

Verwendung von VMware Horizon Client für iOS

März 2016
Horizon Client

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-001481-04

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

Copyright © 2010–2016 VMware, Inc. Alle Rechte vorbehalten. [Informationen zu Copyright und Marken.](#)

VMware, Inc.

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

VMware Global, Inc.

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

Inhalt

Verwendung von VMware Horizon Client für iOS	5
1 Konfiguration und Installation	7
Systemanforderungen	8
Systemanforderungen für Echtzeit-Audio/Video	8
Anforderungen für die Smartcard-Authentifizierung	9
Konfigurieren der Smartcard-Authentifizierung für mobile Clients	10
Anforderungen für Authentifizierung über Touch ID	11
Unterstützte Desktop-Betriebssysteme	12
Vorbereiten des Verbindungsservers für Horizon Client	12
Installieren oder Aktualisieren von Horizon Client auf einem iOS-Gerät	13
Verwenden von eingebetteten RSA SecurID-Software-Token	14
Konfigurieren erweiterter TLS-/SSL-Optionen	15
Konfigurieren der VMware Blast-Optionen	16
Konfigurieren der Horizon Client -Standardansicht	16
Konfigurieren von AirWatch, um Horizon Client auf Mobilgeräten zur Verfügung zu stellen	17
Durch VMware gesammelte Horizon Client -Daten	18
2 Verwenden von URIs zur Konfiguration von Horizon Client	21
Syntax für die Erstellung von vmware-view-URIs	22
Beispiele für vmware-view-URIs	24
3 Verwalten der Remote-Desktop- und Anwendungsverbindungen	27
Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung	27
Zertifikatsprüfungsmodi für Horizon Client	31
Verwalten von gespeicherten Servern	32
Auswählen eines Remote-Desktops oder einer Remoteanwendung als Favorit	33
Trennen der Verbindung mit einem Remote-Desktop oder einer Remoteanwendung	34
Abmelden von einem Remote-Desktop	34
Verwalten von Desktop- und Anwendungsverknüpfungen	35
Verwenden von 3D Touch mit Horizon Client	35
Verwenden der Spotlight-Suche mit Horizon Client	36
Verwenden von Split View und Slide Over mit Horizon Client	36
4 Verwenden von Microsoft Windows-Desktops oder -Anwendungen auf einem mobilen Endgerät	39
Funktionsunterstützungs-Matrix für iOS	39
Externe Tastaturen und Eingabevorrichtungen	42
Aktivieren des japanischen 106/109-Tastaturlayouts	43
Verwenden der Echtzeit-Audio/Video-Funktion für Mikrofone	43
Verwenden nativer Gesten auf Betriebssystemen mit Touch-Umleitung	43

Verwenden der Unity Touch-Sidebar mit einem Remote-Desktop	44
Verwenden der Unity Touch-Sidebar mit einer Remoteanwendung	46
Horizon Client -Tools	48
Gesten	50
Multitasking	51
Speichern von Dokumenten in einer Remoteanwendung	52
Konfiguration von Horizon Client zur Unterstützung von umgekehrten Maustasten	52
Bildschirmauflösungen und Verwendung externer Anzeigen	52
PCoIP-Client-Bildcache	53
Unterdrücken der Warnmeldung bezüglich der Mobilfunkdaten	54
Internationalisierung	54
5 Fehlerbehebung für Horizon Client	55
Erfassen und Versenden von Protokollinformationen	55
Aktivieren der Horizon Client -Protokollerfassung	55
Manuelles Abrufen und Senden von Horizon Client -Protokolldateien	56
Deaktivieren der Horizon Client -Protokollerfassung	57
Zurücksetzen eines Remote-Desktops oder einer Remoteanwendung	57
Deinstallieren von Horizon Client	58
Horizon Client oder der Remote-Desktop reagiert nicht mehr	58
Probleme beim Herstellen einer Verbindung bei Verwendung eines Proxys	59
Index	61

Verwendung von VMware Horizon Client für iOS

Das Handbuch *Verwendung von VMware Horizon Client für iOS* bietet Informationen zur Installation und Verwendung der VMware Horizon[®] Client[™]-Software auf einem Android-Gerät zur Herstellung einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung im Datacenter.

Die Informationen in diesem Dokument enthalten Systemanforderungen und Anleitungen zur Installation von Horizon Client. Dieses Dokument enthält zudem Tipps zur Verbesserung der Benutzererfahrung beim Navigieren und Verwenden von Windows-Desktop-Elementen auf einem iOS-Gerät (zum Beispiel einem iPad).

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

Konfiguration und Installation

Bei der Einrichtung einer View-Bereitstellung für iOS-Clients müssen bestimmte Konfigurationseinstellungen des Verbindungsservers verwendet, die Systemanforderungen für View Server und iOS-Clients erfüllt und die App für Horizon Client aus dem Apple App Store installiert werden. VMware empfiehlt zudem, dass Sie einen Sicherheitsserver konfigurieren, damit Ihre iOS-Clients keine VPN-Verbindung benötigen.

HINWEIS In Horizon 7 und höher wurde der View Administrator in Horizon Administrator umbenannt. Wenn in diesem Dokument von View Administrator die Rede ist, dann bezieht sich dies immer sowohl auf den View Administrator als auch auf den Horizon Administrator.

Dieses Kapitel behandelt die folgenden Themen:

- „Systemanforderungen“, auf Seite 8
- „Systemanforderungen für Echtzeit-Audio/Video“, auf Seite 8
- „Anforderungen für die Smartcard-Authentifizierung“, auf Seite 9
- „Konfigurieren der Smartcard-Authentifizierung für mobile Clients“, auf Seite 10
- „Anforderungen für Authentifizierung über Touch ID“, auf Seite 11
- „Unterstützte Desktop-Betriebssysteme“, auf Seite 12
- „Vorbereiten des Verbindungsservers für Horizon Client“, auf Seite 12
- „Installieren oder Aktualisieren von Horizon Client auf einem iOS-Gerät“, auf Seite 13
- „Verwenden von eingebetteten RSA SecurID-Software-Token“, auf Seite 14
- „Konfigurieren erweiterter TLS-/SSL-Optionen“, auf Seite 15
- „Konfigurieren der VMware Blast-Optionen“, auf Seite 16
- „Konfigurieren der Horizon Client-Standardansicht“, auf Seite 16
- „Konfigurieren von AirWatch, um Horizon Client auf Mobilgeräten zur Verfügung zu stellen“, auf Seite 17
- „Durch VMware gesammelte Horizon Client-Daten“, auf Seite 18

Systemanforderungen

Sie können Horizon Client auf allen iPad- und iPhone-Modellen installieren.

Sowohl das iOS-Gerät, auf dem Sie Horizon Client installieren, als auch die Peripheriegeräte müssen bestimmte Systemanforderungen erfüllen.

iPad- und iPhone-Modelle

- iPhone 4, 4s, 5, 5s, 5c, 6, 6 Plus, 6s und 6s Plus
- iPad 2, iPad (3. Generation), iPad (4. Generation), iPad Mini, iPad Mini 3, iPad mini 4, iPad Mini mit Retina-Display, iPad Air, iPad Air 2 und iPad Pro

Horizon Client 3.4 und höher umfasst eine Unterstützung für 64-Bit-Prozessoren für iPhone 5s, 6 und 6 Plus sowie iPad Air, iPad Air 2, iPad mini 2 und iPad mini 3.

Betriebssysteme

iOS 6.0 und höher, einschließlich iOS 9.x

Externe Tastaturen

(Optional) iPad Keyboard Dock und Apple Wireless Keyboard (Bluetooth)

Smartcard-Authentifizierung

Siehe „[Anforderungen für die Smartcard-Authentifizierung](#)“, auf Seite 9.

Authentifizierung über Touch ID

Siehe „[Anforderungen für Authentifizierung über Touch ID](#)“, auf Seite 11.

Verbindungsserver, Sicherheitsserver und View Agent oder Horizon Agent

Aktuelle Wartungsversion von View 5.3.x und neuere Versionen.

VMware empfiehlt, dass Sie einen Sicherheitsserver konfigurieren, damit Ihre iOS-Clients keine VPN-Verbindung benötigen.

Zur Verwendung der Unity Touch-Funktion mit View 5.3.x-Desktops muss der Remote Experience Agent auf den Desktops installiert sein.

Remoteanwendungen sind auf Servern mit Horizon 6.0 (mit View) und höher verfügbar.

Anzeigeprotokoll für View

- PCoIP
- VMware Blast (erfordert Horizon Client 4.0 oder höher und 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 View-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

View-Remote-Desktop

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 für View. Wenn Sie über View Agent 6.0 oder höher oder über Horizon Agent 7.0 oder höher verfügen, ist kein Feature Pack erforderlich. Echtzeit-Audio/Video wird in Remoteanwendungen nicht unterstützt.

Clientzugriffsgesät

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

Horizon Client 4.0 oder höher muss auf dem Clientgerät installiert sein.

HINWEIS In Horizon Client 4.0 wird nur die Audio-Eingangs-Funktion unterstützt. Die Video-Funktion wird in Horizon Client 4.0 nicht unterstützt.

Anforderungen für die Smartcard-Authentifizierung

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

Horizon Client für iOS unterstützt Smartcards mit Remote-Desktops, auf denen die Gastbetriebssysteme Windows 7, Windows Vista, Windows 8.1, Windows XP oder Windows Server 2008 R2 ausgeführt werden. Für Microsoft RDS-hostbasierte Desktops und Anwendungen werden die Betriebssysteme Windows Server 2008 R2 und Windows Server 2012 R2 unterstützt. VMware empfiehlt, ein iOS 6.1.3-Betriebssystem oder höher zu verwenden. Das baiMobile 301MP USB-Smartcard-Lesegerät und die folgenden Smartcards wurden getestet:

- Oberthur ID One V5.2a DOD CAC
- Gemalto TOPDLGX4 DOD CAC
- ActivIdentity 64K V2C Java Card

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

- Horizon Client
- Ein kompatibler Smartcard-Leser
- Produktspezifische Anwendungstreiber

Sie müssen auf den Remote-Desktops oder dem Microsoft RDS-Host zusätzlich produktspezifische Anwendungstreiber installieren.

Benutzer, die sich mithilfe von Smartcards authentifizieren, müssen über eine Smartcard verfügen, und jede Smartcard muss ein Benutzerzertifikat enthalten.

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

- Informationen zur Konfiguration von Verbindungsservern für die Nutzung von Smartcards finden Sie unter „Konfigurieren der Smartcard-Authentifizierung“ im Dokument *Administration von View*.

Alle anwendbaren CA-Zertifikate (Certificate Authority, Zertifizierungsstelle) für alle vertrauenswürdigen Benutzerzertifikate müssen einer Serververtrauensspeicher-Datei auf dem Verbindungsserver- oder Sicherheitsserver-Host hinzugefügt werden. Diese Zertifikate beinhalten Stammzertifikate und müssen auch Zwischenzertifikate enthalten, wenn das Smartcard-Zertifikat des Benutzers von einer Zwischenzertifizierungsstelle herausgegeben wurde.

- Informationen zu den Aufgaben, die Sie womöglich in Active Directory zur Implementierung der Smartcard-Authentifizierung durchführen müssen, finden Sie in den Abschnitten zur Vorbereitung von Active Directory für die Smartcard-Authentifizierung im Dokument *Installation von View*.

Konfigurieren der Smartcard-Authentifizierung für mobile Clients

Zu den Konfigurationsaufgaben zählen das Verbinden und Koppeln des Kartenlesegeräts mit dem mobilen Endgerät und das Festlegen der Richtlinie zum Entfernen von Smartcards.

Voraussetzungen

- Stellen Sie sicher, dass Sie die richtige Version des Clients, des Desktop-Agents, des Servers, des Betriebssystems für das mobile Gerät, des Smartcard-Lesers und der Smartcard verwenden. Siehe [„Anforderungen für die Smartcard-Authentifizierung“](#), auf Seite 9.
- Führen Sie (soweit noch nicht geschehen) die unter „Vorbereiten von Active Directory für die Smartcard-Authentifizierung“ im Dokument *Installation von View* beschriebenen Aufgaben aus.
- Konfigurieren Sie View Server für die Unterstützung der Nutzung von Smartcards. Weitere Informationen finden Sie unter dem Thema „Konfigurieren der Smartcard-Authentifizierung“ im Dokument *Verwaltung von View*.

Vorgehensweise

- 1 Koppeln Sie gemäß der Dokumentation vom Hersteller des Smartcard-Lesers das mobile Endgerät mit dem Smartcard-Leser.

Falls Ihr iOS-Gerät einen 30-poligen Anschluss aufweist, können Sie den Smartcard-Leser dort anschließen. Für iPad Air und iPhone 5S mit Lightning-Schnittstellen müssen Sie einen 30-poligen Adapter verwenden, um den Smartcard-Leser mit dem 30-poligen Anschluss des Geräts zu verbinden.

- 2 Konfigurieren Sie die Richtlinie zum Entfernen von Smartcards.

Option	Beschreibung
Festlegen der Richtlinie auf dem Server	<p>Für eine mit View Administrator eingerichtete Richtlinie können Sie festlegen, dass die Verbindung der Benutzer mit dem Verbindungsserver getrennt wird, wenn diese ihre Smartcards entfernen, oder dass diese Verbindung aufrechterhalten wird und die Benutzer die Möglichkeit haben, neue Desktop- oder Anwendungssitzungen ohne erneute Authentifizierung zu starten.</p> <ol style="list-style-type: none"> Wählen Sie in View Administrator View-Konfiguration > Server. Wählen Sie auf der Registerkarte Verbindungsserver die Verbindungsserver-Instanz aus und klicken Sie auf Bearbeiten. Auf der Registerkarte Authentifizierung aktivieren oder deaktivieren Sie das Kontrollkästchen Benutzersitzungen nach Entfernung der Smartcard trennen für die Konfiguration der Richtlinie zur Smartcard-Entfernung. Klicken Sie auf OK, um Ihre Änderungen zu speichern. Starten Sie den Verbindungsserver-Dienst neu, damit die Änderungen wirksam werden. <p>Wenn Sie das Kontrollkästchen Benutzersitzungen nach Entfernung der Smartcard trennen aktivieren, kehrt Horizon Client zum Bildschirm Zuletzt verwendete Verbindungen (Horizon Client 3.0) oder zum Bildschirm Zuletzt verwendet (Horizon Client 3.1 und höher) zurück, wenn Benutzer ihre Smartcards entfernen.</p>
Festlegen der Richtlinie auf dem Desktop	<p>Mit dem Gruppenrichtlinien-Editor (<code>gpedit.msc</code>) stehen Ihnen folgende Einstellungsmöglichkeiten zur Verfügung: keine Aktion, Workstation sperren, Abmeldung erzwingen oder Verbindung trennen, wenn eine RDS-Sitzung (Remote Desktop Services, Remotedesktopdienste) durchgeführt wird.</p> <p>Nachdem Sie <code>gpedit.msc</code> im Desktop-Betriebssystem geöffnet haben, navigieren Sie zu Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen > Interaktive Anmeldung: Verhalten beim Entfernen von Smartcards. Nach der Änderung der Konfiguration führen Sie den Befehl <code>gpupdate /force</code> aus, um eine Aktualisierung der Gruppenrichtlinie zu erzwingen.</p>

Anforderungen für Authentifizierung über Touch ID

Um Touch ID für die Benutzerauthentifizierung in Horizon Client zu verwenden, müssen Sie bestimmte Anforderungen erfüllen.

iPad- und iPhone-Modelle	Jedes iPad- oder iPhone-Modell, das Touch ID unterstützt, z. B. iPad Air 2 und iPhone 6.
Betriebssystemanforderungen	<ul style="list-style-type: none"> ■ iOS 8 oder höher. ■ Fügen Sie der Touch ID- und Passcode-Einstellung mindestens einen Fingerabdruck hinzu.
Verbindungsserveranforderungen	<ul style="list-style-type: none"> ■ 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 <i>Administration von View</i>. ■ Die Verbindungsserver-Instanz muss Horizon Client ein gültiges stammsigniertes Zertifikat vorweisen.
Horizon Client-Anforderungen	<ul style="list-style-type: none"> ■ Horizon Client 3.5 oder höher.

