver dahingehend konfiguriert werden soll, SSL nicht zu verwenden. Horizon Client erfordert SSL-Verbindungen. Prüfen Sie, ob die globale Einstellung in Horizon 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 Verbindungsserver konfiguriert ist.
- Stellen Sie eine ordnungsgemäße Funktionsweise des Sicherheitszertifikats für den Verbindungsserver sicher. Ist dies nicht der Fall, wird in Horizon Administrator möglicherweise angezeigt, dass der Agent auf Desktops nicht erreichbar ist.
- Stellen Sie sicher, dass die für die Verbindungsserver-Instanz festgelegten Kennzeichen Verbindungen von diesem Benutzer erlauben. Siehe das Dokument *Administration von View*.
- Stellen Sie sicher, dass der Benutzer zum Zugriff auf den Desktop oder die Anwendung berechtigt ist. Weitere Erläuterungen finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Verwenden des nicht authentifizierten Zugriffs zur Verbindung mit Remoteanwendungen

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

Voraussetzungen

- Führen Sie die unter „Vorbereiten des Verbindungsservers für Horizon Client“, auf Seite 8 beschriebenen administrativen Aufgaben aus.
- Richten Sie Benutzer für einen nicht authentifizierten Zugriff auf der Verbindungsserver-Instanz ein. Informationen dazu finden Sie unter „Bereitstellen eines nicht authentifizierten Zugriffs für veröffentlichte Anwendungen“ im Dokument *Administration von View*.
- Konfigurieren Sie den Zertifikatsprüfungsmodus für das SSL-Zertifikat, das vom Verbindungsserver präsentiert wird. Siehe „Festlegen des Zertifikatsprüfungsmodus für Horizon Client“, auf Seite 17.
- Wenn Sie auf Remoteanwendungen außerhalb des Unternehmensnetzwerks zugreifen, stellen Sie sicher, dass Ihr Clientgerät zur Verwendung einer VPN-Verbindung eingerichtet ist, und aktivieren Sie diese Verbindung.

Vorgehensweise

1 Sollte eine VPN-Verbindung erforderlich sein, müssen Sie das VPN aktivieren.

2 Tippen Sie auf Ihrem Chrome OS-Gerät auf das Symbol „Chrome App Launcher“ in der Taskleiste und dann auf die App „Horizon Client für Chrome OS“.

Das Horizon Client-Fenster wird geöffnet.

3 Tippen Sie auf das Zahnradsymbol **Einstellungen** in der oberen rechten Ecke des Horizon Client-Fensters, dann auf **Nicht authentifizierter Zugriff** und aktivieren Sie schließlich das Kontrollkästchen **Nicht authentifizierter Zugriff**.

4 Stellen Sie eine Verbindung mit dem Server her, auf dem Sie über einen nicht authentifizierten Zugriff auf Remoteanwendungen verfügen.

Option	Beschreibung
Verbindung mit einem neuen Server herstellen	Geben Sie den Namen eines Servers und optional eine Beschreibung ein und tippen Sie auf **Verbinden**.
Verbindung mit einem vorhandenen Server herstellen	Tippen Sie auf der Registerkarte **Server** auf die Serververknüpfung.

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

5 Wenn das Anmeldedialogfeld angezeigt wird, wählen Sie ein Benutzerkonto aus dem Dropdown-Menü **Benutzerkonto** aus, falls erforderlich.

Wenn nur ein Benutzerkonto verfügbar ist, wird das Benutzerkonto automatisch ausgewählt.

6 (Optional) Aktivieren Sie das Kontrollkästchen **Immer dieses Konto verwenden**, um das Anmeldefenster das nächste Mal zu umgehen, wenn Sie eine Verbindung mit dem Server herstellen.

   Um diese Einstellung zu deaktivieren, bevor Sie das nächste Mal eine Verbindung mit dem Server herstellen, berühren Sie die Serververknüpfung und halten Sie diese gedrückt, bis das Kontextmenü angezeigt wird. Tippen Sie auf dann auf **Bearbeiten**, auf **Gespeichertes Konto mit nicht authentifiziertem Zugriff löschen (*Name*)** und schließlich auf **Fertig**.

7 Tippen Sie auf **Verbinden**, um sich beim Server anzumelden.

   Das Auswahlfenster für Anwendungen wird angezeigt.

8 Tippen Sie auf das jeweilige Anwendungssymbol, um die Anwendung zu starten.

Nachdem Sie sich zum ersten Mal bei einer Remoteanwendung angemeldet haben, wird auf der Registerkarte **Zuletzt verwendet** eine Verknüpfung für die Anwendung gespeichert. Wenn Sie das nächste Mal eine Verbindung mit der Remoteanwendung herstellen möchten, können Sie einfach auf die Verknüpfung statt auf das Serversymbol tippen.

Verwalten von Serververknüpfungen

Nachdem Sie eine Verbindung zu einem Server hergestellt haben, erstellt Horizon Client eine Serververknüpfung. Diese Server-Verknüpfungen können Sie bearbeiten und entfernen.

Horizon Client speichert den Servernamen oder die IP-Adresse selbst dann in einer Verknüpfung, wenn Sie den Servernamen oder die IP-Adresse falsch eingeben. Durch Bearbeiten des Servernamens oder der IP-Adresse können Sie diese Informationen löschen oder ändern. Wenn Sie keine Serverbeschreibung eingeben, wird der Servername oder die IP-Adresse zur Serverbeschreibung.

Vorgehensweise

1 Tippen und halten Sie in der Registerkarte **Server** die Serververknüpfung, bis das Kontextmenü angezeigt wird.

2 Verwenden Sie das Kontextmenü, um den Server zu löschen oder den Servernamen, die Serverbeschreibung oder den Benutzernamen zu bearbeiten.

