Verwenden von VMware Horizon Client für Windows 10 UWP

VMware Horizon Client for Windows 10 UWP 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-002509-00

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 Windows 10 UWP

1

Das Handbuch *Verwenden von VMware Horizon Client für Windows 10 UWP* bietet Informationen zur Installation und Verwendung der VMware Horizon® Client™-Software auf einem Windows 10-Gerät zur Herstellung einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung im Datencenter.

Diese Informationen sind für Administratoren vorgesehen, die eine Bereitstellung von Horizon mit Windows 10-Clientgeräten ermöglichen müssen. Die Informationen wurden für erfahrene Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen sowie mit Datencenter-Vorgängen vertraut sind.

Konfiguration und Installation 2

Bei der Einrichtung einer Horizon -Bereitstellung für Windows 10 UWP-Clients müssen bestimmte Verbindungsservereinstellungen verwendet, die Systemanforderungen für Horizon Server und Windows 10-Geräteclients erfüllt und die VMware Horizon ClientWindows-App installiert werden.

Dieses Kapitel behandelt die folgenden Themen:

Systemanforderungen

Das Gerät, auf dem Sie Horizon Client sowie die von ihm verwendeten Peripheriegeräte installieren, müssen bestimmte Systemanforderungen erfüllen.

Betriebssysteme	■ Windows 10 Current Branch (CB) Version 1703 (Creators Update) ■ Windows 10 Current Branch (CB) Version 1607 (Anniversary Update) ■ Windows 10 Current Branch for Business (CBB) Version 1607 (Anniversary Update) ■ Windows 10 Long-Term Servicing Branch (LTSB) Version 1607 (Anniversary Update)
Windows Hello-Authentifizierung	Siehe „Anforderungen für die Windows Hello-Authentifizierung“, auf Seite 8.

Verbindungsserver, Sicherheitsserver und 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.
Anzeigeprotokoll für Remote-Desktops und -anwendungen	■ VMware Blast (erfordert Horizon Agent 7.0 oder höher) ■ PCoIP

Anforderungen für die Windows Hello-Authentifizierung

Für die Verwendung von Windows Hello zur Authentifizierung in Horizon Clientmüssen bestimmte Anforderungen erfüllt sein.

Windows 10-Gerätemodelle	Jedes Windows 10-Gerät, das Windows Hello unterstützt, wie z. B. Microsoft Surface Pro 4.
Betriebssystemanforderungen	Richten Sie Windows Hello unter **Einstellungen > Konten > Anmeldeoptionen**ein.
Verbindungsserveranforderungen	■ Horizon 6 Version 6.2 oder eine höhere Version. ■ Aktivieren Sie die biometrische Authentifizierung im Verbindungsserver. Informationen dazu finden Sie unter „Konfigurieren der biometrischen Authentifizierung“ im Dokument *Administration von View*.
Horizon Client-Anforderungen	Aktivieren Sie Windows Hello durch Antippen von **Windows Hello aktivieren** im Anmeldedialogfeld des Servers. Nach der erfolgreichen Anmeldung werden Ihre Active Directory-Anmeldedaten sicher auf dem Windows 10-Gerät gespeichert. **Windows Hello aktivieren** wird bei der ersten Anmeldung und dann nicht mehr angezeigt, wenn Windows die Hello-Authentifizierung aktiviert ist.

Sie können die Windows-Hello-Authentifizierung als Teil der zweistufigen Authentifizierung mit der RSA SecurID- und RADIUS-Authentifizierung verwenden.

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*.
- 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 die Windows Hello-Authentifizierung zu verwenden, müssen Sie die biometrische Authentifizierung im Verbindungsserver aktivieren. Die biometrische Authentifizierung wird in Horizon 6 Version 6.2 und höher unterstützt. Weitere Informationen finden Sie im Dokument *Administration von View*.

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 der unterstützten Windows-Gastbetriebssysteme finden Sie unter „Unterstützte Betriebssysteme für Horizon Agent“ im Dokument *View-Installation*.

Installieren oder Aktualisieren von Horizon Client für Windows 10 UWP

Die VMware Horizon Client-App ist eine Windows 10 UWP-App, die Sie wie andere Windows 10 UWP-Apps installieren können.

Voraussetzungen

- Stellen Sie sicher, dass Ihr Clientgerät die Systemanforderungen für Horizon Client erfüllt. Siehe „Systemanforderungen“, auf Seite 7.
- Wenn Sie das Clientgerät noch nicht eingerichtet haben, so holen Sie dies nun nach. Siehe Bedienungsanleitung des Geräteherstellers.

Vorgehensweise

1. Öffnen Sie die Microsoft Store-App auf Ihrem Gerät und verwenden Sie Ihr Microsoft-Konto zur Anmeldung.
2. Suchen Sie nach der VMware Horizon Client-App.
3. Klicken Sie auf **Installieren** oder **Kostenlos**, um die VMware Horizon Client-App auf Ihrem Gerät zu installieren.

Speichern von Informationen über zuletzt benutzte Server im Horizon Client -Startfenster

Sie können Horizon Client so konfigurieren, dass auf der Startseite eine Serververknüpfung erstellt wird, wenn Sie zum ersten Mal eine Verbindung mit einem Server herstellen.

