Citrix Workspace-App 1912 LTSR für Windows

Contents

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Info zu diesem Release

September 22, 2023

Neue Features in Release 1912

Das kumulative Update 7 (CU7) ist das neueste Update für 1912 LTSR.

Verbesserung für Microsoft Teams

Die folgende Verbesserung für Microsoft Teams wird für CU6 und höhere Releases unterstützt:

Wenn der Desktop Viewer im Vollbildmodus ausgeführt wird, können Benutzer aus den Bildschirmen, die der Desktop Viewer abdeckt, einen auswählen und freigeben. Im Fenstermodus können Benutzer das Fenster des Desktop Viewers freigeben. Im Seamlessmodus können Benutzer einen der Bildschirme zur Freigabe auswählen. Wenn der Desktop Viewer den Fenstermodus ändert (maximieren, wiederherstellen oder minimieren), wird die Bildschirmfreigabe beendet.

Die folgenden Verbesserungen für Microsoft Teams werden für CU5 und höhere Releases unterstützt:

- Verbesserungen bei der Bildschirmübertragung - Wenn Sie jetzt Ihren Bildschirm freigeben, wird nur der Desktop Viewer-Bildschirm im nativen Bitmap-Format erfasst.
- Peers können jetzt den Mauszeiger des Referenten in einer Bildschirmfreigabesitzung sehen.
- Verbessertes Rendern von Videos.
- Verbesserte Leistung und Zuverlässigkeit
- Die WebRTC Media Engine beachtet jetzt den auf dem Clientgerät konfigurierten Proxyserver.
- Verbesserte Konfigurationen mit Echounterdrückung, automatischer Verstärkungsregelung, Rauschunterdrückung: Wenn diese Optionen in Microsoft Teams konfiguriert sind, übernimmt das von Citrix umgeleitete Microsoft Teams die konfigurierten Werte. Andernfalls sind diese Optionen auf Wahr voreingestellt.
- Sie können jetzt eine bevorzugte Netzwerkschnittstelle für den Medienverkehr konfigurieren.

  Navigieren Sie zu `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` und erstellen Sie einem Schlüssel mit dem Namen `NetworkPreference`(REG_DWORD).

  Wählen Sie einen der folgenden Werte aus:

  - 1: Ethernet

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 2: Wi-Fi
  - 3: Cellular
  - 5: Loopback
  - 6: Any

  Standardmäßig und wenn kein Wert festgelegt ist, wählt die WebRTC Media Engine die beste verfügbare Route aus.

- Sie können jetzt das Audiogerätemodul 2 (ADM2) deaktivieren, sodass das Legacy-Audiogerätemodul (ADM) für 4-Kanal-Mikrofone verwendet wird. Dies hilft bei der Lösung von Problemen im Zusammenhang mit Mikrofonen in einem Anruf.

  Um ADM2 zu deaktivieren, navigieren Sie zu `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`, erstellen Sie einen Schlüssel namens `DisableADM2` (REG_DWORD) und legen Sie den Wert auf 1 fest.

- `DirectWShow` ist jetzt der Standardrenderer.

  Mit folgender Schrittfolge können Sie den Standardrenderer ändern:

  - Öffnen Sie den Registrierungs-Editor.
  - Navigieren Sie zum folgenden Schlüsselspeicherort: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`.
  - Aktualisieren Sie den folgenden Wert: `"UseDirectShowRendererAsPrimary"=dword:00000000`

    Andere mögliche Werte:

    * 0: Media Foundation
    * 1: DirectShow (Standard)

  - Starten Sie die Citrix Workspace-App neu.

> **Hinweis:**
>
> - Die Verbesserungen werden nur auf Endpunkten des Microsoft Windows 10 Desktopbetriebssystems unterstützt.
> - Auf Endpunkten der Betriebssysteme Microsoft Windows 7 und 8 werden die Verbesserungen nicht unterstützt.
> - Die Unterstützung von Verbesserungen wird bei der Installation des Citrix Workspace-App-Pakets festgelegt. Es wird empfohlen, die Citrix Workspace-App zu deinstallieren, wenn Sie das Betriebssystem von Microsoft Windows Version 7 auf Version 10 aktualisieren.

App Protection

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Haftungsausschluss**
>
> Die App Protection-Richtlinien filtern den Zugriff auf erforderliche Funktionen des zugrunde liegenden Betriebssystems (spezifische API-Aufrufe für die Bildschirmerfassung oder das Aufzeichnen von Tastenanschlägen). Damit schützen sie auch vor benutzerdefinierten und speziell entwickelten Hackertools. Die Weiterentwicklung von Betriebssystemen führt jedoch immer wieder zu neuen Einfallstoren für das Keylogging oder die Bildschirmerfassung. Darum ist kein hundertprozentiger Schutz möglich, auch wenn wir diese Schwachstellen kontinuierlich identifizieren und korrigieren.

App Protection ist ein Zusatzfeature, das erweiterte Sicherheit bei der Verwendung von Citrix Virtual Apps and Desktops bietet. Die Funktion beschränkt die Möglichkeit, dass Clients durch Keylogging und Screenshot-Malware kompromittiert werden. App Protection verhindert das Exfiltrieren vertraulicher Informationen wie Benutzeranmeldeinformationen und sensible Informationen, die auf dem Bildschirm angezeigt werden. Die Funktion verhindert, dass Benutzer und Angreifer Screenshots erstellen und Keylogger verwenden, um vertrauliche Informationen zu lesen und zu nutzen.

> **Hinweis:**
>
> Citrix empfiehlt, nur die native Citrix Workspace-App zum Starten einer geschützten Sitzung zu verwenden.

App Protection wird mit dem Controller zwischen StoreFront und dem Controller konfiguriert. Informationen zum Konfigurieren von App Protection auf dem Controller finden Sie in der Dokumentation zu App Protection. Diese Konfiguration wird dann auf die Citrix Workspace-App angewendet, indem App Protection mit einer der folgenden Methoden integriert wird:

- Grafische Benutzeroberfläche
- Befehlszeilenoberfläche

Sie können App Protection zusammen mit der Citrix Workspace-App oder bei Bedarf installieren.

> **Hinweis:**
>
> - Dieses Feature wird nur unter Microsoft Windows Desktop-Betriebssystemen wie Windows 10, Windows 8.1 und Windows 7 unterstützt.
> - Das Feature wird nicht über RDP (Remote Desktop Protocol) unterstützt.

Informationen zum Konfigurieren von App Protection in der Citrix Workspace-App finden Sie unter App Protection.

Verbesserung von App Protection In der Vergangenheit wurde beim Versuch, den Screenshot eines geschützten Fensters zu erstellen, der gesamte Bildschirm, einschließlich der nicht geschützten Apps im Hintergrund, abgedunkelt angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenn Sie nun einen Screenshot mit einem Snipping Tool erstellen, wird nur das geschützte Fenster abgedunkelt oder verborgen. Sie können einen Screenshot des Bereichs außerhalb des geschützten Fensters erstellen, außer im Nicht-Aero-Modus, in dem der gesamte Bildschirm abgedunkelt ist.

Wenn Sie jedoch die Taste **Druck S-Abf** zum Erfassen eines Screenshots verwenden, müssen Sie die Citrix Workspace-App beenden.

Darüber hinaus werden in dieser Version Probleme behoben, um das Feature "App Protection"zu verbessern.

Verbesserungen des Installationsprogramms

Wenn Administratoren in früheren Versionen versuchten, die Citrix Workspace-App auf einem System zu installieren, auf dem bereits eine vom Benutzer installierte App-Instanz vorlag, wurde die Installation blockiert.

Mit diesem Release können Administratoren nun die vom Benutzer installierte Instanz der Citrix Workspace-App überschreiben und die Installation erfolgreich fortsetzen.

Verbesserung von Citrix Workspace-Updates

In früheren Versionen konnte eine vom Administrator installierte Citrix Workspace-App nur vom Administrator aktualisiert werden.

Mit diesem Release können auch Nicht-Administratoren die Citrix Workspace-App auf einer vom Administrator installierten Instanz aktualisieren. Klicken Sie dazu im Infobereich mit der rechten Maustaste auf das Symbol der Citrix Workspace-App und wählen Sie Nach Updates suchen.

> **Hinweis:**
>
> Die Option **Nach Updates suchen** ist jetzt auf vom Benutzer oder vom Administrator installierten Instanzen der Citrix Workspace-App verfügbar.

Unterstützung für ausgehende Proxy

Mit SmartControl können Administratoren detaillierte Richtlinien definieren, um mit Citrix Gateway Benutzerumgebungsattribute für virtuelle Apps und Desktops zu konfigurieren und durchzusetzen. Beispielsweise können Sie verhindern, dass Benutzer ihren Remotedesktops weitere Laufwerke zuordnen. Dies ermöglicht das SmartControl-Feature von Citrix Gateway.

Das Szenario ändert sich jedoch, wenn die Citrix Workspace-App und Citrix Gateway zu separaten Unternehmenskonten gehören. In diesem Fall kann die Clientdomäne das SmartControl-Feature nicht

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

anwenden, da das Gateway in der Clientdomäne fehlt. Stattdessen können Sie den ausgehenden ICA-Proxy nutzen. Mit dem ausgehenden ICA-Proxy können Sie das SmartControl-Feature auch dann verwenden, wenn die Citrix Workspace-App und Citrix Gateway in verschiedenen Organisationen bereitgestellt sind.

Die Citrix Workspace-App unterstützt Sitzungsstarts mit dem Citrix ADC LAN-Proxy. Entweder wird ein einzelner statischer Proxy konfiguriert, oder der Proxyserver wird zur Laufzeit über das Plug-In für ausgehende Proxys ausgewählt.