3 Wenn Sie die Serververknüpfung bearbeitet haben, tippen Sie auf **Fertig**, um Ihre Änderungen zu speichern.

Auswählen eines Remote-Desktops oder einer Remoteanwendung als Favorit

Sie können Remote-Desktops und -Anwendungen als Favoriten auswählen. Favoriten sind durch ein Sternchen gekennzeichnet. Mithilfe des Sternchens können Sie schnell die Favoriten-Desktops und -anwendungen finden. Die Auswahl der Favoriten wird gespeichert, auch nachdem Sie sich vom Server abgemeldet haben.

Voraussetzungen

Besorgen Sie sich die Anmeldeinformationen, die Sie zum Herstellen der Verbindung mit dem Server benötigen, z. B. einen Benutzernamen und ein Kennwort oder eine RSA SecureID und einen Passcode.

Vorgehensweise

1 Tippen Sie auf der Registerkarte **Server** auf die Serververknüpfung.

2 Geben Sie auf Aufforderung entweder Ihren RSA-Benutzernamen und den Passcode oder Ihren Active Directory-Benutzernamen und das entsprechende Kennwort oder beides ein.

3 Führen Sie die folgenden Schritte aus, um einen Desktop oder eine Anwendung als Favorit auszuwählen oder die Auswahl aufzuheben.

Option	Beschreibung
Favorit auswählen	Berühren und halten Sie auf der Registerkarte **Alle** den Desktop- oder Anwendungsnamen, bis das Kontextmenü angezeigt wird. Tippen Sie dann auf **Als Favorit markieren**. In der oberen rechten Ecke des Namens wird ein Sternchen angezeigt und der Name erscheint auf der Registerkarte **Favoriten**.
Die Auswahl eines Favoriten aufheben	Berühren und halten Sie auf der Registerkarte **Alle** oder **Favoriten** den Desktop- bzw. Anwendungsnamen, bis das Kontextmenü angezeigt wird. Tippen Sie dann auf **Markierung als Favorit aufheben**. Das Sternchen in der oberen rechten Ecke des Namens wird nicht mehr angezeigt und der Name verschwindet von der Registerkarte **Favoriten**.

4 Um nur Desktop- oder Anwendungsfavoriten darzustellen, berühren Sie die Registerkarte **Favoriten**.

Sie können auf die Registerkarte **Alle** tippen, um alle verfügbaren Desktops und Anwendungen anzuzeigen.

Trennen der Verbindung mit einem Remote-Desktop oder einer Remoteanwendung

Sie können die Verbindung zu einem Remote-Desktop trennen, ohne sich abzumelden, sodass die Anwendungen auf dem Remote-Desktop geöffnet bleiben. Sie können auch die Verbindung zu einer Remoteanwendung trennen, sodass die Remoteanwendung geöffnet bleibt.

Wenn Sie mit dem Remote-Desktop oder der Remoteanwendung verbunden sind, können Sie die Verbindung trennen, indem Sie auf das Symbol **Verbindung trennen** in der Unity Touch-Sidebar tippen.

Hinweis Der Horizon-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.

Abmelden von einem Remote-Desktop

Sie können sich von einem Remote-Desktop-Betriebssystem abmelden, selbst wenn Sie keinen Desktop in Horizon Client geöffnet haben.

Wenn Sie derzeit mit einem Remote-Desktop verbunden und dort angemeldet sind, können Sie sich über das **Startmenü** abmelden. Nachdem Windows Sie abgemeldet hat, wird die Desktop-Verbindung getrennt.

Hinweis Alle nicht gespeicherten Dateien, die auf dem Remote-Desktop geöffnet sind, werden beim Abmelden ohne vorheriges Speichern geschlossen.

Voraussetzungen

- Besorgen Sie sich die zur Anmeldung benötigten Informationen, so etwa den Active Directory-Benutzernamen und das Active Directory-Kennwort, den RSA SecurID-Benutzernamen und -Passcode oder den RADIUS-Authentifizierungsbenutzernamen oder -Passcode.
- Wenn Sie sich nicht mindestens ein Mal angemeldet haben, sollten Sie sich erst mit dem Vorgang „Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung“, auf Seite 18 vertraut machen.

Vorgehensweise

1 Tippen Sie auf der Registerkarte **Server** auf die Serververknüpfung.

2 Geben Sie auf Aufforderung entweder Ihren RSA-Benutzernamen und den Passcode oder Ihren Active Directory-Benutzernamen und das entsprechende Kennwort oder beides ein.

3 Tippen Sie in der Registerkarte **Alle** auf die Desktop-Verknüpfung und halten Sie diese, bis das Kontextmenü angezeigt wird.

   Ist der Desktop ein Favorit, können Sie diesen Schritt auch auf der Registerkarte **Favoriten** durchführen.

4 Tippen Sie im Kontextmenü auf **Abmelden**.

Weiter

Tippen Sie auf den Zurück-Pfeil in der oberen linken Ecke des Horizon Client-Fensters oder auf das Symbol **Trennen** in der in der oberen rechten Ecke des Horizon Client-Fensters und tippen Sie anschließend auf **Abmelden**, um die Verbindung zum Server zu trennen.

Verwalten von Desktop- und Anwendungsverknüpfungen

Nachdem Sie eine Verbindung zu einem Remote-Desktop oder einer Remoteanwendung hergestellt haben, speichert Horizon Client eine Verknüpfung für den zuletzt verwendeten Desktop bzw. die zuletzt verwendete Anwendung. Diese Verknüpfungen können Sie neu anordnen und entfernen.

Vorgehensweise

- Führen Sie diese Schritte aus, um eine Desktop- oder Anwendungsverknüpfung aus der Registerkarte **Zuletzt verwendet** zu entfernen.

  a Tippen Sie auf die Verknüpfung und halten Sie diese gedrückt, bis **Verknüpfung entfernen** am unteren Fensterrand angezeigt wird.

  b Ziehen Sie die Verknüpfung auf **Verknüpfung entfernen**.