Vorgehensweise

1. Tippen Sie auf das Menü **Option** oben links auf der Menüleiste von Horizon Client.

   Wenn Sie mit einem Server verbunden sind, können Sie auf das Menü **Option** links oben im Auswahlfenster für Desktops und Anwendungen tippen. Wenn Sie mit einem Remote-Desktop oder einer Remoteanwendung verbunden sind, können Sie im Desktop- oder Anwendungsfenster auf die Schaltfläche **Option** tippen und dann auf **Einstellungen**.

2 Erweitern Sie den Abschnitt **Erweitert** und tippen Sie auf die Option **Informationen über letzte Server speichern**, um auf **Ein** umzuschalten.

Wenn für die Option **Aus** festgelegt ist, speichert Horizon Client die zuletzt benutzten Server nicht im Startfenster.

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 Menü **Option** links oben in der Horizon Client-Menüleiste und erweitern Sie den Abschnitt **SSL-Optionen**.

2 Zum Aktivieren oder Deaktivieren eines Sicherheitsprotokolls tippen Sie unter dem Namen des Sicherheitsprotokolls auf **Ein** bzw. **Aus**.

Sie können die Protokolle TLSv1.0, TLSv1.1 und TLSv1.2 aktivieren bzw. deaktivieren. Standardmäßig sind alle drei Protokolle aktiviert.

Hinweis Für TLSv1.0 und TLSv1.2 muss TLSv1.1 aktiviert sein. Sie können TLSv1.1 nicht deaktivieren, wenn TLSv1.0 und TLSv1.2 aktiviert sind.

---

3 Um die Schlüsselsteuerzeichenfolge zu ändern, ersetzen Sie die Standardzeichenfolge und tippen Sie auf **Ändern**.

4 (Optional) Falls Sie die standardmäßige Schlüsselsteuerzeichenfolge wiederherstellen müssen, tippen Sie auf **Standard**.

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

Konfigurieren der VMware Blast-Optionen

Sie können die Optionen für die H.264-Decodierung und für die Netzwerkbedingung für Remote-Desktop- und -anwendungssitzungen konfigurieren, die das VMware Blast-Anzeigeprotokoll verwenden.

Die Option für die Netzwerkbedingung lässt sich nach der Anmeldung bei einem Server nicht mehr ändern. Die H.264-Decodierung können Sie vor und nach der Anmeldung bei einem Server konfigurieren.

Voraussetzungen

Diese Funktion erfordert Horizon Agent 7.0 oder höher.

Vorgehensweise

1 Tippen Sie auf das Menü **Option** links oben in der Horizon Client-Menüleiste und erweitern Sie den Abschnitt **VMware Blast**.

Wenn Sie mit einem Server verbunden sind, tippen Sie auf das Menü **Option** links oben im Fenster für die Desktop- und Anwendungsauswahl, erweitern Sie den Abschnitt **Protokoll** und wählen Sie **VMware Blast** aus. Die Option für die Netzwerkbedingung lässt sich nach der Anmeldung bei einem Server nicht mehr ändern.

2 Konfigurieren Sie die Optionen für das Decodieren und die Netzwerkbedingung.

Option	Aktion
H.264-Decodierung zulassen	Sie können diese Option vor oder nach der Herstellung einer Verbindung mit dem Verbindungsserver konfigurieren, um die H.264-Decodierung in Horizon Client aktivieren. Ist diese Option ausgewählt (Standardeinstellung), verwendet Horizon Client die H.264-Decodierung, wenn der Agent die H.264-Software- oder -Hardwarecodierung unterstützt. Unterstützt der Agent die H.264-Software- oder -Hardwarecodierung nicht, verwendet Horizon Client die JPG/PNG-Decodierung. Deaktivieren Sie diese Option, um die JPG/PNG-Decodierung zu verwenden.
Netzwerkstatus auswählen, um optimale Funktion zu gewährleisten	Sie können diese Option nur vor der Herstellung einer Verbindung mit dem Verbindungsserver konfigurieren. Wählen Sie eine der folgenden Optionen für die Netzwerkbedingung aus: ■ **Hervorragend** – Horizon Client verwendet nur das TCP-Netzwerk. Diese Option ist am besten für eine LAN-Umgebung geeignet. ■ **Normal (Standard)** – Horizon Client arbeitet im gemischten Modus. Im gemischten Modus verwendet Horizon Client das TCP-Netzwerk für die Herstellung einer Verbindung mit dem Server und das Protokoll Blast Extreme Adaptive Transport (BEAT), wenn der Agent und das Blast Security Gateway (bei Aktivierung) eine BEAT-Konnektivität unterstützen. Diese Option ist die Standardeinstellung. ■ **Schlecht** – Horizon Client verwendet nur das BEAT-Netzwerk, wenn BEAT Tunnel Server auf dem Server aktiviert ist. Ist dies nicht der Fall, wird in den gemischten Modus gewechselt. **Hinweis** In Horizon 7 Version 7.1 und früher wird BEAT Tunnel Server von den Instanzen des Verbindungsservers und des Sicherheitsservers nicht unterstützt. Unified Access Gateway 2.9 und höher unterstützt BEAT Tunnel Server. Blast Security Gateway für Verbindungsserver- und Sicherheitsserver-Instanzen unterstützt nicht das BEAT-Netzwerk.