- Aktivieren Sie für den Zertifikatsprüfungsmodus **Nie mit nicht vertrauenswürdigen Servern verbinden** oder **Warnung vor Verbindung mit nicht vertrauenswürdigen Servern ausgeben**. Informationen zum Einstellen des Zertifikatsprüfungsmodus finden Sie unter [„Zertifikatsprüfungsmodi für Horizon Client“](#), auf Seite 31.
- Aktivieren Sie Touch ID durch Antippen von **Touch ID aktivieren** auf dem Anmeldebildschirm von View Server. Nach der erfolgreichen Anmeldung werden Ihre Active Directory-Anmeldedaten sicher im Schlüsselbund Ihres iOS-Geräts gespeichert. Die Option **Touch ID aktivieren** wird nur bei der ersten Anmeldung und dann nicht mehr angezeigt, wenn Touch ID aktiviert ist.

Sie können Touch ID mit der Smartcard-Authentifizierung und als Bestandteil der Zwei-Faktor-Authentifizierung mit der RSA SecurID- und RADIUS-Authentifizierung verwenden. Wenn Sie Touch ID mit der Smartcard-Authentifizierung verwenden, stellt Horizon Client eine Verbindung zum Server her, nachdem Sie Ihre PIN eingegeben haben. Der Touch ID-Anmeldebildschirm wird dann nicht angezeigt.

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 mit unterstützten Windows-Gastbetriebssystemen finden Sie unter dem 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.

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 die Verwendung von Access Point planen, das mit Horizon 6 Version 6.2 oder höher verfügbar ist, konfigurieren Sie den Verbindungsserver für die Zusammenarbeit mit Access Point. Siehe *Bereitstellen und Konfigurieren von Access Point*. Access Point-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. Informationen finden Sie im Dokument *Installation von View*.
- 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.

Navigieren Sie zur Aktivierung oder Deaktivierung der sicheren Tunnelverbindung in View Administrator auf das Dialogfeld View-Verbindungsserver-Einstellungen bearbeiten und setzen Sie einen Haken in das Kontrollkästchen **Sichere Tunnelverbindung zum Desktop verwenden**.

- Vergewissern Sie sich, dass ein Desktop- oder Anwendungspool erstellt wurde und das Benutzerkonto, das Sie verwenden möchten, über die Rechte zum Zugriff auf diesen Pool verfügt. Zu Verbindungsservern der Version 5.3.x finden Sie weitere Informationen in den Themen zur Erstellung von Desktop-Pools im Dokument *ViewAdministration von* . Zu Verbindungsservern der Version 6.0 und höher finden Sie weitere Informationen in den Themen zur Erstellung von Desktop- und Anwendungspools im Dokument *Einrichten von Desktop- und Anwendungspools in View*.
- 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 Touch ID-Authentifizierung mit Horizon Client 3.5 und höher 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 dazu finden Sie unter „Konfigurieren der biometrischen Authentifizierung“ im Dokument *Administration von View*.
- Um Endbenutzern das Speichern ihrer Kennwörter in Horizon Client zu ermöglichen, damit sie ihre Anmeldedaten nicht bei jeder Verbindungsherstellung zu einem Remote-Desktop oder einer Remoteanwendung eingeben müssen, konfigurieren Sie die Richtlinie für diese Funktion auf dem Verbindungsserver.

Benutzer können ihre Kennwörter speichern, wenn die Richtlinienkonfiguration dies zulässt und Horizon Client das vom Verbindungsserver bereitgestellte Serverzertifikat vollständig verifizieren kann. Anweisungen zur Konfiguration dieser Richtlinie finden Sie im Thema „Zulassen, dass Benutzer Anmeldeinformationen speichern“ des Kapitels „Einrichten der Benutzerauthentifizierung“ im Dokument *Administration von View*.

- Stellen Sie sicher, dass für den Desktop- oder Anwendungspool die Verwendung des VMware Blast-Anzeigeprotokolls oder des PCoIP-Anzeigeprotokolls eingerichtet ist. Zu View-Verbindungsservern der Version 5.3.x finden Sie weitere Informationen im Dokument *ViewAdministration von* . Zu Verbindungsservern der Version 6.0 und höher finden Sie weitere Informationen im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Installieren oder Aktualisieren von Horizon Client auf einem iOS-Gerät

Sie können Horizon Client von der VMware Downloads-Seite oder aus dem App Store installieren.

Voraussetzungen

- Wenn Sie das iOS-Gerät noch nicht eingerichtet haben, so holen Sie dies nun nach. Weitere Informationen finden Sie im Apple-Benutzerhandbuch.
- Stellen Sie sicher, dass Sie über die URL für eine Download-Seite verfügen, auf der sich das Horizon Client-Installationsprogramm befindet. Bei dieser URL kann es sich um die VMware Downloads-Seite unter <http://www.vmware.com/go/viewclients> oder um die URL für eine Verbindungsserver-Instanz handeln.

Vorgehensweise

- 1 Durchsuchen Sie den App Store auf Ihrem iOS-Gerät, Mac oder PC nach der Horizon Client-App oder navigieren Sie zur URL, um die Installationsdatei herunterzuladen.
- 2 Laden Sie die App herunter.
- 3 Verbinden Sie Ihr iOS-Gerät mit dem Computer, wenn Sie die App auf einen Mac oder PC heruntergeladen haben, und folgen Sie in iTunes den Anweisungen auf dem Bildschirm.
- 4 Um sicherzustellen, dass die Installation erfolgreich war, überprüfen Sie, ob das App-Symbol für **VMware View** (Horizon Client 3.0) oder **Horizon** (Horizon Client 3.1 oder höher) auf dem iOS-Gerät angezeigt wird.

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-secrid://`
- `com.rsa.secrid.iphone://`
- `com.rsa.secrid://`

Für Endbenutzer, die das Token über ein Antippen der URL installieren, wird nur das Präfix `viewclient-secrid://` unterstützt.

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 auswählen, die Horizon Client verwenden kann. Darüber hinaus können Sie die Schlüsselsteuerzeichenfolge angeben.

- In Horizon Client 3.0 bis 3.4 sind TLS v1.0 und TLS v1.1 standardmäßig aktiviert. Die standardmäßige Schlüsselsteuerzeichenfolge lautet „AES:!aNULL:@STRENGTH“.
- In Horizon Client 3.5 sind TLS v1.0, TLS v1.1 und TLS v1.2 standardmäßig aktiviert. Die standardmäßige Schlüsselsteuerzeichenfolge lautet „!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH“.
- In Horizon Client 4.0 und höher ist TLS v1.0 standardmäßig deaktiviert, TLS v1.1 und TLS v1.2 sind standardmäßig aktiviert und SSL v3 wurde entfernt. Die standardmäßige Schlüsselsteuerzeichenfolge lautet „!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH“.

Voraussetzungen

Überprüfen Sie das Sicherheitsprotokoll, das von der Verbindungsserver-Instanz verwendet werden kann. Wenn Sie ein Sicherheitsprotokoll für Horizon Client konfigurieren, das auf Ihrer Verbindungsserver-Instanz, mit der sich der Client verbindet, nicht aktiviert ist, tritt ein SSL-Fehler auf und die Verbindung schlägt fehl. Informationen zum Konfigurieren der Sicherheitsprotokolle, die von Verbindungsserver-Instanzen akzeptiert werden, finden Sie im Dokument zur *View-Sicherheit*.

Sie sollten die Sicherheitsprotokolle in Horizon Client nur ändern, wenn Sie von Ihrem View-Administrator dazu aufgefordert werden, oder wenn die aktuellen Einstellungen von Ihrer Verbindungsserver-Instanz nicht unterstützt werden.

Vorgehensweise

- 1 Öffnet den Bildschirm „Einstellungen“.

Option	Aktion
Horizon Client 3.0	In Ihrer iOS-App Einstellungen tippen Sie auf VMware View .
Horizon Client 3.1 bis 3.5	In Ihrer iOS-App Einstellungen tippen Sie auf Horizon .
Horizon Client 4.0 und höher	Tippen Sie auf Einstellungen am unteren Rand des Horizon Client-Bildschirms.

- 2 Tippen Sie auf **Erweiterte SSL-Optionen**.
- 3 (Horizon Client 3.0 bis 3.5) Stellen Sie sicher, dass die Option **Auf Standardeinstellungen zurücksetzen** auf „Aus“ eingestellt ist.
- 4 Zum Aktivieren oder Deaktivieren eines Sicherheitsprotokolls tippen Sie neben dem Namen des Sicherheitsprotokolls auf **Ein** bzw. **Aus**.
- 5 Um die Schlüsselsteuerzeichenfolge zu ändern, ersetzen Sie die Standardzeichenfolge.
- 6 (Optional) Wenn Sie zu den Standardeinstellungen zurückkehren möchten, tippen Sie auf die Option **Auf Standardeinstellungen zurücksetzen** zum Umschalten auf „Ein“ (Horizon Client 3.0 bis 3.5) oder Sie tippen auf **Zurücksetzen** rechts oben im Bildschirm (Horizon Client 4.0 und später).

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

Konfigurieren der VMware Blast-Optionen

In Horizon Client 4.0 und später können Sie die Optionen für das Decodieren und die Netzwerkprotokolle für Remote-Desktop- und -anwendungssitzungen konfigurieren, die das VMware Blast-Anzeigeprotokoll verwenden.

Voraussetzungen

Stellen Sie sicher, dass Sie über Horizon Client 4.0 oder höher verfügen. VMware Blast wird in früheren Horizon Client-Versionen nicht unterstützt. Diese Funktion erfordert auch Horizon Agent 7.0 oder höher.

Vorgehensweise

- 1 Tippen Sie auf **Einstellungen** am unteren Rand des Horizon Client-Bildschirms.
- 2 Tippen Sie auf **VMware Blast**.
- 3 Konfigurieren Sie die Optionen für das Decodieren und die Netzwerkprotokolle.

Option	Beschreibung
H.264	Wählen Sie diese Option aus, um die H.264-Decodierung in Horizon Client zuzulassen. Ist diese Option ausgewählt (Standardeinstellung), verwendet Horizon Client die H.264-Decodierung, wenn der Agent die H.264-Softwarecodierung unterstützt. Unterstützt der Agent die H.264-Softwarecodierung nicht, verwendet Horizon Client die JPG/PNG-Decodierung. Deaktivieren Sie diese Option, um immer die JPG/PNG-Decodierung zu verwenden.
UDP	Wählen Sie diese Option aus, um das UDP-Netzwerk in Horizon Client zuzulassen. Ist diese Option ausgewählt (Standardeinstellung), verwendet Horizon Client das UDP-Netzwerk, wenn eine UDP-Konnektivität verfügbar ist. Ist das UDP-Netzwerk gesperrt, verwendet Horizon Client das TCP-Netzwerk. Deaktivieren Sie diese Option, um immer das TCP-Netzwerk zu verwenden. HINWEIS UDP ist standardmäßig auf einem Horizon-Remote-Desktop deaktiviert. Damit das UDP-Netzwerk wirksam ist, muss es auf dem Desktop, dem Client und dem Blast Secure Gateway (BSG) aktiviert werden.

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

In Horizon Client 4.0 und höher können Sie konfigurieren, ob beim Start von Horizon Client der Bildschirm „Zuletzt verwendet“ oder Bildschirm „Server“ angezeigt werden soll.

Voraussetzungen

Stellen Sie sicher, dass Sie über Horizon Client 4.0 oder höher verfügen. Diese Funktion wird in früheren Horizon Client-Versionen nicht unterstützt.

Vorgehensweise

- 1 Tippen Sie auf **Einstellungen** am unteren Rand des Horizon Client-Bildschirms.
- 2 Tippen Sie auf **Standardansicht**.

- 3 Tippen Sie auf die gewünschte Option zur Auswahl der Standardansicht.

Option	Beschreibung
Zuletzt verwendet	Der Bildschirm „Zuletzt verwendet“ wird beim Start von Horizon Client angezeigt. Der Bildschirm „Zuletzt verwendet“ enthält Verknüpfungen zu den zuletzt verwendeten Desktops und Anwendungen. Dies ist die Standardeinstellung.
Server	Der Bildschirm „Server“ wird beim Start von Horizon Client angezeigt. Der Bildschirm „Server“ enthält Verknüpfungen zu den zu Horizon Client hinzugefügten Servern.

Die ausgewählte Standardansicht wird sofort wirksam.

Konfigurieren von AirWatch, um Horizon Client auf Mobilgeräten zur Verfügung zu stellen

Sie können AirWatch konfigurieren, um Horizon Client für Benutzer von mobilen Endgeräten zur Verfügung zu stellen. Optional können Sie eine Standardliste für Verbindungsserver-Instanzen anlegen. Die Verbindungsserver-Instanzen, die Sie festlegen, erscheinen als Verknüpfungen in Horizon Client.

Voraussetzungen

- Installieren und Bereitstellen von AirWatch. Siehe <http://www.air-watch.com>.
- Machen Sie sich mit der AirWatch-Konsole vertraut. Bei diesem Verfahren wird davon ausgegangen, dass Sie die AirWatch-Konsole bereits bedienen können. Weitere Informationen finden Sie in der AirWatch-Dokumentation oder der Online-Hilfe.

Die Integration von AirWatch wird in Horizon Client 3.2 und höher unterstützt.

Vorgehensweise

- 1 Melden Sie sich an der AirWatch-Konsole als Administrator an.
- 2 Wählen Sie **Konten > Benutzer > Listenansicht**, klicken Sie auf **Benutzer hinzufügen** und fügen Sie Benutzerkonten für die Benutzer hinzu, die Horizon Client auf ihren Mobilgeräten ausführen werden.
- 3 Wählen Sie **Konten > Benutzer > Benutzergruppen**, klicken Sie auf **Hinzufügen** und erstellen Sie eine Benutzergruppe für die von Ihnen erstellten Benutzerkonten.
- 4 Laden Sie die Horizon Client-Anwendung und fügen Sie sie zu AirWatch hinzu.
 - a Wählen Sie **Apps & Bücher > Anwendungen > Listenansicht** und klicken Sie auf der Registerkarte **Öffentlich** auf **Anwendung hinzufügen**.
 - b Suchen und wählen Sie VMware Horizon Client für Apple iOS im App Store aus.
 - c Geben Sie auf der Registerkarte **Info** einen Anwendungsnamen ein und geben Sie die unterstützten Modelle der mobilen Endgeräte ein.
 - d Weisen Sie auf der Registerkarte **Zuweisung** die Horizon Client-Anwendung der Benutzergruppe zu, die Sie erstellt haben.