- Wenn Sie eine Desktop- oder Anwendungsverknüpfung verschieben möchten, ziehen Sie das Element an die neue Position.

Verwenden eines Remote-Desktops oder einer Remoteanwendung auf einem Chrome OS-Gerät

3

Auf Chrome OS-Geräten verfügt Horizon Client über zusätzliche Funktionen zur Unterstützung der Navigation.

Dieses Kapitel behandelt die folgenden Themen:

Funktionsunterstützungs-Matrix

Wenn Sie aus Horizon Client für Chrome OS auf einen Remote-Desktop zugreifen, stehen einige Funktionen nicht zur Verfügung.

Tabelle 3-1. Auf Windows-Desktops für Chrome OS Horizon Client unterstützte Funktionen

Funktion	Windows 10-Desktop	Windows 8.x-Desktop	Windows 7-Desktop	Windows XP-Desktop	Windows Vista-Desktop	Windows Server 2008/2012 R2- oder Windows Server 2016-Desktop
RSA SecurID oder RADIUS	X	X	X	Begrenzt	Begrenzt	X
Einmaliges Anmelden	X	X	X	Begrenzt	Begrenzt	X
RDP-Anzeigeprotokoll						
PCoIP-Anzeigeprotokoll	X	X	X	Begrenzt	Begrenzt	X
VMware Blast-Anzeigeprotokoll	X	X	X			X
USB-Umleitung						

Tabelle 3-1. Auf Windows-Desktops für Chrome OS Horizon Client unterstützte Funktionen (Fortsetzung)

Funktion	Windows 10-Desktop	Windows 8.x-Desktop	Windows 7-Desktop	Windows XP-Desktop	Windows Vista-Desktop	Windows Server 2008/2012 R2- oder Windows Server 2016-Desktop
Clientlaufwerksumleitung						
Echtzeit-Audio/Video (nur Audio-Eingang)	X	X	X			X
Wyse MMR						
Windows 7 MMR						
Virtuelles Drucken						
Standortbasierter Druck	X	X	X	Begrenzt	Begrenzt	X
Smartcards						
Mehrere Monitore	X	X	X	Begrenzt	Begrenzt	X

Windows 10-Desktops erfordern View Agent 6.2 oder höher oder Horizon Agent 7.0 oder höher. Windows Server 2012 R2-Desktops erfordern View Agent 6.1 oder höher. Windows Server 2016-Desktops erfordern Horizon Agent 7.0.2 oder höher.

Wichtig Windows XP- und Windows Vista-Desktops werden von View Agent 6.1 und höher und von Horizon Agent 7.0 oder höher nicht unterstützt. View Agent 6.0.2 ist die letzte Version von View, die diese Gastbetriebssysteme unterstützt. Kunden, die über einen Vertrag mit Microsoft über erweiterten Support für Windows XP und Windows Vista sowie über einen Vertrag mit VMware über erweiterten Support für diese Gastbetriebssysteme verfügen, können View Agent 6.0.2 ihrer Windows XP- und Windows Vista-Desktops mit Verbindungsserver 6.1 bereitstellen.

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

Funktionsunterstützung für veröffentlichte Desktops auf RDS-Hosts

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

Hinweis Die folgende Tabelle enthält nur Zeilen für die unterstützten Funktionen. Wenn im Text Mindestversionen von View Agent festgelegt sind, gilt die Angabe „und höher“ auch für Horizon Agent 7.0.x und höher.

Tabelle 3-2. Unterstützte Funktionen für RDS-Hosts mit installiertem View Agent 6.0.x oder höher oder mit Horizon Agent 7.0.x oder höher

Funktion	Windows Server 2008 R2 RDS-Host	Windows Server 2012 RDS-Host	Windows Server 2016 RDS-Host
RSA SecurID oder RADIUS	X	X	Horizon Agent 7.0.2 und höher
Einmaliges Anmelden	X	X	Horizon Agent 7.0.2 und höher
PCoIP-Anzeigeprotokoll	X	X	Horizon Agent 7.0.2 und höher

Tabelle 3-2. Unterstützte Funktionen für RDS-Hosts mit installiertem View Agent 6.0.x oder höher oder mit Horizon Agent 7.0.x oder höher (Fortsetzung)

Funktion	Windows Server 2008 R2 RDS-Host	Windows Server 2012 RDS-Host	Windows Server 2016 RDS-Host
VMware Blast-Anzeigeprotokoll	Horizon Agent 7.0 und höher	Horizon Agent 7.0 und höher	Horizon Agent 7.0.2 und höher
HTML Access	View Agent 6.0.2 und höher (nur virtuelle Maschine)	View Agent 6.0.2 und höher (nur virtuelle Maschine)	Horizon Agent 7.0.2 und höher
Virtueller Druck (für Desktop-Clients)	View Agent 6.0.1 und höher (nur virtuelle Maschine)	View Agent 6.0.1 und höher (nur virtuelle Maschine)	Horizon Agent 7.0.2 und höher (nur virtuelle Maschine)
Standortbasierter Druck	View Agent 6.0.1 und höher (nur virtuelle Maschine)	View Agent 6.0.1 und höher (nur virtuelle Maschine)	Horizon Agent 7.0.2 und höher (nur virtuelle Maschine)
Mehrere Monitore (für Desktop-Clients)	X	X	Horizon Agent 7.0.2 und höher
Unity Touch (für mobile und Chrome OS-Clients)	X	X	Horizon Agent 7.0.2 und höher
Echtzeit-Audio/Video (RTAV)	Horizon Agent 7.0.2 und höher	Horizon Agent 7.0.2 und höher	Horizon Agent 7.0.3 und höher

Informationen darüber, welche Editionen bzw. Service Packs der einzelnen Gastbetriebssysteme unterstützt werden, finden Sie im Dokument *View-Installation*.