Anzeigen der Hilfe für Horizon Client

Um das Hilfesystem aus der App Horizon Client aufzurufen, tippen Sie auf das Menü **Option** links oben in der Menüleiste, dann auf das Info-Symbol (**!**) und schließlich auf den Link unter **Online-Hilfe**. Sie können das Hilfesystem auch nach der Herstellung einer Verbindung mit einem Server oder nach der Anmeldung bei einem Remote-Desktop oder einer Remoteanwendung aufrufen.

Dieses Hilfesystem nutzt Funktionen Ihres Webbrowsers sowie zusätzliche Eigenschaften, damit Sie auf Produktinformationen zugreifen können. Sie können die Hilfe mithilfe von Abfragen durchsuchen, die Anführungszeichen, Platzhalterzeichen und boolesche Operatoren enthalten.

Verwalten der Remote-Desktop- und -anwendungsverbindungen 3

Sie können mit Horizon Client eine Verbindung zu einem Server herstellen und sich bei Remote-Desktops und -anwendungen anmelden.

Je nachdem, wie ein 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:

- 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 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.

Wenn Ihr Administrator dies zulässt, können Sie den Zertifikatsprüfungsmodus festlegen. Tippen Sie im Horizon Client-Startfenster auf das Menü **Option** links oben in der Menüleiste und erweitern Sie den Abschnitt **Zertifikatsprüfungsmodus** . Sie haben folgende 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.
- **Versuch der Verbindung ungeachtet der Serveridentitätszertifikate**. Mit dieser Einstellung werden Zertifikate nicht überprüft.

Da der Zertifikatsmechanismus in Windows 10 UWP-Apps eingeschränkter ist als der für Windows-Desktop-Anwendungen, kann die Zertifikatsprüfung selbst dann fehlschlagen, wenn die Ebene auf **Versuch der Verbindung ungeachtet der Serveridentitätszertifikate** festgelegt ist. Beispielsweise kann die Zertifikatsprüfung aus den folgenden Gründen fehlschlagen:

- Das von der Stammzertifizierungsstelle signierte Zertifikat wurde widerrufen.
- Das von der Zwischenzertifizierungsstelle signierte Zertifikat wurde widerrufen.
- Das Zertifikat ist gültig, aber die Zwischenzertifizierungsstelle wurde widerrufen.
- Das Zertifikat in der Kette enthält eine unbekannte Erweiterung, die als „Kritisch“ markiert ist.

Auswählen eines Anzeigeprotokolls

Sie können das Anzeigeprotokoll für Horizon Client auswählen, wenn Sie eine Verbindung zu einem Remote-Desktop oder einer Remoteanwendung herstellen.

Vorgehensweise

1 Tippen Sie in Horizon Client auf das Menü **Option** links oben in der Horizon Client-Menüleiste.

  Wenn Sie mit einem Server verbunden sind, können Sie auf das Menü **Option** links oben im Auswahlfenster für Desktops und Anwendungen tippen.

2 Erweitern Sie den Abschnitt **Protokoll** und wählen Sie das Anzeigeprotokoll aus, das Sie verwenden möchten.

  VMware Blast erfordert Horizon Agent 7.0 oder höher.

3 (Optional) Wenn Sie **VMware Blast** ausgewählt haben, aktivieren oder deaktivieren Sie die H.264-Codierung durch Tippen und Umschalten der Option **H.264-Decodierung zulassen** auf **Ein** oder **Aus**.

  Wenn für diese Option **Ein** festgelegt ist, ermöglicht Horizon Client die H.264-Codierung, wenn Horizon Agent die H.264-Codierung für den Remote-Desktop oder die Remoteanwendung unterstützt. Wenn Horizon Agent die H.264-Codierung für den Remote-Desktop oder die Remoteanwendung nicht unterstützt, verwendet Horizon Client stattdessen die JPEG/PNG-Codierung. Ist für diese Option **Aus** festgelegt (Standardeinstellung) ist die H.264-Codierung nicht möglich. Horizon Client verwendet in diesem Fall immer die JPEG/PNG-Codierung.

Wenn Sie das nächste Mal eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung herstellen, verwendet Horizon Client das von Ihnen ausgewählte Anzeigeprotokoll. Sie können das Anzeigeprotokoll für eine aktuell verbundene Sitzung nicht ändern.

Wenn Sie eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung herstellen, der bzw. die das von Ihnen ausgewählte Anzeigeprotokoll nicht unterstützt, wird in Horizon Client eine Fehlermeldung eingeblendet.

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.

Für die Verwendung von Remoteanwendungen müssen Sie eine Verbindung mit dem Verbindungsserver der Version 6.0 oder höher herstellen.

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

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.
- Besorgen Sie sich den NETBIOS-Domänennamen für die Anmeldung. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.
- 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.