Es gibt folgende Konfigurationsmethoden für ausgehende Proxys:

- Statischer Proxy: Der Proxyserver wird durch Angabe eines Proxy-Hostnamen und der Portnummer konfiguriert.
- Dynamischer Proxy: Ein einzelner Proxyserver wird mit der Proxy-Plug-In-DLL unter einem oder mehreren Proxyservern ausgewählt.

Sie können den ausgehenden Proxy mit der administrativen Gruppenrichtlinienobjektvorlage und dem Registrierungs-Editor konfigurieren.

Weitere Informationen zum ausgehenden Proxy finden Sie unter Unterstützung für den ausgehenden ICA-Proxy in der Citrix Gateway-Dokumentation.

Weitere Informationen zum Konfigurieren von ausgehenden Proxys in der Citrix Workspace-App finden Sie unter Ausgehender Proxy.

Binärdateien für eingebetteten Citrix Browser

Der eingebettete Citrix Browser wird in diesem Release nicht mehr installiert. Wenn Sie ein Upgrade auf Version 1912 durchführen, wird der eingebettete Citrix Browser entfernt.

Das Fehlen des eingebetteten Citrix Browsers hat folgende Auswirkungen:

- Die Umleitung des Browserinhalts funktioniert nicht.
- SaaS- und Web-Apps werden nicht mit dem eingebetteten Citrix Browser gestartet. Stattdessen werden sie im Citrix Secure Browser Service gestartet.

Verbesserung der Desktopfreigabe mit Microsoft Teams

Wenn Sie Ihren Workspace in Microsoft Teams freigeben, wird in der Citrix Workspace-App der aktuell freigegebene Bildschirmbereich mit einem roten Rahmen markiert. Sie können nur das Desktop Viewer-Fenster oder ein beliebiges lokales Fenster darüber freigeben. Wenn Sie das Desktop Viewer-Fenster minimieren, wird die Bildschirmfreigabe angehalten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Geschätzte Codierungsleistung von Endpunkten in Microsoft Teams

Beim Start von HDxTeams.exe (der in die Citrix Workspace-App eingebetteten WebRTC-Medienengine für die Microsoft Teams-Umleitung) wird die optimale Codierungsauflösung geschätzt, die ohne Überlastung der Endpunkt-CPU aufrechterhalten werden kann. Mögliche Werte sind 240p, 360p, 720p und 1080p.

Diese Schätzung der Endpunktleistung (auch `webrtcapi.EndpointPerformance` genannt) läuft, wenn HdxTeams.exe initialisiert wird. Der Macroblock-Code bestimmt die beste Auflösung, die bei dem jeweiligen Endpunkt erzielt werden kann. Die höchstmögliche Auflösung fließt dann in die Codec-Aushandlung zwischen Peers oder zwischen Peer und Konferenzserver ein.

Weitere Informationen zum Konfigurieren der Endpunkt-Codierung finden Sie unter Geschätzte Codierungsleistung von Endpunkten in Microsoft Teams.

Weitere Informationen finden Sie unter Optimierung für Microsoft Teams in der Dokumentation zu Citrix Virtual Apps and Desktops.

Verbesserung des Citrix Analytics-Diensts

Ab diesem Release ermöglicht die Citrix Workspace-App die sichere Übertragung der öffentlichen IP-Adresse des letzten Netzwerk-Hops an den Citrix Analytics-Dienst. Die Daten werden pro Sitzungsstart erfasst. Mit den Daten kann der Citrix Analytics-Dienst analysieren, ob Leistungsprobleme auf bestimmte geografische Bereiche zurückzuführen sind. Standardmäßig werden die IP-Adressprotokolle an den Citrix Analytics-Dienst gesendet. Sie können diese Option jedoch in der Citrix Workspace-App mit dem Registrierungs-Editor deaktivieren.

Um die Übertragung von IP-Adressprotokollen zu deaktivieren, navigieren Sie zum folgenden Registrierungspfad und legen Sie den Schlüssel `SendPublicIPAddress` auf **Aus** fest.

- Navigieren Sie auf 64-Bit-Windows-Maschinen zu: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`.
- Navigieren Sie auf 32-Bit-Windows-Maschinen zu: `HKEY_LOCAL_MACHINE\SOFTWARE \Citrix\Dazzle`.

> **Hinweis:**
>
> - Zwar überträgt die Citrix Workspace-App jede IP-Adresse, auf der sie gestartet wird, jedoch gelingt die IP-Adressübertragung nicht immer perfekt. Einige der Adressen sind möglicherweise nicht ganz richtig.
> - Stellen Sie in geschlossenen Kundenumgebungen, in denen die Endpunkte innerhalb eines

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Intranets betrieben werden, sicher, dass die URL `https://locus.analytics.cloud.com/api/locateip` auf dem Endpunkt auf einer Positivliste steht.

Weitere Informationen dazu, wie die Leistungsanalyse diese Informationen verwendet, finden Sie unter Self-Service für Leistung.

Behobene Probleme

October 26, 2023

Citrix Workspace-App 1912 LTSR CU7 für Windows

Im Vergleich zu Citrix Workspace-App 1912 LTSR CU6

Inhaltsumleitung

- Wenn Desktop Viewer auf den Vollbildmodus eingestellt ist und der Standardbrowser auf dem Endpunktgerät maximiert ist, bringt die Funktion zur bidirektionalen Inhaltsumleitung das Fenster des lokalen Standardwebbrowsers möglicherweise nicht in den Vordergrund. Das Problem tritt auf, wenn der lokale Standardwebbrowser nicht Internet Explorer ist. [CVADHELP-19041]

Anmeldung und Authentifizierung

- Versuche, eine Citrix Gateway-URL hinzuzufügen, schlagen möglicherweise gelegentlich mit dieser Fehlermeldung fehl:

  Authentication Service cannot be contacted.

  [CVADHELP-19415]

Sitzung/Verbindung

- Das Auflisten von Ressourcen für die Citrix Gateway-URL mithilfe des Storebrowse-Hilfsprogramms schlägt möglicherweise fehl, wenn mindestens einer der konfigurierten Delivery Controller nicht erreichbar ist. [CVADHELP-15416]
- Wenn Citrix IME aktiviert ist, reagieren bestimmte Anwendungen von Drittanbietern möglicherweise nicht und Anwendungsstarts in einer Benutzersitzung schlagen möglicherweise fehl. Das Problem tritt aufgrund eines Fehlers im CtxIme-Modul. [CVADHELP-18511]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Der Versuch, eine App zu aktualisieren oder zu starten, führt zu der Fehlermeldung **Store kann nicht kontaktiert werden**. Dieses Problem tritt auf, wenn das Abrufen der Verknüpfungsbeschreibung für bestimmte abonnierte Apps fehlschlägt.

  Die Apps stehen zurzeit nicht zur Verfügung. Versuchen Sie es in einigen Minuten erneut oder senden Sie folgende Informationen an den Helpdesk: Verbindung mit Store nicht möglich.

  [CVADHELP-18736]

- Versuche, eine Benutzersitzung zu starten, schlagen möglicherweise fehl, nachdem der Befehl **selfservice.exe** –**init** –**ipoll** –**exit** verwendet wurde. [CVADHELP-19095]

- Mit diesem Fix können Sie **TWITaskbarGroupingMode** in `HKEY_CURRENT_USER` oder `HKEY_LOCAL_MACHINE` auf **GroupNone** festlegen. Der Schlüssel **TWITaskbarGroupingMode** ist beispielsweise unter folgendem Pfad verfügbar: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows. [CVADHELP-19106]

Benutzererfahrung

- Wenn die Grafikrichtlinie "Zu verlustfrei verbessern"in einer Umgebung mit mehreren Monitoren aktiviert ist, kann das Ausweiten der Anzeige auf einen Laptop und einen externen Monitor zu einem verzerrten Bild führen. [CVADHELP-19065]

Citrix Workspace-App 1912 LTSR CU6 für Windows

Im Vergleich zu Citrix Workspace-App 1912 LTSR CU5

Probleme bei Clientgeräten

- Citrix Workspace-App-Sitzungen können hängen bleiben, wenn Sie ein YouTube-Video oder einen Microsoft Teams-Anruf beginnen und dann das Headset trennen. [CVADHELP-17629]

Installation, Deinstallation, Upgrade

- Wenn Sie die Citrix Workspace-App für Windows von CU4 auf CU5 aktualisieren, ohne Self-Service zu installieren, wird möglicherweise folgende Meldung angezeigt:

  Upgrade von nicht unterstützter Version

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Workspace deinstalliert automatisch die alte Version und löscht alle Einstellungen. Diese können Sie später wiederherstellen. Andernfalls müssen Sie alles manuell löschen. Klicken Sie auf "OK", um fortzufahren.

[CVADHELP-18790]

Anmeldung und Authentifizierung

- Wenn Sie sich mit einem falschen Kennwort bei Citrix Gateway anmelden, versucht Storebrowse mehrfach eine Authentifizierung und das Benutzerkonto kann gesperrt werden. [CVADHELP-17467]
- Die Citrix Workspace-App-Authentifizierung kann nach der Initialisierung fehlschlagen, wenn versucht wird, eine Smartcard über Citrix Gateway zu verwenden Wenn Sie den Authentifizierungsprozess nach 15 Minuten aktualisieren, wird möglicherweise eine 404-Fehlermeldung in dem in Citrix Workspace eingebetteten Browser angezeigt. Die App verbleibt dann in der Authentifizierungsschleife, bis Sie sie schließen und wieder öffnen. [CVADHELP-18305]

Sitzung/Verbindung

- Das Öffnen einer veröffentlichten Anwendung unter Einsatz der Ordnerumleitung kann mit der folgenden Fehlermeldung fehlschlagen, wenn die Ordnerumleitungsfreigabe offline ist.