Informationen zu den Anforderungen für Echtzeit-Audio/Video (RTAV, Real-Time Audio Video) finden Sie unter „Systemanforderungen für Echtzeit-Audio/Video“, auf Seite 8.

Gesten

VMware hat Benutzerinteraktionshilfen erstellt, die Ihnen dabei helfen, in Elementen von konventionellen Windows-Benutzeroberflächen auf einem Nicht-Windows-Gerät zu navigieren.

Klicken

Wie bei anderen Anwendungen können Sie auf Ihren Touchpad tippen, um auf ein Element der Benutzeroberfläche zu klicken. Wenn Ihr Chrome OS-Gerät über einen Touchscreen verfügt, können Sie durch Berühren auf ein Element der Benutzeroberfläche klicken. Es lässt sich auch eine externe Maus verwenden.

Rechtsklicken

Die folgenden Optionen stehen zum Rechtsklicken zur Verfügung:

- Tippen Sie mit zwei Fingern auf das Touchpad.
- Halten Sie die Alt-Taste auf der Tastatur gedrückt und tippen Sie auf das Touchpad mit einem Finger.
- Für den Rechtsklick verwenden Sie eine externe Maus.
- Wenn Ihr Chrome OS-Gerät über einen Touchscreen verfügt, tippen Sie mit zwei Fingern nahezu gleichzeitig darauf. Zum Rechtsklick kommt es an der Stelle, wo der erste Finger getippt hat.

Rollen und Scrollbalken

Für das vertikale Rollen stehen die folgenden Optionen zur Verfügung.

- Tippen Sie mit Ihrem Daumen, halten Sie diesen an der Stelle und führen Sie dann mit einem Finger auf dem Touchpad einen Bildlauf nach unten aus. Sie können auch mit zwei Fingern einen Bildlauf ausführen.
- Für den Bildlauf verwenden Sie eine externe Maus.
- Wenn Ihr Chrome OS-Gerät über einen Touchscreen verfügt, tippen Sie mit einem oder zwei Fingern und ziehen Sie dann, um einen Bildlauf auszuführen. Der Text unter Ihren Fingern bewegt sich in dieselbe Richtung wie Ihre Finger. Das Rollen mit einem Finger funktioniert nicht, wenn Sie die Zoomfunktion verwenden oder wenn die Bildschirmtastatur angezeigt wird.

Vergrößern und Verkleinern

Wie bei anderen Anwendungen können Sie auch Ihre Tastatur verwenden und mit Strg plus + die Anzeige vergrößern sowie mit Strg plus - verkleinern. Wenn Ihr Chrome OS-Gerät über einen Touchscreen verfügt, können Sie durch pinzettenartiges Auseinanderziehen Ihrer Finger die Darstellung vergrößern und durch Zusammenziehen verkleinern.

Ändern der Größe von Fenstern

Um Ihr Touchpad zur Vergrößerung bzw. Verkleinerung eines Fensters zu verwenden, berühren Sie eine Ecke oder Seite des Fensters, halten Sie den Finger an dieser Position und führen Sie dann eine Ziehbewegung aus, um die Größenänderung vorzunehmen. Wenn Ihr Chrome OS-Gerät über eine externe Maus verfügt, positionieren Sie Ihren Cursor am Fensterrand und ziehen Sie diesen, um das Fenster zu vergrößern oder zu verkleinern. Sie können die Größe des Fensters nicht ändern, wenn es maximiert ist.

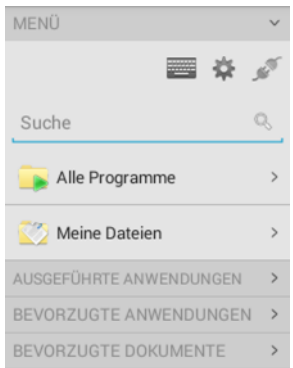
Ton, Musik und Video

Wenn der Ton für Ihr Gerät eingeschaltet ist, können Sie auf einem Remote-Desktop Audiodateien abspielen.

Verwenden der Unity Touch-Sidebar mit einem Remote-Desktop

Sie können von einer Unity Touch-Sidebar aus schnell zu einer Remote-Desktop-Anwendung oder -Datei navigieren. Über diese Sidebar können Sie auf einem Remote-Desktop Dateien und Anwendungen öffnen, zwischen laufenden Anwendungen umschalten sowie Fenster und Anwendungen minimieren, maximieren, wiederherstellen oder schließen.

Abbildung 3-1. Unity Touch-Sidebar für einen Remote-Desktop



Von dieser Sidebar aus können Sie viele Aktionen an einer Datei oder Anwendung ausführen.