  Wenn Ihr Unternehmen ein internes WLAN besitzt, das über einen Router Zugriff auf Remote-Desktops ermöglicht, die von Ihrem Gerät genutzt werden können, brauchen Sie keinen Sicherheitsserver oder eine VPN-Verbindung einrichten.
- 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.
- Konfigurieren Sie den Zertifikatsprüfungsmodus für das SSL-Zertifikat, das vom Verbindungsserver präsentiert wird. Siehe „Festlegen des Zertifikatsprüfungsmodus für Horizon Client“, auf Seite 13.
- Wenn Sie Windows Hello zur Authentifizierung verwenden möchten, müssen Sie sicherstellen, dass Windows Hello auf Ihrem Windows 10-Gerät eingerichtet ist. Die vollständigen Informationen zu den Systemanforderungen finden Sie unter „Anforderungen für die Windows Hello-Authentifizierung“, auf Seite 8.

Vorgehensweise

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

2 Tippen Sie auf die App **VMware Horizon Client**.

3 Stellen Sie eine Verbindung mit einem Server her.

Option	Beschreibung
Verbindung mit einem neuen Server herstellen	Tippen Sie auf **Server hinzufügen**, geben Sie den Namen eines Servers ein und tippen Sie auf **Verbinden**.
Verbindung mit einem vorhandenen Server herstellen	Tippen Sie auf der Startseite auf das Serversymbol.

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-Anmeldedaten oder RADIUS-Authentifizierungsinformationen aufgefordert werden, geben Sie den Benutzernamen und den Passcode ein und tippen Sie auf **Anmelden**.

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

5 Wenn Sie zur Eingabe von Benutzername und Kennwort aufgefordert werden, geben Sie die Active Directory-Anmeldedaten ein.

a Geben Sie den Benutzernamen und das Kennwort eines Benutzers ein, der berechtigt ist, mindestens einen Desktop- oder Anwendungspool zu benutzen.

b Wählen Sie eine Domäne aus.

c (Optional) Wenn die Schaltfläche **Windows Hello aktivieren** aktiviert ist, tippen Sie darauf, um die Windows Hello-Authentifizierung zu verwenden.

Die Schaltfläche **Windows Hello aktivieren** ist nur verfügbar, wenn die biometrische Authentifizierung auf dem Server aktiviert ist und Sie sich nicht bereits mit Windows Hello authentifiziert haben.

d Tippen Sie auf **Anmelden**.

Wenn Windows Hello aktiviert ist und Sie sich zum ersten Mal anmelden, werden Ihre Active Directory-Anmeldedaten sicher auf Ihrem Windows 10-Gerät für die zukünftige Verwendung gespeichert.

6 Wenn Sie zur Windows Hello-Authentifizierung aufgefordert werden, verwenden Sie zur Authentifizierung Ihren Fingerabdruck, Ihr Gesicht, Ihre Iris oder die PIN.

Wenn Sie die Windows Hello-Authentifizierung nicht verwenden möchten, klicken Sie auf **Abbrechen**, um einen Benutzernamen und ein Kennwort einzugeben.

7 Tippen Sie zum Herstellen einer Verbindung mit einem Desktop oder einer Anwendung auf den Desktop bzw. die Anwendung.

Der Remote-Desktop bzw. die Remoteanwendung wird gestartet.

Deaktivieren von Windows-Hello in Horizon Client

Sie können Windows Hello für einen Server deaktivieren, bei dem Sie sich zuvor mit der Windows Hello-Authentifizierung angemeldet haben.

Voraussetzungen

Stellen Sie sicher, dass eine Verknüpfung für den Server im Horizon Client-Startfenster angezeigt wird. Erläuterungen zur Konfiguration von Horizon Client für das Speichern von Serververknüpfungen finden Sie unter „Speichern von Informationen über zuletzt benutzte Server im Horizon Client-Startfenster“, auf Seite 9.

Vorgehensweise

1 Tippen Sie im Horizon Client-Startfenster auf die Serververknüpfung und halten Sie diese gedrückt.

2 Wenn das Kontextmenü angezeigt wird, tippen Sie auf **Vom Server abmelden**.

Wenn Sie das nächste Mal eine Verbindung mit dem Server herstellen, können Sie einen Benutzernamen und das Kennwort eingeben. Die Schaltfläche **Windows Hello aktivieren** wird dann im Anmeldedialogfeld des Servers angezeigt.

Hinzufügen eines Remote-Desktops oder einer Remoteanwendung zum Startbildschirm

Sie haben die Möglichkeit, dem Startbildschirm einen Remote-Desktop oder eine Remoteanwendung hinzuzufügen. Dazu klicken Sie im Auswahlfenster für Desktops und Anwendungen mit der rechten Maustaste auf den Desktop oder die Anwendung und wählen aus dem Kontextmenü die Option **Zur Startseite hinzufügen** aus.

Wenn Sie beim Tippen auf den Remote-Desktop oder die Remoteanwendung im Startbildschirm noch nicht beim Server angemeldet sind, werden Sie von Horizon Client zur Authentifizierung beim Server aufgefordert, bevor der Remote-Desktop oder die Remoteanwendung gestartet wird. Wenn Sie bereits beim Server angemeldet sind, wird der Remote-Desktop oder die Remoteanwendung ohne Authentifizierung beim Server gestartet.

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 bei einem Remote-Desktop oder einer Remoteanwendung angemeldet sind, können Sie die Verbindung trennen, indem Sie im Desktop- oder Anwendungsfenster auf die Schaltfläche **Trennen** 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

Wenn Sie derzeit mit einem Remote-Desktop verbunden und dort angemeldet sind, können Sie sich über das **Startmenü** abmelden.