- e (Optional) Zur Konfiguration einer Standard-Verbindungsserver-Instanz auf der Registerkarte **Bereitstellung** gehen Sie wie folgt vor: Aktivieren Sie das Kontrollkästchen **Anwendungskonfiguration senden**, geben Sie **Server** in das Textfeld **Konfigurationsschlüssel** ein, wählen Sie **String** aus dem Dropdown-Menü **Werttyp** aus und geben Sie eine IP-Adresse oder einen Hostnamen in das Textfeld **Konfigurationswert** ein.

Server beachten die Groß- und Kleinschreibung. Um eine Liste an Verbindungsserver-Instanzen festzulegen, geben Sie mehrere IP-Adressen oder Hostnamen, durch Kommas getrennt, in das Textfeld **Konfigurationswert** ein.

Zum Beispiel: **123.456.1.1, viewserver4.mydomain.com, 123.456.1.2**

HINWEIS Diese Funktion wird erst ab iOS 7 unterstützt. Sie können keine Standardliste mit Verbindungsservern an ein Gerät mit iOS 6 übertragen.

- f Veröffentlichen Sie die Horizon Client-Anwendung.
- 5 Installieren und richten Sie den AirWatch MDM Agent auf jedem iOS-Gerät ein.
Sie können den AirWatch MDM Agent von iTunes herunterladen.
 - 6 Installieren Sie die AirWatch-Konsole mithilfe der Horizon Client-Anwendung auf den Mobilgeräten.
Sie können die Horizon Client-Anwendung vor dem Datum des Inkrafttretens auf der Registerkarte **Bereitstellung** nicht installieren.

AirWatch stellt Horizon Client auf Mobilgeräten in der Benutzergruppe bereit, die Sie mit der Horizon Client-Anwendung verknüpfen.

Wenn ein Benutzer Horizon Client aufruft, kommuniziert Horizon Client mit dem AirWatch MDM Agent auf dem Gerät. Wenn Sie eine Standardliste der Verbindungsserver-Instanzen konfigurieren, überträgt AirWatch die Serverinformationen an den AirWatch MDM Agent auf dem Gerät. Für diese Server erscheinen Verknüpfungen in Horizon Client.

Weiter

Sie können die AirWatch-Konsole verwenden, um die Horizon Client-Anwendung zu bearbeiten und diese Änderungen an Mobilgeräte zu übertragen. So können Sie der Serverliste für die Horizon Client-Anwendung beispielsweise eine Standard-Verbindungsserver-Instanz hinzufügen.

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.

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

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, oder ein Administrator kann nach der Installation eine entsprechende Option in View 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 entwickelte	Nein	VMware
Produktname	Nein	VMware Horizon Client
Client-Produktversion	Nein	(Das Format lautet <i>x.x.x-yyyyyy</i> , wobei <i>x.x.x</i> für die Client-Versionsnummer und <i>yyyyyy</i> für die Build-Nummer steht.)
Client-Binärarchitektur	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ i386 ■ x86_64 ■ arm
Client-Build-Name	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ unbekannt (für Windows Store)
Host-Betriebssystemarchitektur	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ x86_64 ■ i386 ■ armv71 ■ ARM
Hostsystem-Modell	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)

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

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Hostsystem-CPU	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 4096 ■ unbekannt (für Windows Store)
Anzahl der angeschlossenen USB-Geräte	Nein	2 (Die Umleitung von USB-Geräten wird nur für Linux-, Windows- und Mac OS X-Clients unterstützt.)
Maximale Anzahl gleichzeitiger USB-Geräteverbindungen	Nein	2
Hersteller-ID des USB-Geräts	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Kingston ■ NEC ■ Nokia ■ Wacom
Produkt-ID des USB-Geräts	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ DataTraveler ■ Gamepad ■ Speicherlaufwerk ■ Kabellose Maus
USB-Gerätefamilie	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Sicherheit ■ Eingabegeräte ■ Bildverarbeitung
Nutzungszähler für das USB-Gerät	Nein	(Gibt an, wie oft das Gerät gemeinsam genutzt wurde)

Verwenden von URIs zur Konfiguration von Horizon Client

2

Mithilfe so genannter Uniform Resource Identifiers (URIs) können Sie eine Webseite oder E-Mail mit verschiedenen Verknüpfungen erstellen, auf die die Endbenutzer zum Start von Horizon Client, zur Verbindung mit dem Verbindungsserver oder zum Start eines bestimmten Desktops oder einer bestimmten Anwendung mit bestimmten Konfigurationsoptionen klicken.

Sie können die Verbindungsherstellung mit einem Remote-Desktop oder einer Anwendung durch Erstellen von Web- oder E-Mail-Verknüpfungen für die Endbenutzer deutlich vereinfachen. Diese Verknüpfungen werden durch die Generierung von URIs erstellt, die einige oder alle der folgenden Informationen bereitstellen, sodass die Endbenutzer diese nicht angeben müssen:

- Adresse des Verbindungsservers
- Portnummer für den Verbindungsserver
- Active Directory-Benutzername
- RADIUS- oder RSA SecurID-Benutzername, falls dieser nicht mit dem Active Directory-Benutzernamen identisch ist
- Domänenname
- Desktop- oder Anwendungsanzeigename
- Aktionen, darunter „Zurücksetzen“, „Abmelden“ und „Sitzung starten“

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

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

Dieses Kapitel behandelt die folgenden Themen:

- [„Syntax für die Erstellung von vmware-view-URIs“](#), auf Seite 22
- [„Beispiele für vmware-view-URIs“](#), auf Seite 24

Syntax für die Erstellung von vmware-view-URIs

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

URI-Spezifikation

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

```
vmware-view://[authority-part][path-part][?query-part]
```

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

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

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

authority-part

Gibt die Serveradresse und optional einen Benutzernamen, eine nicht standardmäßige Portnummer oder beides an. Beachten Sie, dass Unterstriche (`_`) in Servernamen nicht unterstützt werden. Die Servernamen müssen der DNS-Syntax entsprechen.

Verwenden Sie zur Angabe eines Benutzernamens die folgende Syntax:

```
user1@server-address
```

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

Verwenden Sie zur Angabe einer Portnummer die folgende Syntax:

```
server-address:port-number
```

path-part

Gibt den Desktop oder die Anwendung an. Verwenden Sie den Anzeigenamen des Desktops oder der Anwendung. Dieser Name wurde in View Administrator beim Erstellen des Desktop- oder Anwendungspools angegeben. Weist der Anzeigename ein Leerzeichen auf, müssen Sie den Codierungsmechanismus `%20` verwenden, um das Leerzeichen darzustellen.

query-part

Gibt die zu verwendenden Konfigurationsoptionen oder die durchzuführenden Desktop- oder Anwendungsaktionen an. Für die Abfragen muss die Groß- und Kleinschreibung nicht beachtet werden. Verwenden Sie für den Einsatz mehrerer Abfragen das kaufmännische Und-Zeichen (`&`) zwischen den Abfragen. Sollten die Abfragen miteinander in Konflikt stehen, wird die letzte Abfrage in der Liste verwendet. Verwenden Sie die folgende Syntax:

```
query1=value1[&query2=value2...]
```

Unterstützte Abfragen

In diesem Abschnitt werden die Abfragen aufgeführt, die für diesen Horizon Client-Typ unterstützt werden. Wenn Sie URIs für mehrere Clienttypen generieren, so zum Beispiel für Desktop-Clients oder mobile Clients, finden Sie für jede Art von Clientssystem weitere Anweisungen im Handbuch *Verwendung von VMware Horizon Client*.

action

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

Wert	Beschreibung
browse	Zeigt eine Liste der verfügbaren, auf dem angegebenen Server gehosteten Desktops und Anwendungen an. Bei Verwendung dieser Aktion müssen Sie keinen Desktop bzw. keine Anwendung angeben. Wenn Sie die Aktion <code>browse</code> verwenden und einen Desktop oder eine Anwendung angeben, wird der Desktop oder die Anwendung in der Liste der verfügbaren Elemente hervorgehoben.
start-session	Startet den angegebenen Desktop oder die angegebene Anwendung. Wenn keine „action“-Abfrage bereitgestellt wird und der Desktop- oder Anwendungsname angegeben wird, ist <code>start-session</code> die Standardaktion.
reset	Führt den angegebenen Desktop bzw. die angegebene Anwendung herunter und startet ihn bzw. sie neu. Nicht gespeicherte Daten gehen verloren. Das Zurücksetzen eines Remote-Desktops entspricht dem Betätigen der Reset-Taste auf einem physischen PC. Bei Angabe einer Anwendung in Horizon Client 3.0 wird die Aktion ignoriert.
logoff	Meldet den Benutzer vom Gastbetriebssystem auf dem Remote-Desktop ab. Wenn Sie eine Anwendung angeben, wird die Aktion ignoriert oder der Endbenutzer sieht die Warnmeldung „Ungültige URI-Aktion“.

appProtocol

Gültige Werte für Remoteanwendungen sind **PCOIP** und **BLAST**. Zur Angabe von PCoIP verwenden Sie beispielsweise die Syntax `appProtocol=PCOIP`. Diese Abfrage wird nur in Horizon Client 4.0 und höher unterstützt. In früheren Versionen von Horizon Client wird für Remoteanwendungen immer PCoIP verwendet.

defaultLaunchView

(Horizon Client 4.0 und höher) Legt die Standardstartansicht für Horizon Client fest. Gültige Werte sind **recent** und **servers**.

desktopProtocol

Gültige Werte für Remote-Desktops sind **PCOIP** und **BLAST**. Zur Angabe von PCoIP verwenden Sie beispielsweise die Syntax `desktopProtocol=PCOIP`. Diese Abfrage wird nur in Horizon Client 4.0 und höher unterstützt. In früheren Versionen von Horizon Client wird für Remote-Desktops immer PCoIP verwendet.

domainName

Der NETBIOS-Domänenname, der mit dem Benutzer verknüpft ist, der eine Verbindung zum Remote-Desktop oder zur Remoteanwendung herstellt. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.

tokenUserName

Gibt den RSA- oder RADIUS-Benutzernamen an. Verwenden Sie diese Abfrage nur, wenn der RSA- oder RADIUS-Benutzername nicht mit dem Active Directory-Benutzernamen identisch ist. Wenn Sie diese Abfrage nicht angeben und die RSA- oder RADIUS-Authentifizierung erforderlich ist, wird der Windows-Benutzername verwendet. Die Syntax lautet `tokenUserName=name`.

Beispiele für vmware-view-URIs

Sie können Hypertext-Links oder Schaltflächen mit dem URI-Schema `vmware-view` erstellen und diese Links in E-Mails oder auf einer Webseite einbinden. Ihre Endbenutzer können dann auf diese Links klicken, um beispielsweise einen bestimmten Remote-Desktop mit den von Ihnen angegebenen Startoptionen zu starten.

URI-Syntaxbeispiele

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

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

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

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

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

Dieser URI hat die gleiche Wirkung wie im vorherigen Beispiel, außer dass er den nicht standardmäßigen Port 7555 für den Verbindungsserver verwendet. (Der standardmäßige Port lautet 443.) Da eine Desktop-ID bereitgestellt wird, wird der Desktop gestartet, obwohl die Aktion `start-session` nicht im URI enthalten ist.

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

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

- 4 `vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST`

Horizon Client wird gestartet und stellt eine Verbindung zum `view.mycompany.com`-Server her. In das Anmeldefeld muss der Benutzer den Benutzernamen, den Domännennamen und das Kennwort eingeben. Nach einer erfolgreichen Anmeldung wird vom Client eine Verbindung mit der Anwendung hergestellt, deren Anzeigename als **Berechnung** dargestellt wird. Die Verbindung nutzt das VMware Blast-Anzeigeprotokoll.

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

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

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

Horizon Client wird gestartet und der Benutzer wird zur Anmeldeaufforderung für die Verbindung mit dem Server `view.mycompany.com` geleitet.

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

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

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

8 vmware-view://

Wenn Client bereits ausgeführt wird, wird die Horizon Client-App im Vordergrund angezeigt. Wenn der Client noch nicht ausgeführt wird, wird Horizon Client gestartet.

9 vmware-view://?defaultlaunchview=recent

Horizon Client wird gestartet und der zuletzt verwendete Bildschirm wird dargestellt.

Beispiel für HTML-Code

Sie können URIs verwenden, um Hypertext-Links und Schaltflächen zu erstellen, die in E-Mails oder auf Webseiten eingebunden werden können. Die folgenden Beispiele veranschaulichen, wie Sie den URI aus dem ersten Beispiel verwenden, um einen Hypertext-Link mit dem Text **Test Link** besagt und eine Schaltfläche mit dem Text **TestButton** zu codieren.

```
<html>
<body>

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

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

</body>
</html>
```


Verwalten der Remote-Desktop- und Anwendungsverbindungen

3

Mit Horizon Client können Sie eine Verbindung zu einem Verbindungsserver oder Sicherheitsserver herstellen, die Liste der Verbindungsserver 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:

- [„Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung“](#), auf Seite 27
- [„Zertifikatsprüfungsmodi für Horizon Client“](#), auf Seite 31
- [„Verwalten von gespeicherten Servern“](#), auf Seite 32
- [„Auswählen eines Remote-Desktops oder einer Remoteanwendung als Favorit“](#), auf Seite 33
- [„Trennen der Verbindung mit einem Remote-Desktop oder einer Remoteanwendung“](#), auf Seite 34
- [„Abmelden von einem Remote-Desktop“](#), auf Seite 34
- [„Verwalten von Desktop- und Anwendungsverknüpfungen“](#), auf Seite 35
- [„Verwenden von 3D Touch mit Horizon Client“](#), auf Seite 35
- [„Verwenden der Spotlight-Suche mit Horizon Client“](#), auf Seite 36
- [„Verwenden von Split View und Slide Over mit Horizon Client“](#), auf Seite 36

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 zur Anmeldung benötigten Informationen, so etwa den Active Directory-Benutzernamen und das Active Directory-Kennwort, den RSA SecurID-Benutzernamen und -Passcode oder den RADIUS-Authentifizierungsbenutzernamen oder -Passcode.
- Besorgen Sie sich den 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 12 beschriebenen administrativen Aufgaben aus.
- Wenn Sie sich außerhalb des Firmennetzwerks befinden und für den Zugriff auf den Remote-Desktop keinen Sicherheitsserver verwenden, stellen Sie sicher, dass Ihr Clientgerät für die Verwendung einer VPN-Verbindung konfiguriert ist, und aktivieren Sie diese Verbindung.

WICHTIG VMware empfiehlt die Verwendung eines Sicherheitsservers anstelle eines VPNs.