  Die Anwendung konnte nicht gestartet werden.

  [CVADHELP-16387]
- Wenn Sie versuchen, eine Anwendung über die Verknüpfung zu öffnen und die Optionen **Auf eine Instanz pro Benutzer beschränken** und **vPrefer** sind aktiviert, wird in Citrix Director möglicherweise ein Verbindungsfehler angezeigt. [CVADHELP-17372]
- Während einer Telefonkonferenz mit Microsoft Teams im HDX-optimierten Modus flackert möglicherweise das Video eingehender Anrufe. [CVADHELP-17398]
- Die Citrix Workspace-App ruft möglicherweise externe Beacons für interne Stores ab. Durch diesen Fix werden keine externen Beacons abgerufen, wenn ein Store ohne Gateway verwendet wird. [CVADHELP-18275]
- Für veröffentlichte Anwendungen über die Citrix Workspace-App können keine Verknüpfungen ohne entsprechende Berechtigungen erstellt werden. Aus diesem Grund werden die Symbole evtl. bei jeder Aktualisierung in das Benutzerprofil heruntergeladen, was den Cache am Endpunkt aufbläht und den CPU-Verbrauch auf der StoreFront-Seite erhöht. [CVADHELP-18609]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Ein optimierter Microsoft Teams-Peer-zu-Peer-Anruf von der Citrix Workspace-App für Mac an die Citrix Workspace-App für Windows wird möglicherweise getrennt. [CVADHELP-18696]
- Das Starten von Sitzungen aus Bereitstellungsgruppen mit einer Zugriffsrichtlinienregel, die die Client-IP-Adresse angibt, kann fehlschlagen, wenn ein Client mehrere Netzwerkkarten hat

  ```
  Rule: Set-BrokerAccessPolicyRule -Name <rulename> -includedClientIPs
   <Client ip address>
  ```

  [CVADHELP-18783]

Systemausnahmen

- Citrix Authentication Manager (AuthManSvr.exe) wird während der Anmeldung möglicherweise unerwartet beendet. [CVADHELP-17233]

Benutzererfahrung

- Wenn Sie in einer Umgebung mit mehreren Monitoren ein Desktop-Fenster im Fenstermodus öffnen, kann Folgendes auftreten:

  Wenn das Fenster auf Monitor 1 geöffnet und auf Monitor 2 gezogen wird, wird es möglicherweise maximiert auf Monitor 1 statt auf Monitor 2 angezeigt.

  [CVADHELP-17373]

Benutzeroberfläche

- Durch diesen Fix können Sie zum erforderlichen Konto wechseln, wenn mehrere Konten und die aktuelle Kontoregistrierung konfiguriert sind. [CVADHELP-17718]
- Werden ein aktivierter und ein deaktivierter Store unter Einsatz eines Gruppenrichtlinienobjekts gemeinsam konfiguriert, wird beim ersten Mal für den aktivierten Store eine Nicht-X1-Benutzeroberfläche oder eine grüne Blase anstelle einer X1-Benutzeroberfläche angezeigt. [CVADHELP-17942]
- Beim Deaktivieren eines Store-Kontos in der Citrix Workspace-App werden die App-Verknüpfungen möglicherweise nicht aus dem **Startmenü** oder vom Desktop gelöscht. [CVADHELP-18260]

Citrix Workspace-App 1912 LTSR CU5 für Windows

Im Vergleich zu Citrix Workspace-App 1912 LTSR CU4

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Probleme bei Clientgeräten

- Bei Verwendung der Citrix Workspace-App 1912 LTSR CU4 können Geräte, die mit COM-Ports höher als 9 verbunden sind, in der Sitzung möglicherweise nicht zugeordnet werden. [CVADHELP-17734]

Installation, Deinstallation, Upgrade

- Das Upgrade der Citrix Workspace-App für Windows mit dem Parameter **/forceinstall** schlägt möglicherweise fehl. Das Problem tritt auf, wenn das Hilfsprogramm zur Bereinigung von Receiver die Bereinigung nicht startet. [CVADHELP-17656]

Anmeldung und Authentifizierung

- Wenn eine Citrix Gateway-Sitzung das Zeitlimit überschreitet, fordert Citrix Workspace beim Starten einer Anwendung möglicherweise nicht zur Authentifizierung auf. [CVADHELP-17187]

Seamlessfenster

- Einige Anwendungen von Drittanbietern bleiben möglicherweise im Vordergrund, sodass andere gestartete Anwendungen im Hintergrund bleiben. [CVADHELP-16897]

Sicherheitsprobleme

- Die Installation der Citrix Workspace-App 1912 LTSR für Windows schlägt möglicherweise fehl, wenn die USB-CAT-Dateien mit einem SHA-1-Zertifikat signiert sind. [CVADHELP-17679]

Sitzung/Verbindung

- Beim Navigieren auf Webseiten in einigen Browsern mit HTML oder Animation auf einem GPU-Thin Client reagiert die Citrix Workspace-App für Windows möglicherweise nicht mehr. Das Problem tritt auf, wenn der wfica32-Prozess viel Speicher belegt. [CVADHELP-16172]
- Nach dem Upgrade der Citrix Workspace-App für Windows auf Version 1912 LTSR CU1 oder CU2 schlägt die Sitzungszuverlässigkeit möglicherweise fehl. Das Problem tritt bei einer Verbindung über Citrix Gateway mit aktiviertem Enlightened Data Transport (EDT) auf. [CVADHELP-16694]
- Versuche, eine Sitzung über die Citrix Workspace-App für Windows zu starten, schlagen möglicherweise fehl, wenn der CGP-Port (2598) auf dem Endpunkt blockiert ist. [CVADHELP-17632]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Benutzererfahrung

- Dieser Fix unterdrückt das Popup für vertrauenswürdige Konten durch Verwenden einer neuen Gruppenrichtlinienobjekt-Einstellung: **Liste vertrauenswürdiger Storekonten**. [CVADHELP-16597]
- Beim Verwenden einiger Anwendungen von Drittanbietern auf einem VDA kann es zu Verzögerungen bei der Mausbewegung kommen. [CVADHELP-16737]

Benutzeroberfläche

- Bei Verwendung der Citrix Workspace-App 1912 LTSR CU2 für Windows werden Startmenüverknüpfungen möglicherweise nicht automatisch aktualisiert. Das Problem tritt auf, wenn eine neue Anwendung hinzugefügt oder auf dem Back-End eine Änderung vorgenommen wird. [CVADHELP-17122]
- Die Einstellung des Werts **CurrentAccount** auf **AllAccount** unter dem Registrierungsschlüssel HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle wird u. U. nicht wirksam. Das Problem tritt auf, wenn mindestens ein Storekonto vorhanden ist. [CVADHELP-17229]
- Wenn Sie versuchen, sich bei Wyse Thin Client-Geräten mit der Citrix Workspace-App für Windows anzumelden, wird die Autorisierungsaufforderung möglicherweise hinter dem Bildschirm **Desktop Lock** angezeigt. Daher können Sie sich erst anmelden, wenn Sie das Fenster mit der Autorisierungsaufforderung in den Vordergrund holen. [CVADHELP-17880]

Citrix Workspace-App 1912 LTSR CU4 für Windows

Im Vergleich zu Citrix Workspace-App 1912 LTSR CU3

Probleme bei Clientgeräten

- Wenn die Richtlinie **Client-COM-Portumleitung** aktiviert ist, kann der Zugriff auf den COM-Port des Bluetooth-Geräts fehlschlagen. [CVADHELP-14939]

Anmeldung und Authentifizierung

- Die Anmeldung bei Version 1912 LTSR CU3 der Citrix Workspace-App für Windows kann fehlschlagen, wenn der Benutzername einen Umlaut enthält. [CVADHELP-17267]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sicherheitsprobleme

- Der Ablaufsteuerungsschutz fehlt möglicherweise in den Binärdateien. [CVADHELP-16531]

Sitzung/Verbindung

- Bei Verwendung der Bildschirmfreigabe in Microsoft Teams während eines Peer-zu-Peer-Anrufs wird möglicherweise ein schwarzer Bildschirm angezeigt. [CVADHELP-15605]
- Wenn die Richtlinie **Adaptiver HDX-Transport** auf **Bevorzugt** festgelegt und **MTU-Discovery durch EDT** aktiviert ist, wird beim Starten von Anwendungen oder Desktops möglicherweise ein grauer oder schwarzer Bildschirm mit einer Warnmeldung angezeigt. [CVADHELP-15805]
- Die für eine Anwendung erstellte Verknüpfung wird möglicherweise nicht gelöscht, wenn die Anwendung deaktiviert oder der Pfad der Verknüpfung geändert wurde. [[CVADHELP-16448]
- Das Starten von Anwendungen über die Citrix Workspace-App für Windows kann fehlschlagen, wenn eine VPN-Verbindung über Citrix Gateway hergestellt oder getrennt wird. [CVADHELP-16714]
- In einem Double-Hop-Szenario werden die Namen der Endpunktclients möglicherweise nicht an den Delivery Controller oder an Director übergeben. Das Problem tritt ab VDA-Version 2003 auf. [CVADHELP-16783]
- Nach dem Upgrade der Citrix Workspace-App für Windows auf Version 1912 LTSR CU1 oder CU2 schlägt die Sitzungszuverlässigkeit möglicherweise fehl. Das Problem tritt bei einer Verbindung über Citrix Gateway mit aktiviertem Enlightened Data Transport (EDT) auf. [CVADHELP-16694]