Sie können sich auch abmelden, indem Sie auf die Schaltfläche **Strg+Alt+Entf** im Desktop- oder Anwendungsfenster und dann auf **Abmelden** tippen.

Alle nicht gespeicherten Dateien, die auf dem Remote-Desktop geöffnet sind, werden beim Abmelden ohne vorheriges Speichern geschlossen. Wenn Sie die Verbindung zu einem Remote-Desktop trennen, ohne sich abzumelden, bleiben die Anwendungen im Remote-Desktop geöffnet.

Verwenden eines Remote-Desktops oder einer Remoteanwendung

4

Horizon Client beinhaltet Funktionen, wie sie bei anderen Windows 10 UWP-Apps gängig sind, sowie spezifische Funktionen für Remote-Desktops und Remoteanwendungen.

Dieses Kapitel behandelt die folgenden Themen:

Funktionsunterstützungs-Matrix

Einige Funktionen werden nur auf bestimmten Clienttypen unterstützt. Der USB-Zugriff wird beispielsweise von Horizon Client für Windows, aber nicht von Horizon Client für Windows 10 UWP unterstützt.

Tabelle 4-1. Auf Windows-Desktops für Windows 10 UWP Horizon Clients unterstützte Funktionen

Funktion	Windows 10-Desktop	Windows 8.x-Desktop	Windows 7-Desktop	Windows Vista-Desktop	Windows XP-Desktop	Windows Server 2008/2012 R2- und Windows Server 2016-Desktops
USB-Umleitung						
Echtzeit-Audio/Video (RTAV)						
Umleitung serieller Ports						

Tabelle 4-1. Auf Windows-Desktops für Windows 10 UWP Horizon Clients unterstützte Funktionen (Fortsetzung)

Funktion	Windows 10-Desktop	Windows 8.x-Desktop	Windows 7-Desktop	Windows Vista-Desktop	Windows XP-Desktop	Windows Server 2008/2012 R2- und Windows Server 2016-Desktops
VMware Blast-Anzeigeprotokoll	X	X	X			X
RDP-Anzeigeprotokoll						
PCoIP-Anzeigeprotokoll	X	X	X	Begrenzt	Begrenzt	X
Persona-Verwaltung						
Wyse MMR						
Windows Media MMR						
Standortbasierter Druck	X	X	X	Begrenzt	Begrenzt	X
Virtuelles Drucken						
Smartcards						
RSA SecurID oder RADIUS	X	X	X	Begrenzt	Begrenzt	X
Einmaliges Anmelden	X	X	X	Begrenzt	Begrenzt	X
Mehrere Monitore						

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 oder Horizon Agent 7.0 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 zu diesen 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-Remote-Desktop-Dienste und 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.

Die folgende Tabelle enthält nur Zeilen für die unterstützten Funktionen. Bestimmte Funktionen werden nur auf RDS-Hosts virtueller Maschinen und nicht auf RDS-Hosts physischer Maschinen unterstützt.

Tabelle 4-2. Unterstützte Funktionen für RDS-Hosts mit installiertem View Agent 6.0.x oder höher oder mit Horizon Agent 7.0 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
VMware Blast-Anzeigeprotokoll	Horizon Agent 7.0 und höher	Horizon Agent 7.0 und höher	Horizon Agent 7.0.2 und höher
PCoIP-Anzeigeprotokoll	X	X	Horizon Agent 7.0.2 und höher
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)

Informationen zu den unterstützten Editionen oder Service Packs der Gastbetriebssysteme finden Sie im Thema „Unterstützte Betriebssysteme für View Agent“ in der Dokumentation zur Installation von View 5.x oder 6.x. Im Abschnitt „Unterstützte Betriebssysteme für Horizon Agent“ der Installationsdokumentation von Horizon 7 finden Sie weitere Informationen.

Verwenden des Vollbildmodus

Sie können Remote-Desktops und -anwendungen auf einem Surface Pro 4 oder Surface Book im Vollbildmodus oder im Fenstermodus anzeigen. Standardmäßig ist der Vollbildmodus aktiviert.

Um den Vollbildmodus ein- und auszuschalten, tippen Sie nach der Anmeldung bei einem Remote-Desktop oder einer Remoteanwendung auf die Schaltfläche **Option** im Fenster des Remote-Desktops oder der Remoteanwendung und dann auf **Vollbild**.

Anpassen der Bildschirmauflösung für Remote-Desktops und -anwendungen

Wenn Ihr Tablet über einen hochauflösenden Bildschirm verfügt, haben Sie möglicherweise Probleme, Symbole und Text auf einem Remote-Desktop oder in einer Remoteanwendung zu lesen. Zur Verbesserung der Lesbarkeit können Sie die Bildschirmauflösung verringern.

Um die Bildschirmauflösung vor der Anmeldung bei einem Remote-Desktop oder einer Remoteanwendung zu ändern, tippen Sie auf das Menü **Option** links oben in der Horizon Client-Menüleiste, erweitern Sie den Abschnitt **Auflösungsmodus** und wählen Sie eine Option für die Auflösung aus.

Sie können die Bildschirmauflösung auch nach der Herstellung einer Verbindung mit einem Server oder nach der Anmeldung bei einem Remote-Desktop oder einer Remoteanwendung ändern.