Wenn Ihr Unternehmen ein internes WLAN besitzt, das über einen Router Zugriff auf Remotedesktops ermöglicht, die von Ihrem Gerät genutzt werden können, brauchen Sie keinen View-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. Beachten Sie, dass Unterstriche (_) in Servernamen nicht unterstützt werden. Sie benötigen zudem auch die Portnummer, wenn es sich beim Port nicht um 443 handelt.
- 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 14.
- Konfigurieren Sie den Zertifikatsprüfungsmodus für das SSL-Zertifikat, das vom Verbindungsserver präsentiert wird. Siehe [„Zertifikatsprüfungsmodi für Horizon Client“](#), auf Seite 31.
- Wenn Sie Horizon Client 3.5 oder höher besitzen und eine Authentifizierung über Touch ID planen, müssen Sie der Touch ID- und Passcode-Einstellung auf Ihrem iOS-Gerät mindestens einen Fingerabdruck hinzufügen. Sämtliche Touch ID-Authentifizierungsanforderungen finden Sie unter [„Anforderungen für Authentifizierung über Touch ID“](#), auf Seite 11.

Vorgehensweise

- 1 Sollte eine VPN-Verbindung erforderlich sein, müssen Sie das VPN aktivieren.
- 2 Tippen Sie auf dem Startbildschirm auf das App-Symbol **VMware View** (Horizon Client 3.0) bzw. **Horizon** (Horizon Client 3.1 und höher).

- 3 Stellen Sie eine Verbindung mit einem Server her.

Option	Aktion
Horizon Client 3.0	<ul style="list-style-type: none"> ■ Um eine Verbindung mit einem neuen Server herzustellen, tippen Sie auf Server hinzufügen, geben Sie den Namen eines Servers ein und tippen Sie auf Verbinden. ■ Um eine Verbindung mit einem vorhandenen Server herzustellen, tippen Sie im Bildschirm „Zuletzt verwendete Verbindungen“ auf den Pfeil (>) neben dem Servernamen.
Horizon Client 3.1 und höher	<ul style="list-style-type: none"> ■ Um eine Verbindung mit einem neuen Server herzustellen, geben Sie den Namen eines Servers sowie eine Beschreibung (optional) ein und tippen Sie auf Server hinzufügen. ■ Um eine Verbindung mit einem vorhandenen Server herzustellen, tippen Sie im Bildschirm „Server“ 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 eine Smartcard erforderlich ist oder optional verwendet werden kann, wählen Sie das zu verwendende Zertifikat für Smartcards aus und geben Sie Ihre PIN ein.

Wenn für die Smartcard nur ein Zertifikat zur Verfügung steht, ist dieses Zertifikat bereits ausgewählt. Falls mehrere Zertifikate vorhanden sind, führen Sie ggf. einen Bildlauf durch die Zertifikate durch.

- 5 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.

- 6 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.

- 7 (Optional) Wenn die Einstellung **Touch ID aktivieren** verfügbar ist, aktivieren Sie diese für die Touch ID-Authentifizierung.

Die Einstellung **Touch ID aktivieren** ist nur verfügbar, wenn die biometrische Authentifizierung auf dem Server aktiviert ist und Sie sich nicht bereits mit der Touch ID authentifiziert haben.

- 8 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) Tippen Sie, um die Option **Dieses Kennwort speichern** auf „Ein“ umzuschalten, wenn Ihr Administrator diese Funktion aktiviert hat und das Serverzertifikat vollständig überprüft werden kann.
 - d Tippen Sie auf **Anmelden**.

Wenn die Touch ID aktiviert ist und Sie sich zum ersten Mal anmelden, werden Ihre Active Directory-Anmeldedaten sicher im Schlüsselbund des iOS-Gerätes für die zukünftige Verwendung gespeichert.

- 9 Wenn Sie zur Touch ID-Authentifizierung aufgefordert werden, setzen Sie Ihren Finger auf die Schaltfläche **Start**.
- 10 (Optional) Tippen Sie auf das Symbol der Einstellungen für das Anzeigeprotokoll rechts oben im Bildschirm, um das gewünschte Anzeigeprotokoll auszuwählen.

PCoIP bietet ein optimiertes PC-Benutzererlebnis bei der Bereitstellung von Bildern sowie Audio- und Videoinhalten im LAN oder WAN. **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**.

Sie können ein Anzeigeprotokoll in Horizon Client 4.0 und höher auswählen. Die Versionen Horizon Client 3.x verwenden immer das PCoIP-Anzeigeprotokoll.

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

Wenn Sie die Smartcard-Authentifizierung verwenden, werden Sie nicht erneut zur Eingabe Ihrer PIN aufgefordert, der Anmeldevorgang nimmt jedoch mehr Zeit in Anspruch als bei Verwendung der Active Directory-Authentifizierung.

Wenn Sie eine Verbindung mit einem sitzungsbasierten Remote-Desktop auf einem Microsoft RDS-Host herstellen und für den Desktop bereits die Verwendung des Microsoft RDP-Anzeigeprotokolls festgelegt ist, kann die Verbindung nicht sofort hergestellt werden. Sie werden aufgefordert, sich vom Remote-Betriebssystem abzumelden, damit eine Verbindung unter Verwendung des PCoIP-Anzeigeprotokolls oder des VMware Blast-Anzeigeprotokolls hergestellt werden kann. VMware Blast erfordert Horizon Client 4.0 oder höher und Horizon Agent 7.0 oder höher.

Nachdem Sie zum ersten Mal eine Verbindung mit einem Desktop bzw. einer Anwendung hergestellt haben, wird auf dem Bildschirm „Zuletzt verwendete Verbindungen“ (Horizon Client 3.0) oder „Zuletzt verwendet“ (Horizon Client 3.1 und höher) eine Verknüpfung für den Desktop bzw. die Anwendung gespeichert. Wenn Sie das nächste Mal eine Verbindung mit dem Remote-Desktop oder der Remoteanwendung herstellen möchten, können Sie einfach auf die Verknüpfung tippen, statt den Namen des Servers einzugeben.

Zertifikatsprüfungsmodi 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 unbekanntenen oder nicht als vertrauenswürdig eingestuften Zertifizierungsstelle (CA) signiert worden? Selbstsignierte Zertifikate sind ein Typ der nicht als vertrauenswürdig eingestuften CA.

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

WICHTIG Anweisungen zur Verteilung eines selbstsignierten Stammzertifikats, das die Benutzer auf ihren iOS-Geräten installieren können, finden Sie auf der Apple-Website. Informationen zu iPads finden Sie beispielsweise unter http://www.apple.com/ipad/business/docs/iPad_Certificates.pdf.

Wie Sie den Modus der Zertifikatsprüfung in Abhängigkeit von Ihrer Horizon Client-Version einrichten. In Horizon Client 3.0 tippen Sie auf **VMware View** in Ihrer iOS-App **Einstellungen** und dann auf **Zertifikatsprüfungsmodus**. In Horizon Client 3.1 bis 3.5 tippen Sie auf **Horizon** in Ihrer iOS-App **Einstellungen** und dann auf **Zertifikatsprüfungsmodus**. Tippen Sie in Horizon Client 4.0 und höher auf **Einstellungen** am unteren Rand des Horizon Client-Bildschirms und dann auf **Überprüfungsmodus für Serverzertifikate**. 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.

Verwalten von gespeicherten Servern

Beim Herstellen der Verbindung zu einem View Server speichert Horizon Client den Servernamen im Bildschirm „Zuletzt verwendete Verbindungen“ (Horizon Client 3.0) oder im Bildschirm „Server“ (Horizon Client 3.1 und höher). Sie können gespeicherte Server bearbeiten und entfernen.

Horizon Client speichert den Server selbst dann, wenn Sie den Namen oder die IP-Adresse falsch eingeben. Sie können diese Informationen löschen bzw. ändern.

WICHTIG Um in Horizon Client 3.0 eine Verbindung zu einem Server herzustellen, tippen Sie auf den Pfeil (>) neben dem Servernamen. Um in Horizon Client 3.1 eine Verbindung zu einem Server herzustellen, tippen Sie auf den Servernamen.

Vorgehensweise

- 1 Zeigen Sie die gespeicherten Server an.

Option	Aktion
Horizon Client 3.0	Tippen Sie im Fenster „Zuletzt verwendete Verbindungen“ in der oberen linken Ecke des Bildschirms auf das Symbol „Cloud“.
Horizon Client 3.1 und höher	Tippen Sie auf Server (Cloud-Symbol) im unteren Bereich des Bildschirms.

- 2 Tippen Sie zum Verwalten gespeicherter Server in der oberen rechten Ecke in Horizon Client 3.0 auf **Bearbeiten**, nehmen Sie die gewünschten Änderungen vor und tippen Sie auf **Fertig**.

Option	Aktion
Den Namen eines Servers ändern	Tippen Sie auf den Servernamen. Im Text erscheint ein Cursor, sodass Sie ihn bearbeiten können.
Einen Server aus der Liste entfernen	Tippen Sie auf das rote Minuszeichen neben dem Servernamen oder der Adresse und dann auf Löschen . Sie können auch Kennwort entfernen auswählen, wenn Sie Ihr Kennwort zuvor gespeichert haben. Die mit dem Server verbundenen Desktop- und Anwendungs-Verknüpfungen werden ebenfalls gelöscht.
Reihenfolge der Server in der Liste ändern	Tippen Sie auf das Symbol auf der rechten Seite des Servernamens und halten Sie ihn gedrückt. Wenn sich die Zeile bewegt, ziehen Sie den Namen an die gewünschte Stelle in der Liste.

- 3 Um gespeicherte Server in Horizon Client 3.1 und höher zu verwalten, berühren Sie das Server-Symbol und halten es so lange, bis das Kontextmenü angezeigt wird.

Option	Aktion
Den Benutzernamen, die Domäne, den Servernamen oder die Beschreibung ändern	<ol style="list-style-type: none"> a Tippen Sie im Kontextmenü auf Server bearbeiten. b Nehmen Sie auf dem Bildschirm „Server bearbeiten“ Ihre Änderungen vor. c Tippen Sie auf Update, um Ihre Änderungen zu speichern.
Einen Server entfernen	Tippen Sie im Kontextmenü auf Server löschen . Die mit dem Server verbundenen Desktop- und Anwendungs-Verknüpfungen werden ebenfalls gelöscht.
Gespeichertes Kennwort löschen	Tippen Sie im Kontextmenü auf Kennwort löschen . Diese Option ist nur dann verfügbar, wenn Sie zuvor Ihr Kennwort gespeichert haben.
Touch ID deaktivieren	(Horizon Client 3.5 und höher) gespeichert wurde, und tippen Sie auf Abmelden . Diese Option ist nur verfügbar, wenn Sie vorher die Touch ID aktiviert haben.

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 Stellen Sie eine Verbindung mit dem Server her.

Option	Beschreibung
Horizon Client 3.0	Tippen Sie im Fenster „Zuletzt verwendete Verbindungen“ in der oberen linken Ecke auf das Symbol „Cloud“ und tippen Sie auf den Servernamen.
Horizon Client 3.1 und höher	Tippen Sie im unteren Bereich des Bildschirms auf Server (Cloud-Symbol) und anschließend auf das Serversymbol.

- 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	Aktion
Favorit auswählen	<p>Horizon Client 3.0: Berühren und halten Sie den Desktop- oder Anwendungsnamen, bis das Kontextmenü angezeigt wird. Tippen Sie dann auf Als Favorit markieren. In der oberen rechten Ecke des Desktop- bzw. Anwendungsnamens wird ein Sternchen angezeigt.</p> <p>Horizon Client 3.1 und höher: Berühren und halten Sie 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 Seite „Favoriten“.</p>
Die Auswahl eines Favoriten aufheben	<p>Horizon Client 3.0: Berühren und halten Sie den Desktop- oder 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.</p> <p>Horizon Client 3.1 und höher: Berühren und halten Sie den Desktop- oder 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 Seite „Favoriten“.</p>

- 4 (Optional) Tippen Sie in Horizon Client 3.1 oder höher auf **Favoriten** (Sternchensymbol) im unteren Bereich des Bildschirms, um nur die bevorzugten Desktops bzw. Anwendungen anzuzeigen.

Sie können im unteren Bereich des Bildschirms auf **Alle** (Cloud-Symbol) 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 bei dem Remote-Desktop oder der Remoteanwendung angemeldet sind, können Sie die Verbindung trennen, indem Sie auf das kreisförmige Menüsymbol für die Horizon Client-Tools und dann auf das Symbol **Verbindung trennen** tippen.

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

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 27 vertraut machen.

Vorgehensweise

- 1 Stellen Sie eine Verbindung mit dem Server her.

Option	Beschreibung
Horizon Client 3.0	Tippen Sie im Fenster „Zuletzt verwendete Verbindungen“ auf das Symbol „Cloud“ in der oberen linken Bildschirmcke und anschließend auf den Pfeil (>) neben dem Servernamen.
Horizon Client 3.1 und höher	Tippen Sie im unteren Bereich des Bildschirms auf Server (Cloud-Symbol) und anschließend auf das Serversymbol.

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

Weiter

Tippen Sie auf die Schaltfläche **Abmelden** in der oberen linken Ecke des Bildschirms, 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.

Desktop- und Anwendungsverknüpfungen können auf mehreren Seiten erscheinen. Wenn Sie über die Seiten wischen, werden weitere Verknüpfungen angezeigt. Horizon Client erstellt nach Bedarf neue Seiten für Ihre Verknüpfungen.

Vorgehensweise

- Führen Sie diese Schritte aus, um eine Desktop- oder Anwendungsverknüpfung vom Bildschirm „Zuletzt verwendete Verbindungen“ (Horizon Client 3.0) oder vom Bildschirm „Zuletzt verwendet“ (Horizon Client 3.1 und höher) zu entfernen.
 - a Berühren und halten Sie die Verknüpfung.
 - b Tippen Sie auf die Schaltfläche **X**.
- Wenn Sie eine Desktop- oder Anwendungsverknüpfung verschieben möchten, berühren und halten Sie die Verknüpfung. Ziehen Sie dann das Element an die neue Position und tippen Sie auf **Fertig**.
Eine Verknüpfung kann nur auf eine andere Seite gezogen werden, wenn diese Seite bereits vorhanden ist.

Verwenden von 3D Touch mit Horizon Client

Mit Horizon Client 4.0 oder höher können Sie Peek- und Pop-Gesten zur Interaktion mit Horizon Client auf einem 3D Touch-fähigen iPhone 6s oder iPhone 6s Plus verwenden.

Verwenden von Peek und Pop mit der Horizon-App auf Ihrer Startseite

Sie haben die Möglichkeit, mit Peek in der **Horizon**-App auf Ihrer Startseite ein Quick-Actions-Menü auszuwählen. Im Quick-Actions-Menü können Sie durch Antippen von **Verbindung mit dem letzten Server herstellen** schnell eine Verbindung mit dem zuletzt verwendeten Server herstellen. Ist kein solcher Server vorhanden, haben Sie die Möglichkeit, durch Antippen von **Verbindung mit dem letzten Server herstellen** einen neuen Server hinzuzufügen.

Nachdem Sie mit einem Remote-Desktop oder mit einer Remoteanwendung eine Verbindung hergestellt haben, fügt Horizon Client dem Quick-Actions-Menü eine Verknüpfung für den Desktop oder die Anwendung hinzu. Wenn Sie sich beispielsweise mit einem Remote-Desktop namens Win7 verbinden, fügt Horizon Client **Mit Win7 verbinden** hinzu. Durch Tippen auf eine Verknüpfung wird dann schnell eine Verbindung mit einem Remote-Desktop oder mit einer Remoteanwendung hergestellt. Das **Horizon**-Symbol des Quick-Actions-Menüs kann bis zu drei Verknüpfungen enthalten.