Benutzererfahrung

- Bei Verwendung der Citrix Workspace-App Version 1912 LTSR CU2 für Windows werden in der Sitzung möglicherweise Grafikartefakte angezeigt, die Bildschirminhalte verdecken. [CVADHELP-16451]
- Nach dem Upgrade von Citrix Receiver 4.9.6 für Windows auf die Citrix Workspace-App 1912 LTSR CU2 oder CU3 kommt es vor, dass beim Starten einer Anwendungsverknüpfung die Verknüpfungssymbole auf dem Desktop blinken. [CVADHELP-16967]

Benutzeroberfläche

- Wenn Sie in einer Sitzung **Abmelden** auswählen, wird die Aufforderung **Abmelden** zur Bestätigung angezeigt. Wenn Sie hier **Abbrechen** auswählen, tritt ein Fehler auf. [CVADHELP-15516]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Nach dem Upgrade von Citrix Receiver 4.9 LTSR CU7 für Windows auf die Citrix Workspace-App CU2 oder CU3 für Windows kann es nach dem Versuch, das Standard-Storekonto festzulegen, zu inkonsistentem Verhalten kommen. Beispielsweise wird das Standard-Storekonto immer auf "Alle Konten"eingestellt. Bei dieser Änderung besteht die Einstellung des primären Storekontos auf einen anderen Store weiter, selbst wenn die Citrix Workspace-App beendet und neu gestartet wird. [CVADHELP-16903]

Citrix Workspace-App 1912 LTSR CU3 für Windows

Im Vergleich zu Citrix Workspace-App 1912 LTSR CU2

Installation, Deinstallation, Upgrade

- Wenn Sie versuchen, die Citrix Workspace-App mit der manuell erstellten Verknüpfung zu aktualisieren, wird die Verknüpfung möglicherweise gelöscht und dann neu erstellt. [CVADHELP-15397]

Tastatur

- Wenn Sie eine japanische Tastatur verwenden, funktioniert der Eingabemodus mit voller Breite möglicherweise nicht mit Microsoft Excel, wenn es über lokalen App-Zugriff gestartet wird. Das Problem tritt bei der Citrix Workspace-App für Windows auf, wenn die App-Schutzfunktion aktiviert ist. [CVADHELP-15410]

Anmeldung und Authentifizierung

- Auch wenn Sie die Richtlinien **Angemeldet bleiben** und **60 Tage lang nicht mehr fragen** aktiviert haben, fordert Microsoft Azure Multi-Factor Authentication Sie möglicherweise zur Authentifizierung auf.

  > **Hinweis:**
  >
  > Wir empfehlen, dass Benutzer ihre Stores schließen statt sich vom Store abzumelden. Wenn sich Benutzer mit der Webview-Authentifizierung von Stores abmelden, werden sie möglicherweise erneut zur Authentifizierung aufgefordert, da Internet Explorer-Cookies in solchen Szenarien gelöscht werden. Standardmäßig ist der Fix aktiviert (Cookies werden gespeichert). Sie können den Fix deaktivieren, indem Sie die GPO-Richtlinie **Speichern persistenter Cookies verhindern** unter **Citrix Komponenten > Citrix Workspace > Benutzerauthentifizierung** aktivieren. Wenn Sie den Fix deaktivieren, werden die Cookies

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> nicht gespeichert und während der Abmeldung gelöscht. Wenn Sie den Fix deaktivieren, werden die Cookies nicht gespeichert und während der Abmeldung gelöscht.

[CVADHELP-14814]

- Wenn die Citrix Workspace-App auf Geräten, die zur Azure Active Directory-Domäne (AD) gehören, versucht, auf einen Store zuzugreifen und dann die Endpunktanmeldeinformationen weitergibt, werden Benutzer möglicherweise nicht für die Anmeldung autorisiert. Außerdem gibt es keine Möglichkeit, sich mit einem anderen Benutzerkonto anzumelden. [CVADHELP-14844]

Drucken

- Wenn Sie ein Dokument im unformatierten Datenformat an die Druckerwarteschlange senden, wird das Dokument möglicherweise nicht gedruckt. Das Problem tritt auf, wenn Sie den XPS-Druckertreiber verwenden. [CVADHELP-14497]

Sitzung/Verbindung

- In bestimmten Szenarien stimmt die in Citrix Studio angezeigte Citrix-Produktlizenznutzung nicht mit der im Citrix License Manager angezeigten Lizenznutzung überein. [CVADHELP-14950]
- Wenn die Option **vPrefer** aktiviert ist, werden App-V-Anwendungen u. U. auf einem Remoteserver statt auf einem lokalen Server gestartet. [CVADHELP-15356]
- Wenn Sie einen veröffentlichten Desktop über eine native Citrix Workspace-App für Windows starten, wird die native Citrix Workspace-App automatisch im Vordergrund innerhalb des Desktops ausgeführt. Das Problem tritt auf, wenn das Feature **Lokaler App-Zugriff** aktiviert ist. [CVADHELP-15654]
- Der Prozess Selfservice.exe reagiert möglicherweise nicht mehr und eine Eingabeaufforderung **.NET-BroadcastEventWindow.4.0.0.0.1** wird angezeigt. Das Problem tritt auf, wenn Sie versuchen, sich von einem System mit Windows 10 Version 1909 abzumelden. [CVADHELP-15700]
- Sie konfigurieren die Citrix Workspace-App für Windows, sodass beim Einrichten einer Sitzung eine Verbindung mit allen Storekonten hergestellt wird. Wenn Sie sich von der Citrix Workspace-App abmelden und wieder anmelden, ändert sich die Storekontoeinstellung auf ein Storekonto, statt die Standardwerte für alle Konten zu verwenden. [CVADHELP-15728]
- Wenn die Richtlinie für die bidirektionale Inhaltsumleitung aktiviert ist, können Versuche, eine URL von einem Client zu einem VDA umzuleiten, fehlschlagen. [CVADHELP-15739]
- In Szenarien, in denen Proxyserver nicht den Port 8080 verwenden, kann die Citrix Workspace-App möglicherweise keine Verbindung zu veröffentlichten Anwendungen und Desktops

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

herstellen. Das Problem tritt auf, wenn die Citrix Workspace-App für Windows den Proxyport nicht verwendet und stattdessen den Standardport 8080 nutzt. [CVADHELP-15977]

- Die Citrix Workspace-App für Windows ignoriert möglicherweise die Einstellungen des Proxytyps. Das Problem tritt bei nicht englischsprachigen Microsoft Windows-Versionen auf. [CVADHELP-16017]
- Wenn die Registrierungseinstellung **EnableFactoryReset** auf **False** festgelegt ist, schlagen Versuche, die Citrix Workspace-App zu deinstallieren, möglicherweise mit folgender Fehlermeldung fehl:

  Dieses Feature wurde deaktiviert.

  [CVADHELP-16114]
- Wenn Microsoft Teams im optimierten Modus ist, kann das Audio verzerrt sein, wenn Sie an einer Telefonkonferenz teilnehmen. [CVADHELP-16232]

Systemausnahmen

- Wenn die Richtlinie **EchoCancellation** aktiviert ist und die Audioqualität auf "Mittel"eingestellt ist, wird der Prozess wfica32.exe möglicherweise sporadisch beendet, wodurch die Sitzungen schließlich getrennt werden. [CVADHELP-14568]
- Der Prozess Receiver.exe wird möglicherweise unerwartet beendet. [CVADHELP-15669]

Citrix Workspace-App 1912 LTSR CU2 für Windows

Im Vergleich zu Citrix Workspace-App 1912 LTSR CU1

Installation, Deinstallation, Upgrade

- Versuche, die Citrix Workspace-App für Windows von Version 190*x* auf Version 1912 zu aktualisieren, schlagen möglicherweise fehl. Das Problem tritt auf, wenn eine problematische Datei im Pfad des ausführbaren Ordners vorhanden ist. [CVADHELP-15277]
- Wenn Sie versuchen, die Citrix Workspace-App von Version 1912 auf Version 1912 CU1 oder 2006 zu aktualisieren, funktioniert die Update-Funktion der Citrix Workspace-App unter nicht englischen Betriebssystemen möglicherweise nicht. [CVADHELP-15357]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Tastatur

- Wenn Sie den chinesischen Eingabemethoden-Editor (IME) Wuxiami verwenden, bleibt die Umschalttaste möglicherweise in der Abwärtsposition stecken. Das Problem tritt auf, wenn die generische lokale Zeit auf **ON** festgelegt ist. [CVADHELP-15243]

Sicherheitsprobleme

- Dieser Fix behebt ein Sicherheitsproblem. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX277662. [CVADHELP-15613]

Sitzung/Verbindung

- Wenn das Registrierungsbearbeitungsprogramm deaktiviert ist, werden Registrierungsschlüssel aus der vorherigen Installation bei einem Upgrade möglicherweise nicht beibehalten. Daher schlagen Versuche, einen Desktop zu starten, fehl. [CVADHELP-15104]
- Die Citrix Workspace-App zeigt möglicherweise einen Skriptfehler in Versionen vor 1911 und eine leere Seite für die Versionen 1911 und höher an. Das Problem tritt bei Stores auf, die im Internet Explorer das WebBrowser-Steuerelement verwenden, um Anmeldeseiten anzuzeigen, wenn Microsoft Sicherheitsbaseline-GPO-Richtlinien angewendet werden. [CVADHELP-15475]
- In einem Double-Hop-Szenario schlagen Versuche, eine Anwendung über die Verknüpfung im **Startmenü** zu starten, möglicherweise fehl. Das Problem tritt auf, wenn Sie das Anwendungslimit von einer Instanz pro Benutzer aktivieren. [CVADHELP-15576]
- Wenn Sie sich über die Citrix Workspace-App Version 1912 oder höher bei einem Store anmelden, werden Anwendungen möglicherweise nicht aufgelistet. [CVADHELP-15597]