Tabelle 3-3. Aktionen der Unity Touch-Sidebar für einen Remote-Desktop

Aktion	Prozedur
Ein- oder ausblenden der Bildschirmtastatur	Tippen Sie auf das Symbol **Tastatur**.
Ändern der Horizon Client-Einstellungen	Tippen Sie auf das Symbol **Einstellungen**.
Trennen der Verbindung mit dem Desktop	Tippen Sie auf das Symbol **Verbindung trennen**.
Anzeigen der Sidebar	Ziehen Sie die Sidebar nach rechts oder tippen Sie auf die Sidebar.
Ausblenden der Sidebar	Ziehen Sie die Sidebar nach links oder tippen Sie auf den Desktop-Bereich.
Navigieren zu einer Anwendung	Tippen Sie auf **Alle Programme** und navigieren Sie zur Anwendung, so wie Sie es im Windows-Startmenü tun würden.
Navigieren zu einer Datei	Tippen Sie auf **Meine Dateien**, um auf den Ordner `Benutzer` zuzugreifen, und navigieren Sie zu der Datei. **Meine Dateien** enthält Ordner wie `Meine Bilder`, `Meine Dokumente` und `Downloads`. **Meine Dateien** enthält die Ordner im Benutzerprofil (Verzeichnis `% USERPROFILE%`). Wenn Sie den Ordner `System` in das Verzeichnis `%USERPROFILE%` verschieben, können im Menü **Meine Dateien** auch Inhalte aus dem verschobenen Ordner angezeigt werden; dabei ist es gleichgültig, ob es sich um einen lokal verschobenen Ordner oder eine Netzwerkfreigabe handelt.
Suche nach einer Anwendung oder Datei	■ Tippen Sie in das Feld **Suche** und geben Sie den Namen der Anwendung oder Datei ein. ■ Um die Spracheingabe zu verwenden, tippen Sie auf das Mikrofon auf der Tastatur. ■ Um eine Anwendung oder Datei zu starten, tippen Sie auf den Namen der Anwendung oder Datei in den Suchergebnissen. ■ Um zum Startseitenbildschirm der Sidebar zurückzukehren, tippen Sie auf **X**, um das Feld **Suche** zu schließen.
Öffnen einer Anwendung oder Datei	Tippen Sie auf den Namen der Datei oder Anwendung in der Sidebar. Die Anwendung startet und die Sidebar wird geschlossen.
Umschalten zwischen laufenden Anwendungen oder offenen Fenstern	Tippen Sie auf den Namen der Anwendung unter **Ausgeführte Anwendungen**. Wenn mehr als eine Datei für eine Anwendung geöffnet ist, tippen Sie auf das Zeichen **>** neben der Anwendung, um die Liste zu erweitern.
Minimieren einer laufenden Anwendung oder eines Fensters	Tippen Sie auf den Namen der Anwendung unter **Ausgeführte Anwendungen** und halten Sie diesen, bis das Kontextmenü angezeigt wird. Tippen Sie auf **Minimieren**.
Maximieren einer laufenden Anwendung oder eines Fensters	Tippen Sie auf den Namen der Anwendung unter **Ausgeführte Anwendungen** und halten Sie diesen, bis das Kontextmenü angezeigt wird. Tippen Sie auf **Maximieren**.
Schließen einer laufenden Anwendung oder eines Fensters	Tippen Sie auf den Namen der Anwendung unter **Ausgeführte Anwendungen** und halten Sie diesen, bis das Kontextmenü angezeigt wird. Tippen Sie auf **Schließen**.
Wiederherstellen der vorherigen Größe und Position einer laufenden Anwendung oder eines Fensters	Tippen Sie auf den Namen der Anwendung unter **Ausgeführte Anwendungen** und halten Sie diesen, bis das Kontextmenü angezeigt wird. Tippen Sie auf **Wiederherstellen**.
Erstellen einer Liste der beliebtesten Anwendungen oder Dateien	1 Suchen Sie nach der Anwendung oder Datei, oder tippen Sie in der Liste **Favoriten-Anwendungen** oder **Bevorzugte Dokumente** auf **Verwalten**. Wenn die Leiste **Verwalten** nicht angezeigt wird, tippen Sie auf **>** neben **Favoriten-Anwendungen** oder **Bevorzugte Dateien**. 2 Tippen Sie in der Liste mit den Suchergebnissen oder in der Liste mit verfügbaren Anwendungen oder Dateien auf das Kontrollkästchen neben den Namen Ihrer Favoriten. Der zuletzt hinzugefügte Favorit wird am Anfang der Favoritenliste angezeigt.

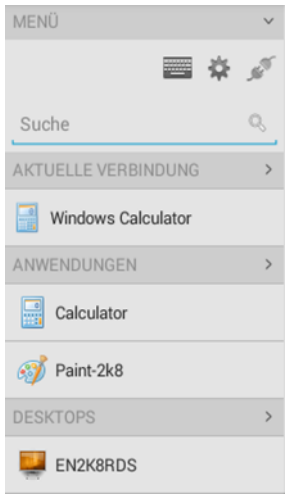
Tabelle 3-3. Aktionen der Unity Touch-Sidebar für einen Remote-Desktop (Fortsetzung)

Aktion	Prozedur
Entfernen einer Anwendung oder Datei aus der Favoritenliste	1 Suchen Sie nach der Anwendung oder Datei, oder tippen Sie in der Liste **Favoriten-Anwendungen** oder **Bevorzugte Dokumente** auf **Verwalten**. Wenn die Leiste **Verwalten** nicht angezeigt wird, tippen Sie auf **>** neben **Favoriten-Anwendungen** oder **Bevorzugte Dokumente**. 2 Tippen Sie, um das Häkchen neben dem Namen der Anwendung oder Datei in der Favoritenliste zu entfernen.
Neuanordnen einer Anwendung oder Datei in der Favoritenliste	1 Tippen Sie auf **Verwalten** unter **Favoriten-Anwendungen** oder unter **Bevorzugte Dokumente**. Wenn die Leiste **Verwalten** nicht angezeigt wird, tippen Sie auf **>** neben **Favoriten-Anwendungen** oder **Bevorzugte Dokumente**. 2 Berühren und halten Sie in der Favoritenliste den Ziehpunkt auf der linken Seite des Anwendungs- oder Dateinamens. Ziehen Sie dann den Favoriten in der Liste nach oben oder unten.

Verwenden der Unity Touch-Sidebar mit einer Remoteanwendung

Sie können von einer Unity Touch-Sidebar aus schnell zu einer Remoteanwendung navigieren. Über diese Sidebar können Sie Anwendungen starten, zwischen laufenden Anwendungen umschalten sowie Remoteanwendungen minimieren, maximieren, wiederherstellen oder schließen. Sie können auch zu einem Remote-Desktop wechseln.