Verwenden von Peek und Pop in Horizon Client

Auf dem Auswahlbildschirm für Desktops und Anwendungen können Sie durch Peek auf einen Remote-Desktop oder eine Remoteanwendung ein Quick-Actions-Menü aufrufen. Sie haben die Möglichkeit, durch Antippen im Quick-Actions-Menü eine Verbindung herzustellen, sich abzumelden, einen Favoriten zu markieren und andere Aktionen durchzuführen, je nach Remote-Desktop und Remoteanwendung. Sie können auch durch Pop auf einen Remote-Desktop oder eine Remoteanwendung eine Verbindung dazu herstellen.

Quick-Actions-Menüs sind auch in den Bildschirmen „Server“, „Zuletzt verwendet“ und „Favoriten“ verfügbar. Auf dem Bildschirm „Server“ können Sie beispielsweise mit Peek auf einen gespeicherten Server und durch Antippen der entsprechenden Option im Quick-Actions-Menü den Server bearbeiten, entfernen oder eine Verbindung dazu herstellen. Auf dem Bildschirm „Zuletzt verwendet“ haben Sie die Möglichkeit,

mit Peek auf eine Remote-Desktop- oder Remoteanwendungsverknüpfung und durch Antippen der entsprechenden Option im Quick-Actions-Menü die Verknüpfung zu entfernen oder eine Verbindung zum Desktop oder zur Anwendung herzustellen. Sie können auch mit Pop auf einen Server oder eine Remote-Desktop- oder Remoteanwendungsverknüpfung eine Verbindung herstellen.

Aktivieren von Peek für die Horizon Client -Tools

Wenn Sie mit einem Remote-Desktop oder einer Remoteanwendung verbunden sind, wird standardmäßig das kreisförmige Menüsymbol für die Horizon Client-Tools in der Bildschirmmitte angezeigt. Tippen Sie darauf, um das Menü zu erweitern und Symbole für jedes Werkzeug anzuzeigen, das Sie jeweils durch Antippen auswählen können. Erläuterungen zu den Grafiken für das kreisförmige Menüsymbol und für die Tools-Symbole finden Sie unter [Tabelle 4-6](#).

Wenn Sie Peek für die Horizon Client-Tools aktivieren, wird das kreisförmige Menüsymbol für die Horizon Client-Tools nicht angezeigt. Um die Symbole für jedes Tool darzustellen, drücken Sie auf eine beliebige Stelle auf dem Bildschirm.

Um Peek für die Horizon Client-Tools zu aktivieren, tippen Sie auf **Einstellungen** am unteren Rand des Horizon Client-Bildschirms, dann auf **Touch** und setzen Sie die Einstellung **Menüvorschau einblenden** auf „Ein“. Wenn Sie mit einem Remote-Desktop oder mit einer Remoteanwendung verbunden sind, können Sie mit den Horizon Client-Tools die Einstellung **Menüvorschau einblenden** aktivieren. Öffnen Sie durch Tippen auf das kreisförmige Menüsymbol und auf das Einstellungensymbol das Dialogfeld „Optionen“ und setzen Sie die Einstellung **Menüvorschau einblenden** auf „Ein“.

Verwenden der Spotlight-Suche mit Horizon Client

Mit Horizon Client 4.0 und höher können Sie auf iOS 9.x-Geräten mit der Spotlight-Suche nach Remote-Desktops und -anwendungen suchen und mit diesen eine Verbindung herstellen.

Wenn Sie sich bei einem Server in Horizon Client anmelden, werden die Remote-Desktops und -anwendungen auf dem Server dem Spotlight-Index hinzugefügt. Es werden dabei nur die Remote-Desktops und -anwendungen des Servers indexiert, bei dem Sie sich zuletzt angemeldet haben.

Um mit der Spotlight-Suche nach einem bestimmten Remote-Desktop oder nach einer bestimmten Remoteanwendung zu suchen, geben Sie den jeweiligen Namen komplett oder teilweise in das Spotlight-Suchfeld ein. Um beispielsweise einen Remote-Desktop namens „Win 2008-RDS-Desktop“ zu finden, können Sie z. B. **Win** oder **RDS** eingeben.

Um mit der Spotlight-Suche nach Ihren als Favoriten markierten Remote-Desktops und -anwendungen zu suchen, geben Sie **favorite** in das Spotlight-Suchfeld ein. Um nach einem beliebigen Remote-Desktop oder nach einer beliebigen Remoteanwendung zu suchen, geben Sie **vmware** oder **horizon** in das Spotlight-Suchfeld ein. Die Suchergebnisse können aus bis zu zehn Elemente bestehen.

Für die Herstellung einer Verbindung mit einem Remote-Desktop oder mit einer Remoteanwendung tippen Sie auf den entsprechenden Namen in den Suchergebnissen. Wenn Sie aktuell mit keinem Server verbunden sind, wird der Horizon Client-Anmeldebildschirm eingeblendet, über den Sie sich dann anmelden können.

Verwenden von Split View und Slide Over mit Horizon Client

Mit Horizon Client 4.0 und höher können Sie Horizon Client Split View (Geteilte Darstellung) und Slide Over (Verschieben) für jedes iPad-Modell verwenden, das Split View sowie Slide Over unterstützt und iOS 9.x ausführt.

Mit Split View und Slide Over haben Sie die Möglichkeit, Horizon Client und eine andere App gleichzeitig zu öffnen. Sie können Horizon Client entweder als primäre oder als sekundäre App ausführen.

Wenn Sie Ihr Gerät drehen oder die vertikale Trennlinie verschieben, die die primäre und die sekundäre App trennt, passt Horizon Client die Größe des Fensters automatisch an. Wenn Sie mit einem Remote-Desktop verbunden sind, wird dieser automatisch an die Größe des Fensters angepasst, wenn für die Einstellung **Auflösung** die Option **Automatisch anpassen** gewählt wurde. Erläuterungen zur Festlegung der Auflösung für einen Remote-Desktop finden Sie unter [„Ändern der Einstellung für die Anzeigeauflösung“](#), auf Seite 53.

HINWEIS Horizon Client unterstützt nicht „Picture in Picture“.

Verwenden von Microsoft Windows-Desktops oder -Anwendungen auf einem mobilen Endgerät

4

Auf mobilen Geräten verfügt Horizon Client über zusätzliche Funktionen zur Unterstützung der Navigation.

Dieses Kapitel behandelt die folgenden Themen:

- „Funktionsunterstützungs-Matrix für iOS“, auf Seite 39
- „Externe Tastaturen und Eingabevorrichtungen“, auf Seite 42
- „Aktivieren des japanischen 106/109-Tastaturlayouts“, auf Seite 43
- „Verwenden der Echtzeit-Audio/Video-Funktion für Mikrofone“, auf Seite 43
- „Verwenden nativer Gesten auf Betriebssystemen mit Touch-Umleitung“, auf Seite 43
- „Verwenden der Unity Touch-Sidebar mit einem Remote-Desktop“, auf Seite 44
- „Verwenden der Unity Touch-Sidebar mit einer Remoteanwendung“, auf Seite 46
- „Horizon Client-Tools“, auf Seite 48
- „Gesten“, auf Seite 50
- „Multitasking“, auf Seite 51
- „Speichern von Dokumenten in einer Remoteanwendung“, auf Seite 52
- „Konfiguration von Horizon Client zur Unterstützung von umgekehrten Maustasten“, auf Seite 52
- „Bildschirmauflösungen und Verwendung externer Anzeigen“, auf Seite 52
- „PCoIP-Client-Bildcache“, auf Seite 53
- „Unterdrücken der Warnmeldung bezüglich der Mobilfunkdaten“, auf Seite 54
- „Internationalisierung“, auf Seite 54

Funktionsunterstützungs-Matrix für iOS

Einige Funktionen werden auf manchen Horizon Client-Typen unterstützt, auf anderen nicht.

Tabelle 4-1. Auf Windows-Desktops für iOS Horizon Client unterstützte Funktionen

Funktion	Windows 10-Desktop	Windows 8.x-Desktop	Windows 7-Desktop	Windows Vista-Desktop	Windows XP-Desktop	Windows Server 2008/2012 R2-Desktop
RSA SecurID oder RADIUS	X	X	X	Begrenzt	Begrenzt	X
Einmaliges Anmelden	X	X	X	Begrenzt	Begrenzt	X

Tabelle 4-1. Auf Windows-Desktops für iOS Horizon Client 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-Desktop
RDP-Anzeigeprotokoll						
PCoIP-Anzeigeprotokoll	X	X	X	Begrenzt	Begrenzt	X
VMware Blast-Anzeigeprotokoll	X	X	X			X
USB-Zugriff						
Echtzeit-Audio/Video (nur Audio-Eingang)	X	X	X			X
Wyse MMR						
Windows 7 MMR						
Virtuelles Drucken						
Standortbasiertes Drucken	X	X	X	Begrenzt	Begrenzt	X
Smartcards	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.

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 finden Sie im Dokument *Planung von View*.

Funktionsunterstützung für sitzungsbasierte 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 und höher.

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 auf einer physischen Maschine	Windows Server 2008 R2 RDS Host auf einer virtuellen Maschine	Windows Server 2012 RDS Host auf einer physischen Maschine	Windows Server 2012 RDS Host auf einer virtuellen Maschine
RSA SecurID oder RADIUS	X	X	X	X
Smartcard	View Agent 6.1 und höher	View Agent 6.1 und höher	View Agent 6.1 und höher	View Agent 6.1 und höher

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 (Fortsetzung)

Funktion	Windows Server 2008 R2 RDS Host auf einer physischen Maschine	Windows Server 2008 R2 RDS Host auf einer virtuellen Maschine	Windows Server 2012 RDS Host auf einer physischen Maschine	Windows Server 2012 RDS Host auf einer virtuellen Maschine
Einmaliges Anmelden	X	X	X	X
RDP-Anzeigeprotokoll (für Desktop-Clients)	X	X	X	X
PCoIP-Anzeigeprotokoll	X	X	X	X
VMware Blast-Anzeigeprotokoll	Horizon Agent 7.0 und höher	Horizon Agent 7.0 und höher	Horizon Agent 7.0 und höher	Horizon Agent 7.0 und höher
HTML Access		View Agent 6.0.2 und höher		View Agent 6.0.2 und höher
Virtuelles Drucken (für Desktop-Clients)		View Agent 6.0.1 und höher		View Agent 6.0.1 und höher
Standortbasiertes Drucken		View Agent 6.0.1 und höher		View Agent 6.0.1 und höher
Mehrere Monitore (für Desktop-Clients)	X	X	X	X
Unity Touch (für mobile Clients)	X	X	X	X

HINWEIS Für die Smartcard-Funktion ist außerdem Horizon Client 3.4 oder höher erforderlich.

Informationen zu den unterstützten Versionen 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.

Einschränkungen für Sonderfunktionen

Für bestimmte Funktionen, die auf Windows-Desktops für Horizon Client für iOS unterstützt werden, gelten spezielle Einschränkungen.

Tabelle 4-3. Anforderungen für Sonderfunktionen

Funktion	Anforderungen
Linkshändermodus	Diese Funktion ist iOS-spezifisch. Wenn Ihr Remote-Desktop so konfiguriert ist, dass die primäre und sekundäre Maustaste vertauscht sind, verwenden Sie die Funktion „Linkshändermodus“. Siehe „ Konfiguration von Horizon Client zur Unterstützung von umgekehrten Maustasten “, auf Seite 52.
Standortbasiertes Drucken für Windows Server 2008 R2 Desktops, RDS-Desktops (auf RDS-Hosts virtueller Maschinen) und Remoteanwendungen	Horizon Client 3.1 und höher und Horizon 6.0.1 (mit View) und höhere Server

Tabelle 4-3. Anforderungen für Sonderfunktionen (Fortsetzung)

Funktion	Anforderungen
Smartcards für RDS-Desktops	Horizon Client 3.4 und höher sowie View Agent 6.1 und höher.
Echtzeit-Audio/Video (nur Audio-Eingang)	Siehe „ Systemanforderungen für Echtzeit-Audio/Video “, auf Seite 8.

HINWEIS Mit Horizon Client haben Sie nicht nur auf Remote-Desktops, sondern auch auf Windows-basierte Remoteanwendungen sicheren Zugriff. Durch die Auswahl einer Anwendung in Horizon Client wird ein Fenster für diese Anwendung auf dem lokalen Clientgerät geöffnet, und das Erscheinungsbild und das Verhalten der Anwendung entspricht einer lokal installierten Anwendung.

Remoteanwendungen können Sie nur verwenden, wenn Sie mit Verbindungsserver 6.0 oder höher verbunden sind. Informationen zu den Betriebssystemen, die für den RDS (Remote Desktop Sessions)-Host, der Remoteanwendungen und sitzungsbasierte Desktops bereitstellt, unterstützt werden, finden Sie im Thema „Unterstützte Betriebssysteme für Horizon 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.

Externe Tastaturen und Eingabevorrichtungen

Horizon Client unterstützt iPad Keyboard Dock und Apple Wireless Keyboard (Bluetooth). Horizon Client 4.0 und höher unterstützt Apple Pencil als Zeigegerät auf iPad Pro.

Die externe iPad Keyboard Dock-Tastatur wird von Horizon Client automatisch erkannt. Um das Apple Wireless Keyboard (Bluetooth) mit einem Remote-Desktop verwenden zu können, müssen Sie das Gerät zuerst mit einem iOS-Gerät koppeln.

Nach der Verbindung von Tastatur und iPad müssen Sie sicherstellen, dass sich die Bildschirmtastatur nicht im Modus „Geteilte Tastatur“ befindet, wenn Sie die Erkennung der Bluetooth-Tastatur durch den iPad starten. Damit das Clientgerät die drahtlose Tastatur erkennen kann, müssen Sie entweder mit drei Fingern gleichzeitig auf den Bildschirm tippen oder auf die Schaltfläche **Tastatur** in den Tools der Horizon Client-Benutzeroberfläche tippen.

Nach Erkennung der externen Tastatur können Sie über das Apple Wireless Keyboard (Bluetooth) die Horizon Client-Tools oder das Drei-Finger-Tippen nicht verwenden, um die Bildschirmtastatur anzuzeigen. Sie müssen zuerst die externe Tastatur durch Drücken der Eject-Taste deaktivieren.

Über das Apple Wireless Keyboard wird die japanische Tilde normaler Breite auf Remote-Desktops nicht eingegeben.

Internationale Tastaturen

Sie können Zeichen für Englisch, Japanisch, Französisch, Deutsch, vereinfachtes Chinesisch, traditionelles Chinesisch und Koreanisch eingeben.

VMware empfiehlt die Verwendung einer englischen Tastatur auf Ihrem iOS-Gerät in Kombination mit einem Remote-Desktop, der einen koreanischen oder japanischen Eingabemethoden-Editor (IME) verwendet. Wenn Sie auf Ihrem iOS-Gerät eine koreanische oder japanische Tastatur verwenden und eine Verbindung zu einem Remote-Desktop herstellen, der einen koreanischen oder japanischen IME verwendet, wird der Windows-IME-Modus Englisch/Koreanisch bzw. Englisch/Japanisch des Remote-Desktops nicht mit dem Gebietsschema der iOS-Tastatur synchronisiert.