Benutzererfahrung

- Wenn Sie über ein VPN eine Verbindung zum Self-Service-Plug-In (SSP) herstellen, schlagen Versuche, das SSP zu aktualisieren, möglicherweise fehl. [CVADHELP-14418]
- Versuche, den Befehl **SelfService.exe -init -ipoll -exit** zu verwenden, um den Prozess SelfService.exe zu beenden, schlagen möglicherweise fehl. [CVADHELP-15126]
- Wenn Sie einen HP Active Pen verwenden, um in einer veröffentlichten Anwendung zu schreiben, kann es zu einer Verzögerung von drei bis vier Sekunden kommen. [CVADHELP-15203]
- Versuche, eine Sitzung zu starten, schlagen möglicherweise fehl, nachdem Sie eine Neuinstallation der Citrix Workspace-App für Windows durchgeführt oder eine vorhandene Installation auf

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

die neueste Version aktualisiert haben. Der Sitzungsstart bleibt auf dem Bildschirm **Ihr Desktop wird vorbereitet** hängen. Das Problem tritt auf, wenn Sie Desktop Lock mit einer Citrix Gateway-URL konfigurieren.

> **Hinweis:**
>
> Ein schwarzer Bildschirm wird für einige Zeit angezeigt, bevor Desktop Lock angezeigt wird, wenn Sie die Citrix Workspace-App für Windows zum ersten Mal mit einer Citrix Gateway-URL und Desktop Lock konfigurieren. Wenn der schwarze Bildschirm lange angezeigt wird, melden Sie sich bei einer physischen Maschine mit **Strg+Alt+Entf** und bei einer virtuellen Maschine mit **Strg+Alt+Ende** ab.

[CVADHELP-15334]

- Nach dem Upgrade der Citrix Workspace-App von Version 1912 auf Version 1912 CU1 ist die Anwendungsenumeration möglicherweise langsam und dauert etwa 10 Minuten. [CVADHELP-15766]

Citrix Workspace-App 1912 LTSR CU1 Hotfix 1 für Windows (19.12.1001)

Im Vergleich zu Citrix Workspace-App 1912 LTSR CU1 für Windows

Sicherheitsprobleme

- Dieser Fix behebt ein Sicherheitsproblem. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX277662. [CVADHELP-15613]

Citrix Workspace-App 1912 LTSR CU1 für Windows

Im Vergleich zu Citrix Workspace-App 1912 LTSR

Inhaltsumleitung

- Wenn Sie versuchen, eine lange URL umzuleiten, wird die URL möglicherweise nicht zu einem VDA umgeleitet und der Prozess Redirector.exe wird unerwartet mit der folgenden Ausnahme beendet:

  INVALID_CRUNTIME_PARAMETER

  [CVADHELP-13197]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Installation, Deinstallation, Upgrade

- Versuche, die Citrix Workspace-App auf einem VDA zu installieren oder zu aktualisieren, auf dem Windows 10 ausgeführt wird, schlagen möglicherweise fehl. Das Problem tritt auf, wenn Sie die folgenden Schritte ausführen:

  1. Installieren Sie die Citrix Workspace-App.
  2. installieren Sie einen VDA.
  3. Aktualisieren Sie die Citrix Workspace-App auf eine höhere Version.

  Das Problem tritt auf, weil das Upgrade oder die Installation dazu führt, dass Citrix Display Adapter entfernt werden. [CVADHELP-13764]

- Versuche, mit dem Feature für automatische Updates die HDX RealTime Media Engine (RTME) und die Citrix Workspace-App gleichzeitig zu aktualisieren, schlagen u. U. fehl. RTME wird nicht auf die neueste Version aktualisiert. [CVADHELP-15047]

Anmeldung und Authentifizierung

- Wenn Sie mit zwei verschiedenen Konten zwei Stores zur Citrix Workspace-App für Windows hinzufügen, funktioniert die Schaltfläche "Anmelden" möglicherweise nicht für den sekundären Store, nachdem Sie den primären Store entfernt haben. [CVADHELP-13805]
- Wenn die Multifaktorauthentifizierung aktiviert ist und das Windows-Sicherheitsdialogfeld zum Anmelden verwendet wird, wird das Dialogfeld "Active Directory-Verbunddienste (ADFS)" bei der Authentifizierung bei Stores nicht angezeigt. [CVADHELP-14316]
- Wenn Sie Citrix Gateway für die Unterstützung von Single Sign-On (SSO) über die Citrix Workspace-App konfigurieren, schlägt SSO möglicherweise fehl. Das Problem tritt auf, wenn ein Benutzername oder ein Kennwort Sonderzeichen wie **%**, **=** oder **&** enthält. [CVADHELP-14564]

SDK

- Dieser Fix bietet eine verbesserte Unterstützung für private Legacy-Schlüsselhandle. [CVADHELP-14530]

Sitzung/Verbindung

- Wenn Sie bei aktiviertem Desktop Lock und lokalem App-Zugriff die Tasten STRG+ALT+ENTF drücken und die Option "Benutzer wechseln" wählen, wird die lokale Benutzersitzung möglicherweise neu verbunden. Der erneute Verbindungsaufbau führt auf dem VDA jedoch

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

zu einem weißen Bildschirm, auf dem die Meldung "Verbunden mit Ihrem Desktop"angezeigt wird. Der Desktop wird nie angezeigt. [CVADHELP-13046]

- In einer Umgebung mit mehreren Monitoren schlagen Versuche, eine Benutzersitzung zu maximieren, möglicherweise fehl. Das Problem tritt auf, wenn Sie Ihren Laptop neu andocken. [CVADHELP-13614]
- In einem Double-Hop-Szenario wird die Citrix HDX Engine möglicherweise unerwartet beendet, wenn Sie versuchen, eine Sitzung zu starten. [CVADHELP-13915]
- Wenn die Option **vPrefer** in der Citrix Workspace-App aktiviert ist, schlagen Versuche, eine App-V-Anwendung zu starten, möglicherweise mit der folgenden Fehlermeldung fehl:

  Fehler beim Start

  [CVADHELP-14039]
- Nachdem Sie veröffentlichte Anwendungen zu **Favoriten** hinzugefügt haben, können Sie nur eine Anwendung öffnen. Das Problem tritt auf, wenn diese veröffentlichten Anwendungen denselben Namen der ausführbaren Datei verwenden, wie in **KEYWORDS:prefer="<application_name>** angegeben. [CVADHELP-14098]
- Die Registrierungswerte für das veraltete Feature **HDX MediaStream für Flash** (z. B. Flash und Flash2) werden möglicherweise nicht aus der Registrierungseinstellung HKEY_LOCAL_MACHINE\SOFTWARE\Client\Engine\Configuration\Advanced\Modules\ICA 3.0\VirtualDriver entfernt, nachdem Sie das Upgrade der Citrix Workspace-App ausgeführt haben. Dieses Problem kann zu einem Verbindungsfehler führen. [CVADHELP-14850]

Systemausnahmen

- Der Prozess wfica32.exe wird möglicherweise unerwartet beendet, wenn Sie versuchen, eine Verbindung zu einer Sitzung wiederherzustellen. Das Problem tritt in Version 1904.1 der Citrix Workspace-App für Windows auf. [CVADHELP-12807]
- Wenn lokaler App-Zugriff aktiviert ist, reagiert eine Sitzung möglicherweise nicht mehr und zeigt die folgende Fehlermeldung an:

  Citrix HDX Engine reagiert nicht

  [CVADHELP-14058]
- Wenn Sie versuchen, die Citrix Workspace-App zu installieren, ohne den Self-Service-Modus zu konfigurieren, tritt u. U. eine Ausnahme auf. Das Problem tritt auf, wenn Sie das Menü **Verknüpfungen und Wiederverbinden** auf der Seite **Erweiterte Einstellungen** öffnen. Das Problem tritt bei den Versionen 1907 bis 2002 der Citrix Workspace-App auf. [CVADHELP-14940]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

TWAIN

- Versuche, Scans mit einem TWAIN-Gerät durchzuführen, schlagen möglicherweise fehl. In der Spalte **Status** auf der Registerkarte **Anwendungen** des Windows Task-Managers wird "Keine Rückmeldung"für die Citrix HDX Engine angezeigt. [CVADHELP-14782]

Benutzererfahrung

- In Double-Hop-Szenarien, in denen VDAs für Multisitzungs-OS im ersten Hop ausgeführt werden und veröffentlichte Anwendungen im zweiten Hop ausgeführt werden, funktioniert die Option "Apps aktualisieren"im Menü des Citrix Workspace-App-Kontos möglicherweise nicht. [CVADHELP-13230]
- Wenn Sie ein Konto mit einer Store-URL in der Citrix Workspace-App für Windows hinzufügen, dauert die Ausführung möglicherweise lange. Das Problem tritt auf, wenn die URL eine Portnummer enthält. [CVADHELP-14051]
- In der Taskleiste werden zwei Citrix Workspace-App-Symbole angezeigt. Das Problem tritt in Version 1912 der Citrix Workspace-App auf. [CVADHELP-14577]
- Wenn Sie Single Sign-On in einer VDA-Umgebung verwenden, wird möglicherweise ein Begrüßungsbildschirm angezeigt. Das Problem tritt auf, wenn Sie die Citrix Workspace-App für Windows auf Version 1911 oder höher aktualisieren. [CVADHELP-14590]