Abbildung 3-2. Unity Touch-Sidebar für eine Remoteanwendung



Von der Unity Touch-Sidebar aus können Sie viele Aktionen für eine Remoteanwendung ausführen.

Tabelle 3-4. Aktionen der Unity Touch-Sidebar für eine Remoteanwendung

Aktion	Prozedur
Ein- oder ausblenden der Bildschirmtastatur	Tippen Sie auf das Symbol **Tastatur**.
Ändern der Horizon Client-Einstellungen	Tippen Sie auf das Symbol **Einstellungen**.
Trennen der Verbindung mit der Anwendung	Tippen Sie auf das Symbol **Verbindung trennen**.
Anzeigen der Sidebar	Ziehen Sie die Sidebar nach rechts oder tippen Sie auf die Sidebar. Bei geöffneter Sidebar können Sie im Anwendungsfenster keine Aktionen ausführen.

Tabelle 3-4. Aktionen der Unity Touch-Sidebar für eine Remoteanwendung (Fortsetzung)

Aktion	Prozedur
Ausblenden der Sidebar	Ziehen Sie die Sidebar nach links oder tippen Sie auf den Anwendungsbereich. Bei geöffneter Sidebar können Sie im Anwendungsfenster keine Aktionen ausführen.
Wechseln zwischen ausgeführten Anwendungen	Tippen Sie auf die Anwendung unter **Aktuelle Verbindung**.
Öffnen einer Anwendung	Tippen Sie auf den Namen der Anwendung unter **Anwendungen** auf der Sidebar. Die Anwendung startet und die Sidebar wird geschlossen.
Schließen einer laufenden Anwendung	1 Tippen Sie unter **Aktuelle Verbindung** auf den Namen der Anwendung und halten Sie diesen, bis das Kontextmenü angezeigt wird. 2 Tippen Sie auf **Schließen**.
Minimieren einer laufenden Anwendung	1 Tippen Sie unter **Aktuelle Verbindung** auf den Namen der Anwendung und halten Sie diesen, bis das Kontextmenü angezeigt wird. 2 Tippen Sie auf **Minimieren**.
Maximieren einer laufenden Anwendung	1 Tippen Sie unter **Aktuelle Verbindung** auf den Namen der Anwendung und halten Sie diesen, bis das Kontextmenü angezeigt wird. 2 Tippen Sie auf **Maximieren**.
Wiederherstellen einer laufenden Anwendung	1 Tippen Sie unter **Aktuelle Verbindung** auf den Namen der Anwendung und halten Sie diesen, bis das Kontextmenü angezeigt wird. 2 Tippen Sie auf **Wiederherstellen**.
Wechseln zu einem Remote-Desktop	Tippen Sie auf den Namen des Desktops unter **Desktops**.

Verwenden der Bildschirmtastatur

Sie haben die Möglichkeit, in einem Remote-Desktop oder in einer Remoteanwendung eine Bildschirmtastatur zu verwenden. Um die Bildschirmtastatur darzustellen, tippen Sie auf das Symbol **Tastatur** in der Unity Touch-Sidebar. Um die Bildschirmtastatur wieder auszublenden, tippen Sie erneut auf das Symbol **Tastatur**.

Zur Bildschirmtastatur gehören die Steuerungstasten BildAuf und BildAb, Funktionstasten und andere Tasten, die in Windows-Umgebungen häufig benutzt werden wie Strg, Alt, Entf, Umschalttaste, Win, Feststelltaste und Esc. Verwenden Sie die Umschalttaste auf dieser Tastatur, wenn Sie Tastenkombinationen verwenden möchten, die die Umschalttaste enthalten, z. B. Strg+Umschalt. Um eine Kombination dieser Tasten zu tippen, z. B. Strg+Alt+Umschalttaste, tippen Sie zuerst auf die Strg-Taste auf dem Bildschirm. Nachdem die Strg-Taste blau geworden ist, tippen Sie auf die Alt-Taste auf dem Bildschirm. Nachdem die Alt-Taste blau geworden ist, tippen Sie auf die Umschalttaste auf dem Bildschirm. Die Tastenkombination Strg+Alt+Entf wird als eine Bildschirmtaste angezeigt.

Sie können auf das Stiftsymbol auf der linken Seite der Strg-Taste tippen, um den lokalen Eingabepuffer anzuzeigen. Von Ihnen in dieses Textfeld eingegebener Text wird erst dann an eine Anwendung gesendet, wenn Sie auf **Senden** tippen. Wenn Sie z. B. eine Anwendung wie Editor öffnen und auf das Stiftsymbol tippen, wird der Text erst dann in Editor übernommen, wenn Sie auf **Senden** tippen. Diese Funktion ist bei einer schwachen Netzwerkverbindung hilfreich, wenn die Zeichen nicht sofort nach der Eingabe erscheinen. Mit dieser Funktion können Sie schnell bis zu 1.000 Zeichen eingeben und dann entweder auf **Senden** oder auf **Enter** tippen, damit alle Zeichen gemeinsam in die Anwendung übernommen werden.

Bildschirmauflösungen und Verwendung externer Anzeigen

Sie können Horizon Client mit externen Bildschirmen verwenden und die Bildschirmauflösung lässt sich ebenfalls ändern.

Wenn Sie Ihr Chrome OS-Gerät mit einem externen Anzeigegerät oder Projektor verbinden, können Sie Horizon Client im Vollbildmodus anzeigen, indem Sie auf Ihrer Tastatur auf die entsprechende Taste drücken.