Aktivieren des japanischen 106/109-Tastaturlayouts

Wenn Sie mit einem Windows XP-Desktop verbunden sind, können Sie für Horizon Client die Verwendung des japanischen 106/109-Tastaturlayouts konfigurieren.

Voraussetzungen

Verwenden Sie Horizon Client, um eine Verbindung zu einem Windows XP-Desktop mit aktiviertem japanischem Tastaturlayout herzustellen.

Vorgehensweise

- 1 Stellen Sie mit den Horizon Client-Tools das Dialogfeld „Optionen“ dar.
- 2 Tippen Sie auf **Japanische 106/109-Tastatur**, um diese Option auf „Ein“ umzuschalten.

Diese Einstellung ist deaktiviert, wenn für den Windows XP-Desktop nicht das japanische Tastaturlayout festgelegt ist. Wenn der Desktop nicht unter Windows XP ausgeführt wird, ist diese Einstellung ausgeblendet.

- 3 Tippen Sie auf **Fertig**.

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. Echtzeit-Audio/Video ist kompatibel mit Standard-Audiogeräten und kann mit standardmäßigen Konferenzanwendungen wie z. B. Skype, WebEx und Google Hangouts verwendet werden.

Die Echtzeit-Audio/Video-Funktion wird standardmäßig bei der Installation von Horizon Client 4.0 oder höher auf Ihrem Gerät installiert. Diese Funktion wird in früheren Horizon Client-Versionen nicht unterstützt.

HINWEIS In Horizon Client 4.0 wird nur die Audio-Eingangs-Funktion unterstützt. Die Video-Funktion wird in Horizon Client 4.0 nicht unterstützt.

Informationen zur Einrichtung der Echtzeit-Audio/Video-Funktion auf einem Remote-Desktop finden Sie im Dokument *Einrichten von Desktop- und Anwendungspools für View*.

Bei der ersten Anwendung des Mikrofons werden Sie von Horizon Client zur Eingabe der Zugriffsberechtigung aufgefordert. Sie müssen über eine Berechtigung für das Mikrofon verfügen, damit Sie es mit Ihrem Remote-Desktop verwenden können. Der Zugriff auf das Mikrofon kann durch Änderung der Mikrofonberechtigung für Horizon Client in der App der iOS-Einstellungen aktiviert und deaktiviert werden.

Verwenden nativer Gesten auf Betriebssystemen mit Touch-Umleitung

Mit Horizon Client 3.2 oder höher können Sie native Gesten des Betriebssystems auf Ihrem Touch-basierten mobilen Endgerät verwenden, wenn Sie mit einem Windows 8- oder Windows Server 2012-basierten Remote-Desktop oder einer auf Windows Server 2012 gehosteten Remoteanwendung verbunden sind. Beispielsweise können Sie ein Element auf einem Windows 8-Desktop berühren, halten und loslassen, um das Kontextmenü des Elements anzuzeigen.

Wenn die Touch-Umleitung aktiviert ist, können Sie nur native Touch-Gesten des Betriebssystems verwenden. Lokale Gesten in Horizon Client wie z. B. das Doppelklicken oder Fingerspreizen funktionieren nicht mehr. Sie müssen die Registerkarten-Schaltfläche von Unity Touch ziehen, um die Unity Touch-Sidebar einzublenden.

Die Touch-Umleitung wird standardmäßig aktiviert, wenn Sie eine Verbindung zu einem Windows 8- oder Windows Server 2012-basierten Remote-Desktop oder einer auf Windows Server 2012 gehosteten Remoteanwendung herstellen.

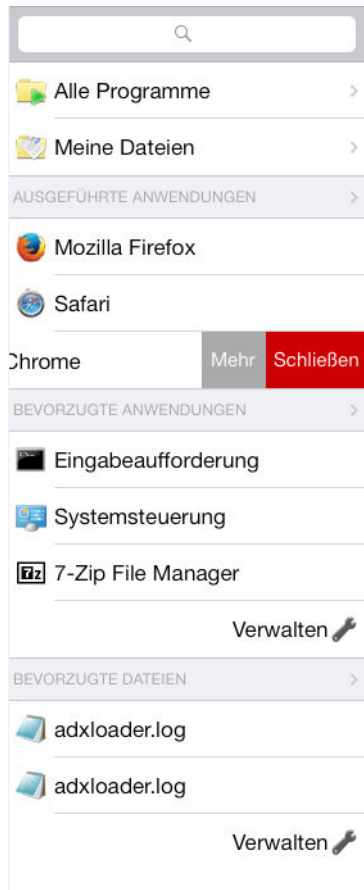
Um die Touch-Umleitung von einem Remote-Desktop zu deaktivieren, rufen Sie mit den Horizon Client-Tools das Dialogfeld „Optionen“ auf und setzen Sie die Einstellung **Native Windows 8-Gesten** auf „Aus“. In Horizon Client 4.0 und höher können Sie die Touch-Umleitung auch auf dem Bildschirm der Horizon Client-Einstellungen deaktivieren. Tippen Sie auf **Einstellungen** am unteren Rand des Horizon Client-Bildschirms und tippen Sie auf **Touch**, um die Einstellung **Native Windows 8-Gesten** aufzurufen.

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.

Wenn die Unity Touch-Funktion aktiviert ist, erscheint die Sidebar auf der linken Seite des Bildschirms, wenn Sie zum ersten Mal auf einen Remote-Desktop zugreifen.

Abbildung 4-1. Unity Touch-Sidebar



Wenn Sie auf einen Desktop zugreifen, bei dem Unity Touch aktiviert ist, aber die Sidebar nicht angezeigt wird, sehen Sie auf der linken Seite des Bildschirms eine Registerkarte. Sie können diese Registerkarte nach rechts wischen, um die Sidebar zu öffnen, und nach oben oder unten verschieben.

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

Tabelle 4-4. Aktionen der Unity Touch-Sidebar für einen Remote-Desktop

Aktion	Prozedur
Anzeigen the Sidebar	Wischen Sie über die Registerkarte nach rechts. Wenn die Sidebar geöffnet ist, können Sie keine Aktionen auf dem Desktop-Bildschirm oder im kreisförmigen Menü für die Horizon Client-Tools ausführen.
Ausblenden der Sidebar	Wischen Sie die Registerkarte auf die linken Seite, um die Sidebar zu schließen. Wenn die Sidebar geöffnet ist, können Sie keine Aktionen auf dem Desktop-Bildschirm oder im kreisförmigen Menü für die Horizon Client-Tools ausführen. In Horizon Client 3.1 oder höher können Sie auch auf den Desktop-Bildschirm tippen, einschließlich des kreisförmigen Menüs für die Horizon Client-Tools, um die Sidebar auszublenden.
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	<ul style="list-style-type: none"> ■ 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	<ol style="list-style-type: none"> 1 Tippen Sie auf den Namen der Anwendung unter Ausgeführte Anwendungen und wischen Sie von rechts nach links. 2 Tippen Sie auf die angezeigte Schaltfläche Mehr. 3 Tippen Sie auf Minimieren.
Maximieren einer laufenden Anwendung oder eines Fensters	<ol style="list-style-type: none"> 1 Tippen Sie auf den Namen der Anwendung unter Ausgeführte Anwendungen und wischen Sie von rechts nach links. 2 Tippen Sie auf die angezeigte Schaltfläche Mehr. 3 Tippen Sie auf Maximieren.
Schließen einer laufenden Anwendung oder eines Fensters	Tippen Sie auf den Namen der Anwendung unter Ausgeführte Anwendungen und wischen Sie von rechts nach links. Tippen Sie auf die erscheinende Schaltfläche Schließen .
Wiederherstellen der vorherigen Größe und Position einer laufenden Anwendung oder eines Fensters	<ol style="list-style-type: none"> 1 Tippen Sie auf den Namen der Anwendung unter Ausgeführte Anwendungen und wischen Sie von rechts nach links. 2 Tippen Sie auf die angezeigte Schaltfläche Mehr. 3 Tippen Sie auf Wiederherstellen.

Tabelle 4-4. Aktionen der Unity Touch-Sidebar für einen Remote-Desktop (Fortsetzung)

Aktion	Prozedur
Erstellen einer Liste der beliebtesten Anwendungen oder Dateien	<ol style="list-style-type: none"> 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. 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. Ihre Favoriten stehen auf sämtlichen mobilen Geräten zur Verfügung, sodass Sie zum Beispiel immer die gleiche Liste sehen, gleichgültig, ob Sie Ihr Smartphone oder Ihr Tablet benutzen.
Entfernen einer Anwendung oder Datei aus der Favoritenliste	<ol style="list-style-type: none"> 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. 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	<ol style="list-style-type: none"> 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. 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.

HINWEIS Zur Verwendung der Unity Touch-Funktion mit View 5.3.x-Desktops muss der Remote Experience Agent auf den Desktops installiert sein. Wenn Sie den Remote Experience Agent installiert haben, diese Funktion aber deaktivieren möchten, können Sie einen Registrierungswert auf dem Remote-Desktop festlegen.

Wenn Benutzer einen dynamischen Desktop verwenden, können bevorzugte Anwendungen und Dateien des Benutzers nur dann gespeichert werden, wenn Windows-Roaming-Benutzerprofile für den Desktop konfiguriert sind. Administratoren können eine standardmäßige Liste der **Favoriten-Anwendungen** erstellen, die Endbenutzer beim ersten Anzeigen der Sidebar angezeigt bekommen.

Für Server von Verbindungsserver 5.3.x finden Sie weitere Informationen im Dokument *View Feature Pack Installation und Verwaltung*. Zu Verbindungsservern der Version 6.0 und höheren Servern finden Sie weitere Informationen im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

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.

Wenn Sie auf eine Remoteanwendung zugreifen, wird die Unity Touch-Sidebar auf der linken Seite des Bildschirms angezeigt. Falls die Unity Touch-Sidebar geschlossen ist, wird links im Bildschirm eine Registerkarte angezeigt. Sie können diese Registerkarte nach rechts wischen, um die Sidebar neu zu öffnen. Sie können die Registerkarte auch nach oben oder unten wischen.

HINWEIS Remoteanwendungen können Sie nur verwenden, wenn Sie mit Verbindungsserver 6.0 oder höher verbunden sind.

Abbildung 4-2. Unity Touch-Sidebar für eine Remoteanwendung



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

Tabelle 4-5. Aktionen der Unity Touch-Sidebar für eine Remoteanwendung

Aktion	Prozedur
Anzeigen the Sidebar	Wischen Sie über die Registerkarte nach rechts, um die Sidebar zu öffnen. Bei geöffneter Sidebar können Sie auf dem Anwendungsbildschirm keine Aktionen ausführen.
Ausblenden der Sidebar	Wischen Sie die Registerkarte auf die linken Seite, um die Sidebar zu schließen. Bei geöffneter Sidebar können Sie auf dem Anwendungsbildschirm keine Aktionen ausführen. In Horizon Client 3.1 oder höher können Sie auch auf den Anwendungsbildschirm tippen, einschließlich des kreisförmigen Menüs für die Horizon Client-Tools, um die Sidebar auszublenden.
Wechseln zwischen ausgeführten Anwendungen	Tippen Sie auf die Anwendung unter Aktuelle Verbindung .
Öffnen einer Anwendung	Tippen Sie auf den Namen der Anwendung unter Verfügbare Anwendungen auf der Sidebar. Die Anwendung startet und die Sidebar wird geschlossen.
Schließen einer laufenden Anwendung	<ol style="list-style-type: none"> 1 Tippen Sie auf den Namen der Anwendung unter Aktuelle Verbindung und wischen Sie von rechts nach links. 2 Tippen Sie auf die erscheinende Schaltfläche Schließen.
Minimieren einer laufenden Anwendung	<ol style="list-style-type: none"> 1 Tippen Sie auf den Namen der Anwendung unter Aktuelle Verbindung und wischen Sie von rechts nach links. 2 Tippen Sie auf die angezeigte Schaltfläche Mehr. 3 Tippen Sie auf Minimieren.
Maximieren einer laufenden Anwendung	<ol style="list-style-type: none"> 1 Tippen Sie auf den Namen der Anwendung unter Aktuelle Verbindung und wischen Sie von rechts nach links. 2 Tippen Sie auf die angezeigte Schaltfläche Mehr. 3 Tippen Sie auf Maximieren.

Tabelle 4-5. Aktionen der Unity Touch-Sidebar für eine Remoteanwendung (Fortsetzung)

Aktion	Prozedur
Wiederherstellen einer laufenden Anwendung	<ol style="list-style-type: none"> 1 Tippen Sie auf den Namen der Anwendung unter Aktuelle Verbindung und wischen Sie von rechts nach links. 2 Tippen Sie auf die angezeigte Schaltfläche Mehr. 3 Tippen Sie auf Wiederherstellen.
Wechseln zu einem Remote-Desktop	Tippen Sie auf den Namen des Desktops unter Desktops .








Horizon Client -Tools

Die Horizon Client-Tools umfassen Schaltflächen, mit denen Sie die Bildschirmtastatur, das virtuelle Touchpad, Konfigurationseinstellungen und einen virtuellen Ziffernblock mit Pfeil- und Funktionstasten anzeigen können.

Wenn Sie mit einem Remote-Desktop oder einer Remoteanwendung verbunden sind, wird das kreisförmige Horizon Client-Menüsymbol in der Bildschirmmitte angezeigt. Tippen Sie darauf, um das kreisförmige Menü zu erweitern und Symbole für jedes Werkzeug anzuzeigen, das Sie jeweils durch Antippen auswählen können. Tippen Sie auf einen Bereich außerhalb der Tool-Symbole, um diese wieder auf das kreisförmige Menüsymbol zu reduzieren.

Das kreisförmige Menü enthält verschiedene Werkzeuge.

Tabelle 4-6. Symbole des kreisförmigen Menüs

Symbol	Beschreibung
	Kreisförmiges Horizon Client-Tools-Menü
	Trennen
	Bildschirmtastatur, wechselt zwischen zeigen und verbergen
	Einstellungen
	Navigationstasten
	Virtuelles Touchpad
	Bewegungshilfe

Tastatur auf dem Bildschirm

Die Bildschirmtastatur verfügt über mehr Tasten als die Standard-Bildschirmtastatur. So sind z. B. auch Steuerungs- und Funktionstasten verfügbar. Um die Bildschirmtastatur anzuzeigen, tippen Sie mit drei Fingern gleichzeitig auf den Bildschirm oder auf das Symbol **Tastatur**.

Sie erhalten auch Zugriff auf eine Funktion, die bei jedem Tippen auf ein Textfeld, etwa in eine Notiz oder auf einen neuen Kontakt, die Bildschirmtastatur anzeigt. Wenn Sie dann in einen Bereich tippen, der kein Textfeld ist, wird die Tastatur deaktiviert.

WICHTIG Um das Drei-Finger-Tippen zu verwenden, stellen Sie sicher, dass die iOS-Barrierefreiheitsfunktion zum Vergrößern deaktiviert ist. Wenn die Barrierefreiheitsfunktion zum Vergrößern aktiviert ist, vergrößern Sie die Anzeige durch Doppeltippen mit drei Fingern. Das Einfachtippen mit drei Fingern hat dann keinen Effekt.