Benutzeroberfläche

- Eine Anwendung versucht u. U. in den Vordergrund zu kommen, wodurch die aktuelle Anwendung verdrängt wird. Das Symbol in der Taskleiste blinkt möglicherweise und informiert den Benutzer darüber, dass die Anwendung versucht, in den Vordergrund zu kommen. [CVADHELP-13071]

Citrix Workspace-App 1912 LTSR für Windows

> **Hinweis:**
>
> Wenn Sie derzeit das aktuelle Release der Citrix Workspace-App 1911 verwenden und zur LTSR-Version wechseln möchten:
>
> Dieses Release enthält folgende Fixes im Vergleich zur Citrix Workspace-App 1911.
>
> Wenn Sie derzeit Citrix Receiver 4.9 für Windows verwenden und weiterhin die LTSR-Version nutzen möchten:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Dieses Release enthält alle Fixes in Citrix Receiver für Windows 4.9 bis 4.12 (einschließlich Kumulativer Updates), alle Fixes der Citrix Workspace-App 1808 bis 1911 sowie folgende Fixes der Citrix Workspace-App 2002 (im Vergleich zur Citrix Workspace-App 1911): Version 1912 enthält alle Fixes zwischen Citrix Receiver für Windows 4.9 LTSR CU9 und der Citrix Workspace-App Version 1911 sowie folgende Fixes:

HDX MediaStream Windows Media-Umleitung

- Wenn Sie in einer Umgebung mit mehreren Monitoren ein MP4-Video mit dem Windows Media Player in einer Benutzersitzung wiedergeben, wird das Video möglicherweise auf dem primären Monitor korrekt wiedergegeben. Wenn Sie den Player jedoch auf einen anderen Bildschirm verschieben, wird u. U. ein schwarzer Bildschirm auf dem sekundären oder auf einem erweiterten Monitor angezeigt, der mit DisplayLink über eine Dockingstation verbunden ist. [CVADHELP-11848]

Sitzung/Verbindung

- Wenn Sie versuchen, sich mit Schneller Smartcard von der HDX RealTime Media Engine erneut mit einer Sitzung zu verbinden, wird die HDX RealTime Media Engine möglicherweise unerwartet beendet. [CVADHELP-12605]
- Wenn veröffentlichte Anwendungen in kurzer Zeit viele Anforderungen zur Wiedergabe kurzer Töne erhalten, wird der Prozess wfica32.exe möglicherweise unerwartet beendet. [CVADHELP-12855]
- Nach Erreichen eines Sitzungstimeouts wird die Sitzung möglicherweise automatisch abgemeldet. Wenn Sie die Sitzung dann neu starten, dauert der Sitzungsstart länger als normal. Dieses Problem tritt auf, wenn eine Netzwerkunterbrechung vorliegt. [CVADHELP-13017]
- Das Fenster einer Seamlessanwendung wird möglicherweise verkürzt angezeigt, und Sie müssen die Fenstergröße manuell ändern. [CVADHELP-13108]
- Die Citrix Workspace-App prüft nun bei jedem Start oder Aktualisieren, ob Verknüpfungssymbole vorhanden sind. Wenn ein Symbol nicht verfügbar ist, ruft die Citrix Workspace-App das Symbol erneut ab. Dadurch wird sichergestellt, dass Verknüpfungen fehlerfrei angezeigt werden. [RFWIN-15501]
- Wenn Sie die Richtlinie "Bidirektionale Inhaltsumleitung"aktivieren wollen (unter **Computerkonfiguration > Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Workspace > Benutzererfahrung**), werden Sie auch bei deaktivierten URL-spezifischen Außerkraftsetzungen für Anwendungen oder Desktops aufgefordert, einen URL-spezifischen Eintrag einzugeben. [RFWIN-15867]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Systemausnahmen

- Der Prozess Receiver.exe wird beim Erfassen der CDF-Traces möglicherweise unerwartet beendet. [CVADHELP-13077]

Bekannte Probleme

October 26, 2023

Bekannte Probleme in der Citrix Workspace-App 1912 LTSR CU7 für Windows

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in der Citrix Workspace-App 1912 LTSR CU6 für Windows

- Wenn Sie Ihren Bildschirm in Microsoft Teams als veröffentlichte App freigeben, wird der rote Rand unten im freigegebenen Bildschirm nicht angezeigt. [LCMRFWIN-4194]

Bekannte Probleme in der Citrix Workspace-App 1912 LTSR CU5 für Windows

- Wenn Sie bestimmte Remoteanwendungen von Drittanbietern wie mRemoteNG mit einem Endpunkt verbinden und die Anwendungssymbolleiste der veröffentlichten Anwendung an die Seiten andocken, reagiert das System möglicherweise nicht mehr und die CPU-Auslastung steigt auf 100 %. [LCMRFWIN-4164]
- Wenn Sie versuchen, die Bildschirmfreigabe während eines für Microsoft Teams optimierten Anrufs zu stoppen, reagiert die Sitzung möglicherweise zeitweise nicht mehr. [LCMRFWIN-4184]

Bekannte Probleme in der Citrix Workspace-App 1912 LTSR CU4 für Windows

- Wenn Sie in einer Sitzung auf **Nach Updates suchen** klicken und Updates erfolgreich heruntergeladen werden, wird die aktuelle Sitzung nicht im Dialogfeld **Download wurde abgeschlossen** aufgeführt. [RFWIN-23152]

Bekannte Probleme in der Citrix Workspace-App 1912 LTSR CU3 für Windows

In diesem Release wurden keine neuen Probleme festgestellt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bekannte Probleme in der Citrix Workspace-App 1912 LTSR CU2 für Windows

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in der Citrix Workspace-App 1912 LTSR CU1 für Windows

- Versuche, die Webcam in einer WebEx-Besprechung zu verwenden, können dazu führen, dass die Citrix Workspace-App nicht mehr reagiert. Das Problem tritt auf, wenn Sie für das UDP-Audio **Mittel** einstellen.

  Navigieren Sie als Workaround zum folgenden Pfad im Registrierungs-Editor und legen Sie Folgendes fest:

  Pfad: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advance

  Name: EchoCancellation

  Typ: REG_SZ

  Wert: FALSE

  [DOCFB-3805]

Bekannte Probleme in der Citrix Workspace-App 1912 LTSR für Windows

- Versuche, einen Bildschirm mit der Taste **Druck/S-Abf** aufzuzeichnen, schlagen möglicherweise fehl. Dieses Problem tritt auf, wenn Sie eine geschützte Citrix Workspace-App-Sitzung minimieren. [RFWIN-15155]
- Wenn Sie Microsoft Word sowohl in einer veröffentlichten Sitzung als auch auf Ihrem lokalen Gerät starten und den Store in **Konten** löschen, wird beim Starten der App auf dem lokalen Gerät die folgende Fehlermeldung angezeigt:

  Möchten Sie eine Anwendung in Citrix Workspace suchen, um diese Datei zu öffnen?

  [RFWIN-15884]
- Der Sitzungsstart auf einem SSL-fähigen VDA schlägt möglicherweise fehl. [RFWIN-16129]
- In einer geschützten Desktopsitzung können möglicherweise keine Screenshots einer nicht geschützten Sitzung erstellt werden. [RFWIN-16704]
- Möglicherweise können Sie Storedetails nicht entfernen, die mit der administrativen Gruppenrichtlinienobjektvorlage über die grafische Benutzeroberfläche hinzugefügt wurden. [RFWIN-16754]
- Beim Versuch, die Anzeige in einer geschützten Sitzung zu ändern, wird die Sitzung möglicherweise beendet. [RFWIN-16784]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hinweise zu Drittanbietern

June 14, 2023

Die Citrix Workspace-App 1912 LTSR für Windows enthält ggf. Software von Drittanbietern, die gemäß den im folgenden Dokument aufgeführten Bestimmungen lizenziert ist:

Citrix Workspace-App für Windows –Hinweise zu Drittanbietern (PDF-Download)

Systemanforderungen und Kompatibilität

April 22, 2024

Anforderungen

- 1 GB RAM
- Anforderungen für .NET Framework
  - Das Self-Service-Plug-In erfordert .NET 4.6.2. Sie können die Apps und Desktops über die Benutzeroberfläche der Citrix Workspace-App für Windows oder über die Befehlszeile abonnieren und starten. Weitere Informationen finden Sie unter Verwenden von Befehlszeilenparametern.
- Aktuelle Version von Microsoft Visual C++ Redistributable.

  > **Hinweis:**
  >
  > Citrix empfiehlt, die neueste Version von Microsoft Visual C++ Redistributable zu verwenden. Andernfalls wird während eines Upgrades möglicherweise eine Aufforderung zum Neustart angezeigt.

  Ab Version 1904 enthält das Citrix Workspace App-Installationspaket keine einzelnen Microsoft Visual C++ Redistributable-Binärdateien, sondern das Microsoft Visual C++ Redistributable-Installationsprogramm. Während der Installation überprüft das Citrix Workspace-App-Installationsprogramm, ob das Microsoft Visual C++ Redistributable-Paket auf dem System vorhanden ist und installiert es gegebenenfalls. Für die Citrix Workspace-App Version 1912 und höher ist Microsoft Visual C++ Redistributable Version 14.24.28127.4 oder höher erforderlich.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Versuche, die Citrix Workspace-App mit Nicht-Administratorrechten auf einem System ohne Microsoft Visual C++ Redistributable-Paket zu installieren, schlagen möglicherweise fehl.