Vergrößern der Bildschirmauflösung für Remote-Desktops

Standardmäßig ist die Anzeigeauflösung so eingestellt, dass der gesamte Windows-Desktop auf Ihrem Gerät angezeigt wird und die Desktop- und Taskleistensymbole eine bestimmte Größe aufweisen. Wenn Sie den Standardwert in eine höhere Auflösung ändern, wird der Desktop weiterhin auf dem Gerät angezeigt, nur die Desktop- und Taskleistensymbole werden kleiner.

Ändern der Einstellung für die Anzeigeauflösung

Zur Änderung der Auflösungseinstellungen tippen Sie auf das Symbol **Einstellungen** in der oberen rechten Ecke des Horizon Client-Fensters, dann auf **Anzeige** und schließlich auf **Auflösung**.

Verwenden von Projektoren

Sie können mit der Einstellung **Auflösung** auch eine größere Auflösung für Projektoren festlegen.

Verwenden der Funktion für mehrere Monitore

Mit der Funktion für mehrere Monitore können Sie einen Remote-Desktop auf einen externen Monitor erweitern. Erläuterungen zur Aktivierung der Funktion für mehrere Monitore finden Sie unter „Aktivieren der Funktion für mehrere Monitore für Horizon Client“, auf Seite 12.

Verwenden der Echtzeit-Audio/Video-Funktion für Mikrofone

Mit der Echtzeit-Audio/Video-Funktion können Sie ein Mikrofon, das mit Ihrem Mobilgerät verbunden ist, auf Ihrem Remote-Desktop verwenden. Die Echtzeit-Audio/Video-Funktion ist mit Standardaudiogeräten sowie mit Standardkonferenzanwendungen wie Skype, WebEx und Google Hangouts kompatibel.

Die Echtzeit-Audio/Video-Funktion wird standardmäßig bei der Installation von Horizon Client auf Ihrem Gerät installiert.

Hinweis Es wird nur die Audio-Eingangs-Funktion unterstützt. Die Video-Funktion wird nicht unterstützt.

Informationen zur Einrichtung der Echtzeit-Audio/Video-Funktion auf einem Remote-Desktop finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Speichern von Dokumenten in einer Remoteanwendung

Sie können mit bestimmten Remoteanwendungen, z. B. Microsoft Word oder WordPad, Dokumente erstellen und speichern. Der Speicherort für diese Dokumente hängt von der Netzwerkumgebung Ihres Unternehmens ab. Beispielsweise können die Dokumente in einer Basisfreigabe gespeichert werden, die auf Ihrem lokalen Computer gemountet wird.

Administratoren können anhand einer ADMX-Vorlagendatei eine Gruppenrichtlinie zur Angabe des Speicherorts für Dokumente einrichten. Hierbei handelt es sich um die Richtlinie **Basisverzeichnis für Remote-Desktop-Dienste-Benutzer festlegen**. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Internationalisierung

Die Benutzeroberfläche und die Dokumentation sind in den Sprachen Englisch, Japanisch, Französisch, Deutsch, vereinfachtes Chinesisch, traditionelles Chinesisch, Koreanisch und Spanisch verfügbar. Sie können auch Zeichen für diese Sprachen eingeben.

Fehlerbehebung für Horizon Client 4

Die meisten Probleme mit Horizon Client lassen sich durch Zurücksetzen oder Neuinstallieren der App beheben.

Dieses Kapitel behandelt die folgenden Themen:

Neustarten eines Remote-Desktops

Eventuell muss ein Remote-Desktop neu gestartet werden, wenn das Desktop-Betriebssystem nicht mehr reagiert. Der Neustart eines Remote-Desktops entspricht dem Neustart des Windows-Betriebssystems. In der Regel werden Sie dabei vom Desktop-Betriebssystem aufgefordert, alle nicht gespeicherten Daten zu speichern, bevor der Neustart erfolgt.

Sie können einen Remote-Desktop nur dann neu starten, wenn ein Horizon-Administrator die Funktion zum Neustart eines Desktops für den Desktop aktiviert hat.

Informationen zur Aktivierung der Funktion zum Neustart eines Desktops finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Voraussetzungen

- Besorgen Sie sich die Anmeldedaten, etwa einen Active Directory-Benutzernamen und das zugehörige Kennwort, den RSA SecurID-Benutzernamen und -Passcode oder den RADIUS-Authentifizierungsbenutzernamen oder -Passcode.
- Wenn Sie sich nicht mindestens ein Mal angemeldet haben, sollten Sie sich erst mit dem Vorgang „Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung“, auf Seite 18 vertraut machen.

Vorgehensweise

1 In der Registerkarte **Server** tippen Sie auf die Serververknüpfung, um eine Verbindung mit dem Server herzustellen.

2 Geben Sie auf Aufforderung entweder Ihren RSA-Benutzernamen und den Passcode oder Ihren Active Directory-Benutzernamen und das entsprechende Kennwort oder beides ein.

3 Berühren und halten Sie den Desktop-Namen, bis das Kontextmenü angezeigt wird.

Sie können diesen Schritt entweder von der Registerkarte **Alle** oder **Favoriten** aus durchführen.

4 Tippen Sie im Kontextmenü auf **Neu starten**.

Die Option **Neu starten** ist nur verfügbar, wenn sich der Desktop in einem Status befindet, in dem diese Aktion vorgenommen werden kann.

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

Weiter

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

Wenn das Problem durch den Neustart des Remote-Desktops nicht behoben werden kann, müssen Sie den Remote-Desktop eventuell zurücksetzen. Siehe „Zurücksetzen eines Remote-Desktops oder von Remoteanwendungen“, auf Seite 34.

Zurücksetzen eines Remote-Desktops oder von Remoteanwendungen

Sie müssen einen Remote-Desktop eventuell zurücksetzen, wenn das Betriebssystem nicht mehr reagiert und der Neustart des Remote-Desktops das Problem nicht löst. Durch das Zurücksetzen von Remoteanwendungen werden alle geöffneten Anwendungen beendet.