Selbst wenn Sie eine externe Tastatur verwenden, wird eventuell trotzdem eine einzeilige Tastatur mit Funktionstasten und den Strg-, Alt-, Win- und Pfeiltasten angezeigt. Manche externe Tastaturen verfügen nicht über all diese Tasten.

Senden einer Zeichenfolge

Tippen Sie auf der Bildschirmtastatur auf das Stiftsymbol auf der linken Seite der Strg-Taste, 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.

Verwenden Sie diese Funktion, wenn Sie eine schlechte Netzwerkverbindung haben. Das heißt, Sie sollten diese Funktion verwenden, wenn Sie Zeichen eingeben und die Zeichen nicht sofort in der Anwendung angezeigt werden. 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.

Navigationstasten

Tippen Sie auf das Symbol **Strg/Seite** in den Horizon Client-Tools oder auf der Bildschirmtastatur, um die Navigationstasten anzuzeigen. Dies betrifft Tasten wie Seite Auf, Seite Ab, Pfeiltasten, Funktionstasten und andere Tasten, die Sie häufig in Windows-Umgebungen finden, z. B. Alt, Entf, Umschalt, Strg, Win und Esc. Pfeiltasten können Sie drücken und gedrückt halten, um ihre Funktion kontinuierlich zu verwenden. Ein Bild des Strg/Page-Symbols finden Sie in der Tabelle zu Beginn dieses Themas.

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+Entf, 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 Löschtaste.

Touchpad auf dem Bildschirm und Vollbild-Touchpad

Das virtuelle Touchpad kann entweder in normaler Größe (wie ein Touchpad auf einem Laptop) oder als Vollbild angezeigt werden (sodass der gesamte Gerätebildschirm als Touchpad agiert).

Sie können bei Antippen des Touchpad-Symbols standardmäßig einen beliebigen Punkt auf dem Bildschirm berühren, um den Mauszeiger zu bewegen. Der Bildschirm wird zu einem Vollbild-Touchpad.

- Durch Bewegen Ihres Fingers auf dem Touchpad wird ein Mauszeiger über den Remote-Desktop oder die Remoteanwendung gezogen.
- Sie können das virtuelle Touchpad in Standardgröße und das virtuelle Vollbild-Touchpad für das Einfach- oder Doppelklicken verwenden.
- Das Standard-Touchpad enthält auch Tasten für das Links- und Rechtsklicken.
- Doppeltippen Sie mit einem Finger und ziehen Sie, um das Gedrückthalten der linken Maustaste beim Ziehen zu simulieren.

Um diese Funktion zu aktivieren, verwenden Sie die Horizon Client-Tools zur Anzeige des Dialogfelds „Optionen“ und klicken Sie auf die Option **Touchpad Tippen & Ziehen**, um sie auf „Ein“ zu setzen.

- Sie können mit zwei Fingern tippen und dann ziehen, um vertikal zu rollen.

Sie können das virtuelle Touchpad in Standardgröße zur Seite des Geräts ziehen, damit Sie Ihren Daumen zum Bedienen des Touchpads verwenden können, während Sie das Gerät in der Hand halten.

Das virtuelle Touchpad kann wie ein Touchpad auf einem Laptop angezeigt und verwendet werden, inklusive des Klickens mit der rechten und linken Taste. Dazu rufen Sie mit den Horizon Client-Tools das Dialogfeld „Optionen“ auf und schalten Sie die Einstellung **Vollbild-Touchpad-Modus** auf „Aus“.

Zur Anpassung der Schnelligkeit des Mauszeigers bei Benutzung des Touchpads tippen Sie auf das kreisförmige Menüsymbol für die Horizon Client-Tools und das Symbol **Einstellungen**, um das Dialogfeld „Optionen“ anzuzeigen, und ziehen Sie den Schieberegler in der Option **Touchpad-Empfindlichkeit**.

In Horizon Client 4.0 und höher können Sie die Optionen **Vollbild-Touchpad-Modus** und **Touchpad-Empfindlichkeit** auch im Bildschirm der Horizon Client-Einstellungen aktivieren. Tippen Sie auf **Einstellungen** am unteren Rand des Horizon Client-Bildschirms und tippen Sie auf **Touch**, um die Touchpad-Einstellungen aufzurufen.

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 tippen Sie darauf, um auf ein Element der Benutzeroberfläche zu klicken.

Wenn Sie bei einem Remote-Desktop tippen und Ihren Finger eine Sekunde lang getippt halten, wird neben dem Mauszeiger eine Lupe angezeigt, die Ihnen eine genaue Platzierung ermöglicht. Diese Funktion ist besonders beim Ändern der Größe eines Fensters nützlich.

HINWEIS Wenn Ihr Remote-Desktop für Linkshänder konfiguriert ist, siehe [„Konfiguration von Horizon Client zur Unterstützung von umgekehrten Maustasten“](#), auf Seite 52.

Rechtsklicken

Die folgenden Optionen stehen zum Rechtsklicken zur Verfügung:

- Verwenden Sie die Horizon Client-Tools, um das reguläre virtuelle Touchpad anzuzeigen und die Rechtsklicktaste des Touchpads zu verwenden.
- Tippen Sie mit zwei Fingern nahezu gleichzeitig. 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 einem oder zwei Fingern auf den Bildschirm, und ziehen Sie dann, um einen Bildlauf auszuführen. Der Text unter Ihren Fingern bewegt sich in dieselbe Richtung wie Ihre Finger.

WICHTIG Das Rollen mit einem Finger ist folgendermaßen einschränkt: Es funktioniert nicht, wenn Sie die Zoomfunktion verwenden, wenn die Bildschirmtastatur angezeigt wird oder wenn Sie das Vollbild-Touchpad verwenden.

- Verwenden Sie die Horizon Client-Tools zur Anzeige des Touchpads, tippen Sie mit zwei Fingern auf das Touchpad, und ziehen Sie dann, um einen Bildlauf auszuführen.
- Verwenden Sie das Touchpad auf dem Bildschirm, um den Mauszeiger zu bewegen und auf die Rollbalken zu klicken.

Vergrößern und Verkleinern

Wie bei anderen Anwendungen ziehen Sie Ihre Finger pinzettenartig zusammen oder auseinander, um zu verkleinern bzw. zu vergrößern.

Ändern der Größe von Fenstern

Bei Verwendung des Vollbild-Touchpads zur Vergrößerung bzw. Verkleinerung eines Fensters 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. Alternativ können Sie auch mit einem Finger doppelt tippen und dann die Ziehbewegung ausführen.

Wenn Sie das virtuelle Touchpad in Standardgröße verwenden, doppelklicken Sie mit einem Finger und ziehen Sie, um das Gedrückthalten der linken Maustaste beim Ziehen der Ecke oder der Seite eines Fensters zu simulieren.

Wenn Sie einen anderen Typ des virtuellen Touchpads verwenden, tippen Sie mit dem Finger und halten Sie ihn an dieser Position, bis die Lupe in der Ecke oder an der Seite des Fensters angezeigt wird. Bewegen Sie Ihre Finger auf dem Fenster, bis Pfeile zum Ändern der Größe angezeigt werden. Nehmen Sie Ihren Finger vom Bildschirm. Die Lupe wird durch einen Kreis zum Ändern der Größe ersetzt. Tippen Sie auf diesen Kreis, und ziehen Sie ihn, um die Größe des Fensters zu ändern.

Ton, Musik und Video

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

Multitasking

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

In einem WiFi-Netzwerk wird Horizon Client standardmäßig im Hintergrund bis zu drei Minuten lang auf Geräten von iOS 7.0 und höher ausgeführt. In einem 3G-Netzwerk hält Horizon Client die Datenübertragung an, wenn Sie zu einer anderen Anwendung wechseln. Die Datenübertragung wird fortgesetzt, wenn Sie wieder zurück zu Horizon Client wechseln.

Sie können einfachen Text zwischen einer iOS-App und einem Remote-Desktop oder zwischen zwei Remote-Desktops kopieren und einfügen. Formatierungsinformationen werden nicht kopiert.

- Text, den Sie in die Zwischenablage kopieren, wird automatisch auch in die Zwischenablage Ihres Remote-Desktops kopiert, wenn Sie sich beim Remote-Desktop anmelden.
- Sind Sie bei einem Remote-Desktop angemeldet, wird Text, den Sie in die Zwischenablage des Remote-Desktops kopieren, in die Zwischenablage Ihres iOS-Geräts kopiert, wenn Sie die Home-Taste drücken oder zum Hintergrund wechseln.

Standardmäßig können Sie einfachen Text zwischen einer iOS-Anwendung und einer Remoteanwendung kopieren und einfügen. In der Zwischenablage können bis zu 1 MB an Daten für Kopier- und Einfügevorgänge gespeichert werden. Damit Benutzer einfachen Text zwischen einer Remoteanwendung und einer iOS-Anwendung kopieren und einfügen können, muss die Gruppenrichtlinieneinstellung für PCoIP-Sitzungen mit der Bezeichnung **Zwischenablagenumleitung konfigurieren** auf dem RDS-Host, auf dem der Remoteanwendungspool gehostet wird, geändert werden. Weitere Informationen zum Konfigurieren dieser Gruppenrichtlinieneinstellung finden Sie im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

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 Netzwerkkumgebung 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 Thema „RDS-Profileinstellungen“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Konfiguration von Horizon Client zur Unterstützung von umgekehrten Maustasten

Sie können den **Linkshändermodus** verwenden, wenn die primären und sekundären Maustasten auf Ihrem Remote-Desktop vertauscht sind.

Wenn Sie wie die meisten Linkshänder die Mauseigenschaften für Ihren Remote-Desktop so einrichten, dass die rechte Maustaste die primäre Maustaste ist, müssen Sie die Option **Linkshändermodus** in Horizon Client aktivieren. Wenn Sie diese Option bei der Umkehrung der Maustasten nicht aktivieren, wird das einfache Antippen als Klick der sekundären Maustaste gewertet. Durch ein einfaches Antippen wird dann beispielsweise nicht wie erwartet eine Auswahl getroffen oder ein Cursor eingefügt, sondern ein Kontextmenü angezeigt.

Vorgehensweise

- Wenn Sie bereits mit einem Remote-Desktop verbunden sind, führen Sie die nachfolgend aufgeführten Schritte aus.
 - a Tippen Sie auf das kreisförmige Menüsymbol der Horizon Client-Tools, um diese zu erweitern, und tippen Sie auf das Symbol „Einstellungen“, um das Dialogfeld „Optionen“ aufzurufen.
 - b Tippen Sie auf **Linkshändermodus**, um die Option zu aktivieren.
 - c Tippen Sie auf einen Punkt außerhalb des Optionen-Dialogfelds, um dieses zu schließen.
- (Horizon Client 4.0 und höher) Wenn Sie nicht mit einem Remote-Desktop verbunden sind, führen Sie die nachfolgend aufgeführten Schritte aus.
 - a Tippen Sie auf **Einstellungen** am unteren Rand des Horizon Client-Bildschirms.
 - b Tippen Sie im Bildschirm für Einstellungen **Touch**.
 - c Tippen Sie auf **Linkshändermodus**, um die Option zu aktivieren.

Ein einfaches Antippen wird jetzt als Klick mit der primären Maustaste gewertet.

Bildschirmauflösungen und Verwendung externer Anzeigen

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

Wenn Sie Ihr Gerät mit einem externen Anzeigegerät oder Projektor verbinden, unterstützt Horizon Client bestimmte maximale Anzeigeaufösungen. Sie können die auf dem Gerät verwendete Bildschirmauflösung so ändern, dass ein Bildlauf bei einer größeren Bildschirmauflösung zugelassen wird.

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.

Durch Auseinanderziehen der Finger können Sie den Desktop so vergrößern, dass er über die Anzeigebmessungen des Gerätebildschirms hinausgeht. Sie können dann tippen und ziehen, um auf die Desktop-Ränder zuzugreifen.

Ändern der Einstellung für die Anzeigeauflösung

Um die Auflösung von einem Remote-Desktop zu ändern, rufen Sie mit den Horizon Client-Tools das Dialogfeld „Optionen“ auf und tippen Sie dort auf die Einstellung **Anzeigeauflösung**. In Horizon Client 4.0 und höher können Sie die Auflösung auch auf dem Bildschirm der Horizon Client-Einstellungen ändern. Tippen Sie auf **Einstellungen** am unteren Rand des Horizon Client-Bildschirms und dann auf **Auflösung**.

HINWEIS Bestimmte Optionen wie „3/4-Skalierung“ oder „Keine Skalierung“ sind für das iPhone 6 im Zoom-Modus nicht verfügbar. Damit diese Optionen angezeigt werden, müssen Sie den Zoom-Modus beenden.

Bildschirmauflösungen für Projektoren

Mithilfe der Einstellung **Anzeigeauflösung** (Dialogfeld „Optionen“ in einem Remote-Desktop) oder **Auflösung** (Einstellungsbildschirm in Horizon Client 4.0 und höher) können Sie eine größere Auflösung für Projektoren festlegen.

Um die Tastatur und ein erweitertes Bildschirm-Touchpad auf dem Gerät anzuzeigen, wenn der Remote-Desktop auf dem Projektor oder auf dem angeschlossenen Monitor dargestellt wird, aktivieren Sie die Einstellung **Präsentationsmodus** im Dialogfeld „Optionen“ des Remote-Desktops. Das erweiterte Touchpad und die Tastatur werden angezeigt, wenn das Gerät an den externen Monitor angeschlossen wird. Das Gerät erkennt die maximale Auflösung, welche die externe Anzeige darstellen kann.

Sie können die gesamte Geräteanzeige auf einen Projektor oder einen angeschlossenen Monitor spiegeln, einschließlich der Unity Touch-Sidebar, indem Sie die Einstellung **Präsentationsmodus** deaktivieren. Wenn Sie mit einem Remote-Desktop verbunden sind und die Einstellung **Präsentationsmodus** aktiviert ist, können Sie auf **Fertig** klicken, um in den Spiegelungsmodus zu wechseln.

Verwenden Sie die Einstellung **Aktiviert lassen**, um im Präsentationsmodus eine Abschaltung des Displays nach einem bestimmten Zeitraum der Inaktivität zu verhindern. Sie können diese Einstellung im Dialogfeld „Optionen“ eines Remote-Desktops aktivieren. In Horizon Client 4.0 und höher lässt sich diese Einstellung auch auf dem Bildschirm der Horizon Client-Einstellungen aktivieren. Um den Bildschirm „Einstellungen“ aufzurufen, tippen Sie auf **Einstellungen** am unteren Rand des Horizon Client-Bildschirms.

PCoIP-Client-Bildcache

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

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

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

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

Mithilfe der clientseitigen Zwischenspeicherung speichert der Client Teile der Anzeige, die zuvor übertra- gen wurden. Die Cachegröße beträgt die Hälfte des verfügbaren RAMs. Umfasst das RAM weniger als 50 MB, beträgt die Cachegröße 50 MB.