Nur ein Administrator kann das Microsoft Visual C++ Redistributable-Paket installieren.

Informationen zur Behebung von Problemen mit der Installation von .NET Framework oder Microsoft Visual C++ Redistributable finden Sie im Knowledge Center-Artikel CTX250044.

Kompatibilitätsmatrix

Die Citrix Workspace-App ist auch kompatibel mit allen derzeit unterstützten Versionen von Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) und Citrix Gateway, die in der Citrix Product Lifecycle Matrix aufgeführt sind.

Die Citrix Workspace-App ist mit folgenden Windows-Betriebssystemen kompatibel:

> **Hinweis:**
>
> Das Citrix Gateway Plug-In für die Endpunktanalyse (EPA) wird für Citrix Workspace unterstützt. In der nativen Citrix Workspace-App wird es nur unterstützt, wenn die Multifaktorauthentifizierung verwendet wird. Weitere Informationen finden Sie unter Konfigurieren des EPA-Scans für die Vor- und Nachauthentifizierung als Faktor in der Multifaktorauthentifizierung (nFactor) in der Dokumentation zu Citrix ADC.

Betriebssystem
Windows 10 (32-Bit- und 64-Bit-Enterprise Editionen) Weitere Informationen zum kompatiblen Windows 10-Betriebssystem finden Sie unter Kompatibilität von Windows 10 mit der Citrix Workspace-App für Windows.
Windows 10 32-Bit- und 64-Bit-Pro-Editionen (unterstützt ab Citrix Workspace-App 1912 LTSR CU5 für Windows)
Windows 8.1, 32-Bit- und 64-Bit-Editionen (inkl. Embedded Edition)
Windows 7, 32-Bit- und 64-Bit-Editionen (Erweitertes Sicherheitsupdate –ESU)
Windows 7 Embedded Standard (Erweitertes Sicherheitsupdate - ESU)
Windows Thin PC
Windows Server 2016
Windows Server 2012 R2, Standard und Datacenter Edition

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Betriebssystem
Windows Server 2019
Windows Server 2008 R2
Windows 10 Enterprise LTSC 2019
Windows 10 Enterprise 2016 LTSB 1607

Kompatibilität von Windows 10 mit der Citrix Workspace-App für Windows

> **Hinweis:**
>
> - Die Installation von Citrix-Softwareversionen, die vor der Version für den halbjährlichen Kanal veröffentlicht wurden, wird nicht empfohlen. Kunden, die diese Versionen dennoch installieren, müssen im Supportfall prüfen, ob ihr Problem nicht durch ein Upgrade auf eine neuere Citrix-Softwareversion behoben werden kann (sofern verfügbar) und diese gegebenenfalls installieren.
> - Sobald eine Windows 10-Version ihr Dienstende erreicht, wird sie von Microsoft nicht länger unterstützt. Citrix unterstützt die eigene Software nur für Betriebssysteme, die vom Hersteller unterstützt werden. Weitere Informationen zum Dienstende von Windows 10-Versionen finden Sie im Informationsblatt zum Lebenszyklus von Windows.

Version der Citrix Workspace-App	Version der Windows 10 Enterprise Edition	Buildnummer
1912 CU7 und höher	LTSC 2021	19044
1912 CU6 und höher	21H2	19044
1912 CU6 und höher	21H2	19044
1912 CU5 und höher	21H1	19043.1165
1912 CU2 und höher	20H2	19042.685
1912 CU1 und höher	2004	19041.329
1911 und höher	1909	18363.418
1909 und höher	1903	18362.116
1812 und höher	1809	17763.107
1808 und höher	10 1803	17134.376

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Unterstützte Browser

Eine Liste der unterstützten Browser finden Sie unter Zugriff auf Stores über Citrix Receiver für Web-Sites.

Betriebssystemmatrix

Auf Touchgeräten unterstützte Betriebssysteme
Windows 10
Windows 8
Windows 7

Auf VDAs unterstützte Betriebssysteme
Windows 10
Windows 8
Windows 7
Windows 2012 R2
Windows Server 2016
Windows 2008 R2

Überprüfen auf freien Speicherplatz

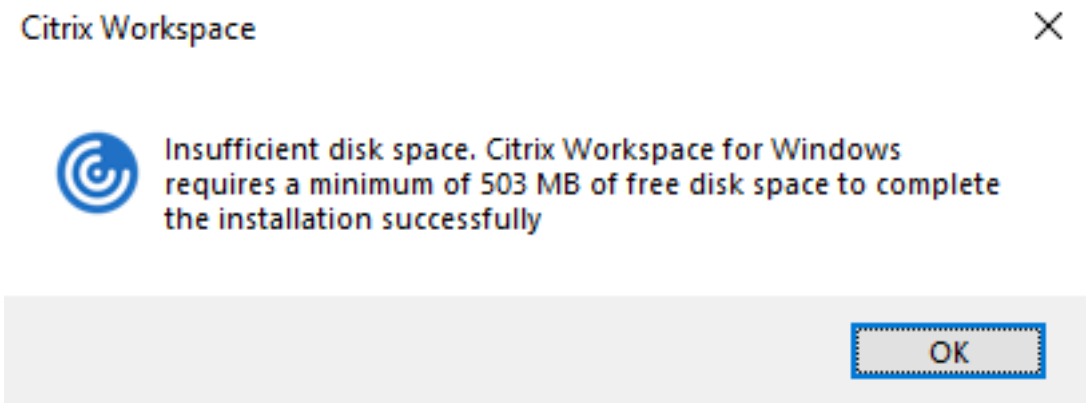
Die folgende Tabelle enthält Informationen zum Speicherplatz, der für die Installation der Citrix Workspace-App für Windows erforderlich ist:

Installationstyp	Erforderlicher Speicherplatz
Neuinstallation	572 MB
Upgrade	350 MB

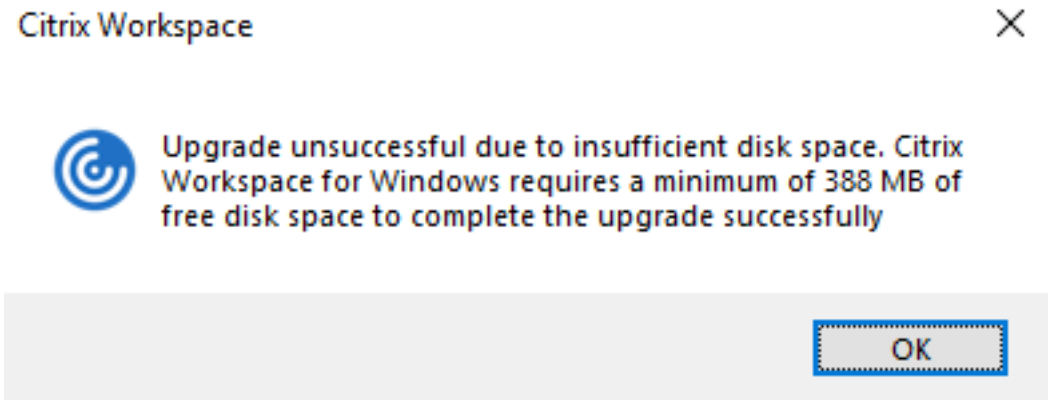
Die Citrix Workspace-App prüft, ob genügend Speicherplatz zum Abschließen der Installation verfügbar ist. Die Überprüfung erfolgt sowohl bei einer Neuinstallation als auch bei einem Upgrade.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bei einer Neuinstallation wird die Installation abgebrochen, wenn nicht genügend Speicherplatz vorhanden ist, und das folgende Dialogfeld wird angezeigt.



Bei einem Upgrade wird die Installation abgebrochen, wenn nicht genügend Speicherplatz vorhanden ist, und das folgende Dialogfeld wird angezeigt.



Hinweis:

- Das Installationsprogramm führt die Überprüfung des Speicherplatzes erst aus, wenn Sie das Installationspaket extrahiert haben.
- Wenn bei einer automatischen Installation nicht genug Speicherplatz vorhanden ist, wird das Dialogfeld nicht angezeigt, aber die Fehlermeldung wird im Protokoll `CTXInstall\\_TrolleyExpress-\*.log` aufgezeichnet.

Verbindungen, Zertifikate und Authentifizierung

Verbindungen

- HTTP-Store
- HTTPS-Store
- Citrix Gateway 10.5 und höher

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Webinterface 5.4

Zertifikate

> **Hinweis:**
>
> Die Citrix Workspace-App für Windows ist digital signiert. Die digitale Signatur ist mit einem Zeitstempel versehen. Das Zertifikat ist also auch nach Ablauf gültig.

- Privat (selbstsigniert)
- Stamm
- Platzhalter
- Zwischenzertifikat

Private (selbstsignierte) Zertifikate

Wenn ein privates Zertifikat auf dem Remotegateway installiert ist, muss das Stammzertifikat der Zertifizierungsstelle des Unternehmens auf dem Benutzergerät installiert sein, mit dem Sie auf Citrix-Ressourcen zugreifen.

> **Hinweis:**
>
> Wenn das Zertifikat des Remotegateways beim Herstellen der Verbindung nicht verifiziert werden kann (da das Stammzertifikat nicht im lokalen Schlüsselspeicher ist), wird eine Warnung über ein nicht vertrauenswürdiges Zertifikat angezeigt. Wenn der Benutzer weiterarbeitet, werden die Apps angezeigt, können jedoch nicht gestartet werden.

Stammzertifikate

Für in Domänen eingebundene Computer können Sie ZS-Zertifikate mit der administrativen Gruppenrichtlinienobjektvorlage verteilen und als vertrauenswürdig einstufen.