Aktivieren der Funktion „Lokaler Zoom“

Wenn Sie die Funktion „Lokaler Zoom“ aktivieren, können Sie durch Zusammen- oder Auseinanderziehen Ihrer Finger auf Ihrem Touchscreen die Darstellung auf Ihrem Remote-Desktop oder in Ihrer Remtoeanwendung verkleinern oder vergrößern.

Bei Desktops virtueller Windows 8- und Windows 10-Maschinen und für Windows Server 2012 R2- und Windows Server 2016 RDS-Desktops und -Anwendungen besteht diese Möglichkeit für Verkleinern/Vergrößern durch Zusammen- oder Auseinanderziehen Ihrer Finger nur dann, wenn Sie die Funktion „Lokaler Zoom“ aktivieren.

Vorgehensweise

1 Stellen Sie eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung her.

2 Tippen Sie auf die Schaltfläche **Option** im Desktop- oder Anwendungsfenster und dann auf **Einstellungen**.

3 Erweitern Sie den Abschnitt **Erweitert** und tippen Sie auf die Option **Lokaler Zoom**, auf **Ein** umzuschalten.

Ist für die Option **Aus** eingestellt, können Sie die Funktion „Lokaler Zoom“ nicht auf einem Remote-Desktop oder in einer Remoteanwendung verwenden. Für die Option ist standardmäßig **Aus** eingestellt.

Verhindern der Bildschirmsperre

Nach einer bestimmten Zeit im Leerlauf kann es sein, dass Ihr Windows 10-Gerät die Anzeige abblendet, die Bildschirmsperre aktiviert oder die Anzeige zur Reduzierung des Stromverbrauchs herunterfährt. Mit einer Option können Sie die Bildschirmsperre für einen Remote-Desktop oder eine Remoteanwendung unterbinden.

Hinweis Windows 10-Geräte behandeln passive Aktivitäten wie die Bildschirmbetrachtung und das Anhören von Ton als Leerlaufzeit des Benutzers. Der Zeitpunkt, ab der ein Bildschirm im Leerlauf gesperrt wird, hängt von den Benutzereinstellungen Ihres Geräts für die Leerlaufzeit ab.

Vorgehensweise

1 Stellen Sie eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung her.

2 Tippen Sie auf die Schaltfläche **Option** im Desktop- oder Anwendungsfenster und dann auf **Einstellungen**.

3 Erweitern Sie den Abschnitt **Erweitert** und tippen Sie auf die Option **Bildschirm immer anzeigen**, um auf **Ein** umzuschalten.

Wenn für die Option **Aus** eingestellt ist, kann der Bildschirm gesperrt werden.

Verwenden der Sidebar

Nach der Herstellung einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung können Sie mithilfe der Sidebar andere Desktops und Anwendungen öffnen.

Tabelle 4-3. Sidebar-Aktionen

Aktion	Beschreibung
Anzeigen der Sidebar	Tippen Sie auf die Schaltfläche **Option** im Remote-Desktop- oder Remoteanwendungsfenster und dann auf **Sidebar**.
Ausblenden der Sidebar	Tippen Sie auf eine beliebige Stelle im Remote-Desktop- oder Remoteanwendungsfenster.
Öffnen eines Remote-Desktops oder einer Remoteanwendung	Tippen Sie auf den Namen des Remote-Desktops oder der Remoteanwendung in der Sidebar.
Suchen nach einem Remote-Desktop oder einer Remoteanwendung	Geben Sie den Namen des Remote-Desktops oder der Remoteanwendung in das Feld **Suchen** ein. Um den Remote-Desktop oder die Remoteanwendung zu öffnen, tippen Sie auf den entsprechenden Namen in den Suchergebnissen.

Bewegungs- und Navigationshilfen

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

Klicken

Wie bei anderen Anwendungen tippen Sie darauf, um auf ein Element der Benutzeroberfläche zu klicken. Es lässt sich auch eine externe Maus verwenden.

Rechtsklicken

Die folgenden Optionen stehen zum Rechtsklicken zur Verfügung:

- Für den Rechtsklick verwenden Sie eine externe Maus.
- Auf einem Touchpad tippen Sie mit zwei Fingern.
- Auf einem Touchscreen tippen Sie und halten Sie die Stelle, bis das Kontextmenü angezeigt wird.

Vergrößern und Verkleinern

Auf einem Touchscreen können Sie durch Auseinander- oder Zusammenziehen Ihrer Finger die Darstellung vergrößern oder verkleinern.

Bei Betriebssystemen, die eine Toucheingabe unterstützen, ist das Vergrößern und Verkleinern auf einem Touchscreen nur möglich, wenn die Funktion „Lokaler Zoom“ aktiviert ist Siehe „Aktivieren der Funktion „Lokaler Zoom““, auf Seite 21. Windows 8, Windows 8.1, Windows 10, Windows Server 2012 und Windows Server 2016 unterstützen die Toucheingabe.