Das Zurücksetzen eines Remote-Desktops entspricht dem Betätigen der Reset-Taste auf einem physischen Computer, mit der der Neustart des Computers erzwungen wird. Alle Dateien, die auf dem Remote-Desktop geöffnet sind, werden geschlossen und nicht gespeichert.

Das Zurücksetzen von Remoteanwendungen entspricht dem Beenden der Anwendungen, ohne nicht gespeicherte Daten zu speichern. Alle geöffneten Anwendungen werden geschlossen, auch die Anwendungen, die zu verschiedenen RDS-Server-Farmen gehören.

Sie können einen Remote-Desktop nur zurücksetzen, wenn ein Horizon-Administrator die Funktion zum Zurücksetzen eines Desktops für den Desktop aktiviert hat.

Informationen zur Aktivierung der Funktion zum Zurücksetzen eines Desktops finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Voraussetzungen

- Besorgen Sie sich die Anmeldedaten, etwa einen Active Directory-Benutzernamen und das zugehörige Kennwort, den RSA SecurID-Benutzernamen und -Passcode oder den RADIUS-Authentifizierungsbenutzernamen oder -Passcode.
- Wenn Sie sich nicht mindestens ein Mal angemeldet haben, sollten Sie sich erst mit dem Vorgang „Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung“, auf Seite 18 vertraut machen.

Vorgehensweise

1 Tippen Sie auf der Registerkarte **Server** auf die Serververknüpfung, um eine Verbindung mit dem Server herzustellen.

2 Geben Sie auf Aufforderung entweder Ihren RSA-Benutzernamen und den Passcode oder Ihren Active Directory-Benutzernamen und das entsprechende Kennwort oder beides ein.

3 Berühren und halten Sie den Namen des Desktops oder der Anwendung, bis das Kontextmenü angezeigt wird.

Sie können diesen Schritt entweder von der Registerkarte **Alle** oder **Favoriten** aus durchführen.

4 Tippen Sie im Kontextmenü auf **Zurücksetzen**.

Zurücksetzen ist nur verfügbar, wenn sich der Desktop bzw. die Anwendung in einem Status befindet, in dem diese Aktion vorgenommen werden kann.

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

Weiter

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

Deinstallieren von Horizon Client

Manchmal können Sie Probleme mit Horizon Client beheben, indem Sie Horizon Client für Chrome OS deinstallieren und neu installieren.

Sie können Horizon Client für Chrome OS wie jede andere Chrome OS-App deinstallieren.

Vorgehensweise

- Auf Ihrem Chrome OS-Gerät tippen Sie auf das App Launcher-Symbol in der Taskleiste, klicken mit der rechten Maustaste auf das App-Symbol von **Horizon Client für Chrome OS** und wählen im eingeblendeten Kontextmenü die Option **Deinstallieren**.

Weiter

Installieren Sie Horizon Client erneut.

Siehe „Installieren oder Aktualisieren von Horizon Client für Chrome OS“, auf Seite 11.

Horizon Client oder der Remote-Desktop reagiert nicht mehr

Wenn das Fenster nicht mehr reagiert, versuchen Sie zunächst, das Betriebssystem des Remote-Desktops zurückzusetzen.

Problem

Horizon Client funktioniert nicht oder wird mehrmals unerwartet beendet oder der Remote-Desktop reagiert nicht mehr.

Ursache

Vorausgesetzt, dass die Horizon-Server richtig konfiguriert sind und bei den umgebenden Firewalls die richtigen Ports geöffnet sind, beziehen sich andere Probleme meist auf Horizon Client auf dem Endgerät oder auf das Gastbetriebssystem auf dem Remote-Desktop.

Lösung

- Wenn das Betriebssystem im Remote-Desktop nicht mehr reagiert, verwenden Sie Horizon Client auf dem Gerät, um den Desktop zurückzusetzen.

  Diese Option ist nur verfügbar, wenn der Horizon-Administrator diese Funktion aktiviert hat.
- Deinstallieren Sie die App und installieren Sie sie neu auf dem Gerät.
- Falls das Zurücksetzen des Remote-Desktops und das Neuinstallieren von Horizon Client nicht helfen, können Sie das Chrome OS-Gerät zurücksetzen, wie im Benutzerhandbuch für Ihr Gerät beschrieben.
- Wenn Sie beim Versuch, eine Verbindung zum Server herzustellen, ein Verbindungsfehler erhalten, müssen Sie möglicherweise Ihre Proxy-Einstellungen ändern.

Probleme beim Herstellen einer Verbindung bei Verwendung eines Proxys

Manchmal wird bei dem Versuch, in einem LAN über einen Proxy eine Verbindung mit dem Verbindungsserver herzustellen, ein Fehler angezeigt.

Problem

Wenn die Horizon-Umgebung so eingerichtet ist, dass eine sichere Verbindung vom Remote-Desktop zum Verbindungsserver verwendet wird, und das Clientgerät zur Verwendung eines HTTP-Proxys konfiguriert ist, können Sie eventuell keine Verbindung herstellen.

Ursache

Im Gegensatz zum Windows Internet Explorer verfügt das Clientgerät nicht über eine Internetoption, mit der die Proxyserver-Konfiguration für lokale Adressen umgangen werden kann. Bei Verwendung eines HTTP-Proxys für das Browsen externer Adressen und dem Versuch einer Verbindungsherstellung mit dem Verbindungsserver über eine interne Adresse wird eventuell die Fehlermeldung `Verbindung konnte nicht hergestellt werden` angezeigt.

Lösung

- Entfernen Sie die Proxy-Einstellungen, sodass das Gerät keinen Proxy mehr verwendet.

Index

V

Z