Unterdrücken der Warnmeldung bezüglich der Mobilfunkdaten

Wenn Horizon Client erkennt, dass Sie eine mobile Datenverbindung verwenden, erscheint das Dialogfeld „Netzwerkverwendung“, um Sie darüber zu informieren, dass Ihre Remote-Desktop- bzw. Remoteanwen- dungsverbindung möglicherweise einen wesentlichen Teil Ihres Datenvolumens verbraucht.

In Horizon Client 3.1 und höher wird das Dialogfeld „Netzwerkverwendung“ angezeigt, wenn Sie eine Ver- bindung zu einem Server hergestellt haben und versuchen, einen Remote-Desktop oder eine Remoteanwen- dung zu starten, oder nachdem Sie auf eine neuere Desktop- oder Anwendungsverknüpfung getippt haben, oder nachdem Sie eine Verbindung mit einer Remoteanwendung hergestellt haben und versuchen, von der Unity Touch-Sidebar aus eine weitere Anwendung oder einen weiteren Remote-Desktop zu starten. In Horizon Client 3.2 und höher wird das Dialogfeld „Netzwerkverwendung“ nur beim Starten von Horizon Client angezeigt.

In Horizon Client 3.1 und höher können Sie das Dialogfeld „Netzwerkverwendung“ unterdrücken, wenn es erscheint. Darüber hinaus können Sie eine Option festlegen, um das Dialogfeld "Netzwerkverwendung" im- mer zu unterdrücken.

Vorgehensweise

- Um das Dialogfeld „Netzwerkverwendung“ nach seiner Anzeige in Horizon Client 3.1 und höher zu unterdrücken, tippen Sie im Dialogfeld „Netzwerkverwendung“ auf **Diese Meldung nicht erneut an- zeigen**.
- Um das Dialogfeld „Netzwerkverwendung“ nach seiner Anzeige in Horizon Client 3.2 und höher zu unterdrücken, tippen Sie im Dialogfeld „Netzwerkverwendung“ auf **Nie erinnern**.
- Um festzulegen, dass das Dialogfeld „Netzwerkverwendung“ nach der Herstellung einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung nicht angezeigt wird, tippen Sie zuerst auf das kreisförmige Menüsymbol für die Horizon Client-Tools, dann auf das Symbol „Einstellungen“, um das Dialogfeld „Optionen“ einzublenden, und setzen Sie schließlich die Option **Warnung zu Mobil- funkdaten** auf „Aus“.
- (Horizon Client 4.0 und höher) Um festzulegen, dass das Dialogfeld „Netzwerkverwendung“ vor der Herstellung einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung nicht ange- zeigt wird, tippen Sie auf **Einstellungen** am unteren Rand des Horizon Client-Bildschirms und setzen Sie die Option **Warnung zu Mobilfunkdaten** auf „Aus“.

Internationalisierung

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

Fehlerbehebung für Horizon Client

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:

- [„Erfassen und Versenden von Protokollinformationen“](#), auf Seite 55
- [„Zurücksetzen eines Remote-Desktops oder einer Remoteanwendung“](#), auf Seite 57
- [„Deinstallieren von Horizon Client“](#), auf Seite 58
- [„Horizon Client oder der Remote-Desktop reagiert nicht mehr“](#), auf Seite 58
- [„Probleme beim Herstellen einer Verbindung bei Verwendung eines Proxys“](#), auf Seite 59

Erfassen und Versenden von Protokollinformationen

Sie können Horizon Client so konfigurieren, dass Protokollinformationen erfasst und Protokolldateien zur Fehlerbehebung an VMware gesendet werden.

Falls Horizon Client unerwartet beendet wird, während die Protokollerfassung aktiviert ist, fordert Horizon Client Sie beim nächsten Start von Horizon Client auf, die Protokolldateien an VMware zu senden.

Wenn Sie die Protokolldateien an VMware senden möchten, sendet Horizon Client eine Nachricht aus dem auf Ihrem Gerät konfigurierten E-Mail-Konto und hängt eine GZ-Datei an, die die letzten fünf Protokolldateien enthält. Der Name der Datei enthält einen Zeitstempel, z. B. `Horizon_View_Client_logs_zeitstempel.zip`.

Sie können die Protokolldateien jederzeit auch manuell abrufen und senden.

Aktivieren der Horizon Client -Protokollerfassung

Wenn Sie die Protokollerfassung aktiviert haben, erstellt Horizon Client Protokolldateien mit Informationen, die VMware dabei helfen können, Probleme mit Horizon Client zu beheben.

Da die Protokollerfassung sich auf die Leistung von Horizon Client auswirkt, sollten Sie sie nur aktivieren, wenn ein Problem auftritt.

Voraussetzungen

Vergewissern Sie sich, dass auf Ihrem Gerät ein E-Mail-Konto eingerichtet ist. Horizon Client verwendet dieses E-Mail-Konto, um Protokolldateien zu senden.

Vorgehensweise

- 1 Öffnen Sie auf Ihrem iOS-Gerät die Horizon Client-Einstellungen.

Option	Beschreibung
Horizon Client 3.0	Tippen Sie auf die iOS-App Einstellungen und anschließend auf VMware View .
Horizon Client 3.1 bis 3.5	Tippen Sie auf die iOS-App Einstellungen und anschließend auf Horizon .
Horizon Client 4.0 und höher	Tippen Sie auf Einstellungen am unteren Rand des Horizon Client-Bildschirms.

- 2 Tippen Sie zum Umschalten der Option **Protokollierung** (Horizon Client 3.0 bis 3.5) oder der Option **Protokollsammlung** (Horizon Client 4.0 und höher) auf „Ein“.

Nachdem die Protokollerfassung aktiviert wurde, erstellt Horizon Client mehrere Protokolldateien. Wenn Horizon Client unerwartet beendet wird oder beendet und neu gestartet wird, werden die Protokolldateien zusammengeführt und zu einer einzelnen GZ-Datei komprimiert. Wenn Sie das Protokoll senden möchten, hängt Horizon Client die GZ-Datei an eine E-Mail-Nachricht an.

Wenn Sie vom aktiven Desktop zu den Einstellungen wechseln, die Protokollerfassung aktivieren und dann wieder den Desktop aufrufen, müssen Sie die Verbindung zum Desktop erneut herstellen, um eine vollständige Protokolldatei zu erfassen.

Manuelles Abrufen und Senden von Horizon Client -Protokolldateien

Wenn die Horizon Client-Protokollerfassung auf Ihrem Gerät aktiviert ist, können Sie die Protokolldateien jederzeit manuell abrufen und senden.

Diese Schritte zeigen Ihnen, wie Sie Protokolldateien über Horizon Client abrufen und senden können. Wenn Ihr Gerät mit einem PC oder Mac verbunden ist, können Sie die Protokolldateien auch mit iTunes abrufen.

Voraussetzungen

- Vergewissern Sie sich, dass auf Ihrem Gerät ein E-Mail-Konto eingerichtet ist. Horizon Client sendet die Protokolldateien aus diesem E-Mail-Konto.
- Aktivieren Sie die Horizon Client-Protokollerfassung. Siehe „[Aktivieren der Horizon Client-Protokollerfassung](#)“, auf Seite 55.

Vorgehensweise

- 1 Tippen Sie in Horizon Client auf das E-Mail-Symbol im oberen Bereich des Bildschirms.
- 2 Geben Sie die Adresse des E-Mail-Empfängers in die Zeile **An:** ein und klicken Sie auf **Senden**, um die Nachricht zu versenden.

Das auf Ihrem Gerät konfigurierte E-Mail-Konto wird in der Zeile **Von:** angezeigt.

Die bestehende GZ-Protokolldatei wird an die Nachricht angehängt. Horizon Client speichert maximal fünf GZ-Protokolldateien. Die ältesten Dateien werden gelöscht, wenn mehr als fünf Protokolldateien für die GZ-Datei vorliegen.

Deaktivieren der Horizon Client -Protokollerfassung

Da die Protokollerfassung sich auf die Leistung von Horizon Client auswirkt, sollten Sie sie deaktivieren, solange Sie kein Problem beheben müssen.

Vorgehensweise

- 1 Öffnen Sie auf Ihrem iOS-Gerät die Horizon Client-Einstellungen.

Option	Beschreibung
Horizon Client 3.0	Tippen Sie auf die iOS-App Einstellungen und anschließend auf VMware View .
Horizon Client 3.1 bis 3.5	Tippen Sie auf die iOS-App Einstellungen und anschließend auf Horizon .
Horizon Client 4.0 und höher	Tippen Sie auf Einstellungen am unteren Rand des Horizon Client-Bildschirms.

- 2 Tippen Sie zum Umschalten der Option **Protokollierung** (Horizon Client 3.0 bis 3.5) oder der Option **Protokollsammlung** (Horizon Client 4.0 und höher) auf „Aus“.

Zurücksetzen eines Remote-Desktops oder einer Remoteanwendung

Beim Zurücksetzen eines Remote-Desktops wird dieser heruntergefahren und neu gestartet. Beim Zurücksetzen einer Remoteanwendung wird diese beendet. Eventuell muss der Desktop oder die Anwendung zurückgesetzt 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 ohne vorheriges Speichern geschlossen.

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

HINWEIS Ein View-Administrator kann die Funktion zum Zurücksetzen für bestimmte Desktop-Typen deaktivieren. Weitere Informationen finden Sie im Dokument *Verwaltung von View*.

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 27 vertraut machen.

Vorgehensweise

- 1 Stellen Sie eine Verbindung mit dem Server her.

Option	Beschreibung
Horizon Client 3.0	Tippen Sie im Fenster „Zuletzt verwendete Verbindungen“ auf das Symbol „Cloud“ in der oberen linken Bildschirmecke und anschließend auf den Pfeil (>) neben dem Servernamen.
Horizon Client 3.1 und höher	Tippen Sie im unteren Bereich des Bildschirms auf Server (Cloud-Symbol) und anschließend auf das Serversymbol.

- 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.
- 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.

Deinstallieren von Horizon Client

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

Vorgehensweise

- 1 Wenn Sie in iTunes auf Ihrem Mac oder PC über Horizon Client verfügen, durchsuchen Sie die App-Bibliothek nach der Horizon Client-App und entfernen Sie sie.
Wenden Sie hierbei die gleiche Vorgehensweise wie für jede andere iTunes-App an.
- 2 Verbinden Sie das Gerät mit Ihrem Computer und lassen Sie die Synchronisierung mit iTunes auf Ihrem Mac oder PC zu.
- 3 Wenn die Horizon Client-App daraufhin nicht von Ihrem Gerät entfernt wird, berühren und halten Sie das App-Symbol für **VMware View** (Horizon Client 3.0) oder **Horizon** (Horizon Client 3.1 und höher), bis es sich bewegt. Tippen Sie dann auf das **X**-Symbol, um die App zu löschen.

Weiter

Installieren Sie Horizon Client erneut.

Siehe „[Installieren oder Aktualisieren von Horizon Client auf einem iOS-Gerät](#)“, auf Seite 13.

Horizon Client oder der Remote-Desktop reagiert nicht mehr

Wenn der Bildschirm 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 View-Server richtig konfiguriert sind und bei den Firewalls um sie herum die richtigen Ports geöffnet sind, betreffen andere Probleme in der Regel Horizon Client auf dem mobilen Endgerät oder 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 View-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 iOS-Gerät zurücksetzen, wie im Benutzerhandbuch für Ihr Gerät von Apple 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 View-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

Zahlen

3D Touch **35**

A

Abmeldung **34**

Agent, Installationsanforderungen **12**

AirWatch-Integration **17**

Anmelden

an einem Desktop **27**

bei einem Server **27**

Anzeigeanforderungen **52**

Anzeigegeräte, Externes **52**

App Store **13**

Auflösung, Bildschirm **52**

Ausführen im Hintergrund **51**

Authentifizierung über Touch ID **11**

B

Betriebssystem-, auf dem Agent unterstützt **12**

Bewegungen auf dem Tablet **50**

Bildcache, Client **53**

Bildschirmauflösung **52**

C

Client-Bildcache **53**

E

Echtzeit-Audio/Video-Funktion **8, 43**

Eingabevorrichtungen für den iPad **42**

Externe Anzeigegeräte **52**

F

Favoriten **33**

Favoritenliste in Unity Touch Sidebar **44**

Fehlerbehebung, Verbindungsprobleme **59**

Funktionsunterstützungs-Matrix **39**

H

Hardwareanforderungen

iOS-Geräte **8**

Smartcard-Authentifizierung **9**

Horizon Client

Anmelden **27**

Fehlerbehebung **58**

Konfiguration für iOS-Clients **7**

Systemanforderungen für iPad und iPhone **8**

Trennen der Verbindung mit einem Desktop **34**

Horizon Client für iOS

deinstallieren **58**

installieren **13**

I

iOS, Installieren von Horizon Client auf **8**

iOS Horizon Client

deinstallieren **58**

installieren **13**

iTunes Store **58**

J

Japanisches Tastaturlayout **43**

K

keyboard (Tastatur)

auf dem Bildschirm **48, 50**

Navigationstasten **48**

Kopieren und Einfügen **51**

L

Linkshändermodus **52**

M

Mac iOS, Installieren von Horizon Client auf **8**

Maustasten, umgekehrt **52**

Multitasking **51**

Multitasking im Hintergrund **51**

N

Navigationstasten **48**

O

Optionen, Konfiguration **48**

P

PCoIP-Client-Bildcache **53**

Programm zur Verbesserung der Benutzerfreundlichkeit, Desktop-Pool-Daten **18**

Projektoren **52**

Protokollerfassung **56, 57**

Protokollieren **55**

Proxy-Verbindungen **59**

R

- Rollen **50**
- RSA SecurID-Token **14**

S

- Serververbindungen, Verwalten **27**
- Sicherheitsserver **12**
- Sidebar, Unity Touch **44**
- Smartcard-Authentifizierung
 - Anforderungen **9**
 - auf mobilen Geräten **10**
- Software-Token **14**
- Speichern von Dokumenten in einer Remoteanwendung **52**
- Split View **36**
- Spotlight-Suche **36**
- SSL-Optionen **15**
- Standardansicht **16**
- Symboleiste, Horizon Client **48**
- Systemanforderungen, für iPad und iPhone **8**

T

- Tastaturunterstützung **42**
- Tasten, Navigation **48**
- Token, RSA SecurID **14**
- Touchpad, virtuell **48**
- Trennen der Verbindung mit einem Remote-Desktop **34**

U

- umgekehrte Maustasten **52**
- Unity Touch-Merkmal **44**
- Unity Touch-Sidebar **46**
- URI-Beispiele **24**
- URI-Syntax für Horizon Clients **22**
- URIs (Uniform Resource Identifier) **21**

V

- Verändern der Fenstergröße **50**
- Verbindungsprobleme **59**
- Verbindungsserver **12**
- Verknüpfung, Desktops **35**
- Verwalten von Desktop-Verknüpfungen **35**
- Verwalten von Desktops **27**
- VMware Blast **16**
- Voraussetzungen für Clientgeräte **12**

W

- Warnmeldung bezüglich Mobilfunkdaten **54**
- Windows 8-Gesten **43**

Z

- Zertifikate, Ignorieren von Problemen **31**

- Zurücksetzen eines Desktops **57**
- Zwischenspeicherung, Clientseitiges Bild **53**