Bildlauf und Bildlaufleisten

Für den vertikalen Bildlauf stehen die folgenden Optionen zur Verfügung:

- Für den Bildlauf verwenden Sie eine externe Maus.
- Auf einem Touchpad tippen Sie und halten Sie die Stelle mit Ihrem Daumen und führen Sie dann mit zwei Fingern einen Bildlauf nach durch.
- Auf einem Touchscreen tippen Sie auf den Bildschirm mit zwei Fingern und ziehen diese für den Bildlauf oder Sie führen den Bildlauf mit einem Finger auf der Bildlaufleiste durch. Der Text unter Ihren Fingern bewegt sich in dieselbe Richtung wie Ihre Finger.

Ton, Musik und Video

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

Strg+Alt+Entf

Da die Windows-Tastenkombination Strg+Alt+Entf für Remote-Desktops und -anwendungen nicht unterstützt wird, tippen Sie stattdessen auf die Schaltfläche **Strg+Alt+Entf** im Fenster des Remote-Desktops oder der Remoteanwendung.

Multitasking

Sie können zwischen Horizon Client und anderen Apps wechseln, ohne dabei eine Remote-Desktop- oder Anwendungsverbindung zu verlieren.

Sie können die Größe der Horizon Client-App anpassen, sodass sie den Bildschirm zusammen mit einer anderen Anwendung teilt.

Wenn sich eine Sitzung für einige Zeit im Leerlauf befindet, werden Sie vor dem Überschreiten des Zeitlimits für die Sitzung gefragt, ob die Sitzung weiterhin aktiv bleiben soll. Tippen bzw. klicken Sie auf eine beliebige Stelle auf dem Bildschirm oder drücken Sie eine Taste auf der Tastatur, damit die Sitzung aktiv bleibt. Wenn zu viel Zeit vergangen ist und die Verbindung zum Remote-Desktop bzw. zur Remoteanwendung unterbrochen wurde, kehrt Horizon Client zum Auswahlfenster für Desktops und Anwendungen zurück. Sie werden dann aufgefordert, die Verbindung erneut herzustellen.

Verwenden von Horizon Client mit einem Microsoft Display Dock

Die VMware Horizon Client-App kann mit Continuum für Windows 10 Mobile verwendet werden. Sie können mit dem Microsoft Display Dock Ihr Windows 10-Smartphone an ein externes Anzeigegerät oder an eine Maus anschließen. Mit dieser Funktion lässt sich Horizon Client wie auf einem Desktop-PC verwenden.

Kopieren und Einfügen von Text und Bildern

Sie können standardmäßig Text von Ihrem Clientsystem auf einen Remote-Desktop oder in eine Remoteanwendung kopieren und einfügen. Wenn ein Horizon-Administrator die Funktion aktiviert, können Sie auch Text zwischen einem Remote-Desktop oder einer Remoteanwendung und Ihrem Clientsystem oder zwischen zwei Remote-Desktops oder -anwendungen kopieren und einfügen.

Sie können nur einfachen Text kopieren und einfügen. Bilder und RTF-Texte (Rich Text Format) werden nicht unterstützt.

Ein Horizon-Administrator kann diese Funktion so einstellen, dass Kopier- und Einfügevorgänge nur von Ihrem Clientsystem zu einem Remote-Desktop bzw. zu einer Remoteanwendung oder nur von einem Remote-Desktop bzw. von einer Remoteanwendung zu Ihrem Clientsystem zugelassen werden oder beide bzw. keiner der beiden Vorgänge möglich sind.

Horizon-Administratoren haben die Möglichkeit, das Kopieren/Einfügen durch entsprechende Konfiguration der Gruppenrichtlinieneinstellungen zu aktivieren, die Horizon Agent zugeordnet sind. Je nach installierter Version von Horizon Server und Agent können Administratoren auch mit Gruppenrichtlinien Zwischenablageformate für das Kopieren/Einfügen beschränken oder das Kopieren/Einfügen auf Remote-Desktops mithilfe von intelligenten Richtlinien steuern. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

In der Zwischenablage können bis zu 64 K an Daten für Kopier- und Einfügevorgänge gespeichert werden. Wenn Sie versuchen, mehr als die maximale Größe der Zwischenablage zu kopieren, wird der Text abgeschnitten.

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

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 5

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

Sie können auch die Protokollerfassung aktivieren und diese Daten zur Fehlerbehebung an VMware senden.

Dieses Kapitel behandelt die folgenden Themen:

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.
- Wenn Sie beim Versuch, eine Verbindung zum Server herzustellen, ein Verbindungsfehler erhalten, müssen Sie möglicherweise Ihre Proxy-Einstellungen ändern.

Zurücksetzen eines Remote-Desktops oder einer Remoteanwendung

Wenn Sie aktuell mit einem Remote-Desktop oder einer Remoteanwendung verbunden und dort angemeldet sind, können Sie durch Tippen auf die Schaltfläche **Trennen** im Desktop- oder Anwendungsfenster und durch Tippen auf **Zurücksetzen** den Remote-Desktop oder die Remoteanwendung zurücksetzen.

Der Befehl **Zurücksetzen** ist nur verfügbar, wenn der Horizon-Administrator ihn zugelassen hat und sich der Remote-Desktop bzw. die Remoteanwendung in einem Status befindet, in dem diese Aktion vorgenommen werden kann.

Eventuell muss der Remote-Desktop oder die Remoteanwendung neu gestartet werden, wenn das Desktop-Betriebssystem oder die Anwendung nicht mehr reagiert.

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 dabei nicht gespeichert.

Beim Zurücksetzen einer Remoteanwendung werden alle Remoteanwendungen beendet und alle Remoteanwendungssitzungen abgemeldet. Nicht gespeicherte Änderungen in Remoteanwendungen gehen möglicherweise verloren.

Deinstallieren der VMware Horizon Client -App

Sie können manche Probleme mit Horizon Client beheben, indem Sie die VMware Horizon Client-App vom Windows 10 UWP-Gerät deinstallieren und anschließend neu installieren.

Deinstallieren Sie Horizon Client genau wie alle anderen Windows 10 UWP-Apps.

Vorgehensweise

1 Suchen Sie auf Ihrem Gerät die VMware Horizon Client-App.

2 Klicken Sie mit der rechten Maustaste auf die **VMware Horizon Client**-Kachel oder auf das entsprechende Symbol und tippen Sie auf **Deinstallieren**.

Weiter

Installieren Sie die VMware Horizon Client-App erneut. Siehe „Installieren oder Aktualisieren von Horizon Client für Windows 10 UWP“, auf Seite 9.

Herstellen einer Verbindung mit einem Server im Workspace ONE -Modus

Wenn Sie mit Horizon Client keine direkte Verbindung mit einem Server herstellen können oder wenn Ihre Desktop- und Anwendungsberechtigungen in Horizon Client nicht angezeigt werden, kann eventuell der Workspace ONE-Modus auf dem Server aktiviert werden.

Problem

- Wenn Sie versuchen, eine direkte Verbindung mit dem Server über Horizon Client herzustellen, werden Sie von Horizon Client zum Workspace ONE-Portal umgeleitet.
- Wenn Sie einen Desktop oder eine Anwendung über einen URI oder eine Verknüpfung öffnen oder wenn Sie eine lokale Datei über die Dateiverknüpfung öffnen, leitet die Anforderung Sie zum Workspace ONE-Portal zur Authentifizierung weiter.
- Nach dem Öffnen eines Desktops oder einer Anwendung über Workspace ONE und dem Start von Horizon Client werden andere berechtigte Remote-Desktops oder -anwendungen in Horizon Client nicht angezeigt oder können nicht geöffnet werden.

Ursache

Ab Horizon 7 Version 7.2 hat ein Administrator die Möglichkeit, den Workspace ONE-Modus auf einer Verbindungsserver-Instanz zu aktivieren. Dies ist das Standardverhalten, wenn der Workspace ONE-Modus auf einer Verbindungsserver-Instanz aktiviert ist.

Lösung

Verwenden Sie Workspace ONE, um eine Verbindung mit einem Workspace ONE-aktivierten Server herzustellen und um auf Ihre Remote-Desktops und -anwendungen zuzugreifen.

Protokollerfassung zur Übersendung an den technischen Support

Sie können die Protokollierung aktivieren und die Protokolle gebündelt erfassen, um sie an den technischen Support zu senden.

Bei manchen Problemen werden Sie zum Zweck der Fehlerbehebung möglicherweise aufgefordert, Protokolle zu erfassen und sie an den technischen Support zu senden. Das Protokollieren beeinträchtigt die Leistung von Horizon Client, wenn eine sichere Tunnel-Sitzung zum Herstellen einer Verbindung mit dem Remote-Desktop verwendet wird. Vergewissern Sie sich, dass Sie die erweiterte Protokollierungsfunktion ausschalten, wenn die Protokollierung nicht mehr erforderlich ist.

Voraussetzungen

Wenden Sie sich an den technischen Support von VMware, um zu erfahren, wohin Sie die erfassten Protokolldateien senden können.

Vorgehensweise

1 Tippen Sie in Horizon Clientauf das Menü **Option** links oben in der Menüleiste.

  Wenn Sie mit einem Server verbunden sind, können Sie auf das Menü **Option** links oben im Auswahlfenster für Desktops und Anwendungen tippen. Wenn Sie mit einem Remote-Desktop oder einer Remoteanwendung verbunden sind, können Sie im Desktop- oder Anwendungsfenster auf die Schaltfläche **Option** tippen und dann auf **Einstellungen**.

2 Erweitern Sie den Abschnitt **Protokollierung** und tippen Sie auf die Option **Erweiterte Protokollierung aktivieren**, um auf „Ein“ umzuschalten.

3 Tippen Sie auf **Support-Informationen einholen**, navigieren Sie zum Speicherort auf Ihrem Gerät, in dem die Protokolldateien gespeichert werden sollen, wählen Sie das Verzeichnis aus und tippen Sie auf **Ordner auswählen**.

  Sie können beispielsweise auf das **Desktop**-Element tippen, um die Protokolle in einem Ordner auf Ihrem lokalen Desktop zu speichern.

  Horizon Client erstellt einen Ordner namens `vmware-view-logs-`*`Zeitstempel`* im von Ihnen angegebenen Speicherort.

4 (Optional) Um eine `.zip`-Datei des Protokollordners zu erstellen, bevor Sie diese an den technischen Support senden, klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie die Option **Senden an > ZIP-komprimierter Ordner** aus.

Weiter

Senden Sie die Protokolle an den technischen Support von VMware.

Index