Für nicht domänengebundene Computer können Unternehmen ein benutzerdefiniertes Installationspaket erstellen und damit das Zertifikat der Zertifizierungsstelle verteilen und installieren. Wenden Sie sich bei Fragen an den Systemadministrator.

Zertifikate mit Platzhalterzeichen

Zertifikate mit Platzhalterzeichen werden für einen Server in derselben Domäne verwendet.

Die Citrix Workspace-App unterstützt Zertifikate mit Platzhalterzeichen. Diese dürfen jedoch nur gemäß den jeweils gültigen Sicherheitsrichtlinien verwendet werden. In der Praxis kann als Alternative zu Zertifikaten mit Platzhalterzeichen ein Zertifikat verwendet werden, das eine Liste der

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Servernamen mit der SAN-Erweiterung (Subject Alternative Name) enthält. Private und öffentliche Zertifizierungsstellen stellen diese Zertifikate aus.

Zwischenzertifikate

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem Citrix Gateway-Serverzertifikat angehängt werden. Weitere Informationen finden Sie unter Konfigurieren von Zwischenzertifikaten.

Authentifizierung

Authentifizierung bei StoreFront

	Workspace für Web über Browser	StoreFront Services-Site (nativ)	StoreFront, Citrix Virtual Apps and Desktops (nativ), Citrix DaaS	Citrix Gateway bei Workspace für Web (Browser)	Citrix Gateway bei StoreFront Services-Site (nativ)
Anonym	Ja	Ja			
Domäne	Ja	Ja	Ja	Ja*	Ja*
Domänen-Passthrough	Ja	Ja	Ja		
Sicherheitstoken				Ja*	Ja*
Zweistufige Authen-tifizierung (Domäne mit Sicherheitsto-ken)				Ja*	Ja*
SMS				Ja*	Ja*
Smartcard	Ja	Ja		Ja	Ja
Benutzerzertifikat				Ja (Citrix Gateway Plug-In)	Ja (Citrix Gateway Plug-In)

* Mit oder ohne Citrix Gateway als installiertes Plug-In auf dem Gerät.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Die Citrix Workspace-App unterstützt die zweistufige Authentifizierung (Domäne plus Sicherheitstoken) über Citrix Gateway beim nativen StoreFront-Service.

Authentifizierung beim Webinterface Die Citrix Workspace-App unterstützt die folgenden Authentifizierungsmethoden (beim Webinterface wird die Authentifizierung mit Domäne und Sicherheitstoken als **explizit** bezeichnet):

	Webinterface (Browser)	**Webinterface-Site mit Citrix Gateway**	**Citrix Gateway bei Webinterface (Browser)**	**Citrix Gateway bei Webinterface-Site mit Citrix Gateway**
Anonym	Ja			
Domäne	Ja	Ja	Ja*	
Domänen-Passthrough	Ja	Ja		
Sicherheitstoken			Ja*	
Zweistufige Authentifizierung (Domäne mit Sicherheitstoken)			Ja*	
SMS			Ja*	
Smartcard	Ja	Ja		
Benutzerzertifikat			Ja (Citrix Gateway Plug-In)	

* Nur in Bereitstellungen verfügbar, die Citrix Gateway mit oder ohne installiertem zugeordneten Plug-In auf dem Gerät enthalten.

Informationen zur Authentifizierung finden Sie hier:

- Konfigurieren von Authentifizierung und Autorisierung in der Citrix Gateway-Dokumentation.
- Konfigurieren von Authentifizierung und Delegierung in der StoreFront-Dokumentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Zertifikatsperrliste

Wenn Sie die Überprüfung von Zertifikatsperrlisten (CRL) aktivieren, überprüft die Citrix Workspace-App, ob das Zertifikat des Servers widerrufen wurde. Durch diese Überprüfung wird die kryptografische Authentifizierung für den Server sowie die allgemeine Sicherheit der TLS-Verbindung zwischen Benutzergerät und Server verbessert.

Sie können die Überprüfung der Zertifikatsperrlisten in mehreren Stufen einstellen. Sie können die Citrix Workspace-App beispielsweise so konfigurieren, dass nur die lokale Zertifikatsperrliste oder die lokale und die Netzwerkzertifikatsperrliste überprüft werden. Außerdem können Sie die Überprüfung der Zertifikatsperrliste so konfigurieren, dass Benutzer sich nur anmelden können, wenn alle Zertifikatsperrlisten überprüft wurden.

Schließen Sie die Citrix Workspace-App und alle Citrix Workspace-Komponenten, einschließlich **Connection Center**.

Weitere Informationen finden Sie unter TLS.

Installation und Deinstallation

May 23, 2024

Hinweise für Administratoren vor der Installation der Citrix Workspace-App 1912 LTSR für Windows

- Die Citrix Workspace-App 1912 LTSR für Windows erfordert .NET Framework Version 4.6.2 oder höher. Wenn es nicht vorhanden ist, wird .NET Framework bei der Installation der Citrix Workspace-App heruntergeladen und installiert. Es wird jedoch empfohlen, die erforderliche .NET Framework-Version manuell zu installieren, bevor Sie die Citrix Workspace-App installieren oder aktualisieren.
- Informationen zu einer unbeaufsichtigten Installation finden Sie im Knowledge Center-Artikel CTX257546.
- Aktuelle Informationen zu unterstützten und nicht unterstützten Verschlüsselungssammlungen finden Sie im Knowledge Center-Artikel CTX250104.

Zum Installieren der Citrix Workspace-App können Sie das Installationspaket `CitrixWorkspaceApp.exe` von der Downloadseite oder der Downloadseite Ihres Unternehmens (falls verfügbar) herunterladen. Sie können das Paket wie folgt installieren:

- Ausführen eines interaktiven Windows-Installationsassistenten oder

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Eingeben des Dateinamens des Installationsprogramms, der Installationsbefehle und der Installationseigenschaften über die Befehlszeilenschnittstelle. Informationen zum Installieren der Citrix Workspace-App über die Befehlszeilenschnittstelle finden Sie unter Verwenden von Befehlszeilenparametern.

Installation mit Administrator- und Nicht-Administrator-Rechten:

Benutzer und Administratoren können die Citrix Workspace-App installieren. Sie benötigen nur dann Administratorrechte, wenn Sie die Passthrough-Authentifizierung und Citrix Ready Workspace Hub mit der Citrix Workspace-App für Windows verwenden.

Die folgende Tabelle zeigt die Unterschiede bei der Installation der Citrix Workspace-App als Administrator oder als Benutzer:

	Installationsordner	Installationstyp
Administrator	C:\Programme (x86)\Citrix\ICA Client	Installation pro System
Benutzer	%USERPROFILE%\AppData\Local\Citrix\ICA Client	Installation pro Benutzer

> **Hinweis:**
>
> Wenn eine vom Benutzer installierte Instanz der Citrix Workspace-App für Windows auf dem System vorhanden ist und ein Administrator die App auf demselben System installiert, verursacht dies einen Konflikt. Citrix empfiehlt, dass Sie alle von Benutzern installierten Instanzen der Citrix Workspace-App für Windows deinstallieren, bevor Sie die App als Administrator installieren.

Verwenden eines Windows-basierten Installationsprogramms

Sie können die Citrix Workspace-App für Windows vom Installationsmedium, von einer Netzwerkfreigabe und Windows Explorer oder über eine Befehlszeile durch manuelles Ausführen des Installationspakets `CitrixWorkspaceApp.exe` installieren.

Standardmäßig befinden sich die Installationsprotokolle unter `%temp%\CTXReceiverInstallLogs*.logs`.

1. Starten Sie die Datei `CitrixWorkspaceApp.exe` und klicken Sie auf **Start**.
2. Lesen und akzeptieren Sie die Lizenzvereinbarung und fahren Sie mit der Installation fort.
3. Wenn Sie die Installation auf einer domänengebundenen Maschine mit Administratorrechten durchführen, wird ein zusätzliches Dialogfeld angezeigt, um Single Sign-On zu aktivieren oder zu deaktivieren. Weitere Informationen finden Sie unter Domänen-Passthrough-Authentifizierung.
4. Folgen Sie dem Windows-basierten Installationsprogramm, um die Installation abzuschließen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verwenden von Befehlszeilenparametern

Sie können die Citrix Workspace-App installieren, indem Sie den Dateinamen des Installationsprogramms, die Installationsbefehle und die Installationseigenschaften an der Befehlszeilenschnittstelle eingeben. Sie können das Installationsprogramm für die Citrix Workspace-App durch Festlegen von Befehlszeilenoptionen anpassen. Das Installationspaket wird automatisch vor dem Start des Setupprogramms im temporären Ordner des Betriebssystems extrahiert. Der benötigte Speicherplatz berücksichtigt Programmdateien, Benutzerdaten und temporäre Ordner nach dem Start mehrerer Anwendungen.

Um die Citrix Workspace-App über die Windows-Befehlszeile zu installieren, starten Sie die Eingabeaufforderung und geben dann den Dateinamen des Installationsprogramms, die Installationsbefehle und Installationseigenschaften in einer einzigen Zeile ein. Die verfügbaren Installationsbefehle und -eigenschaften sind nachfolgend aufgeführt:

```
CitrixWorkspaceApp.exe [commands] [properties]
```

Liste der Befehlszeilenparameter

Die Parameter werden wie folgt klassifiziert:

- Allgemeine Parameter
- Installationsparameter
- HDX-Parameter
- Parameter für Einstellungen und Benutzeroberfläche
- Authentifizierungsparameter

Allgemeine Parameter

- /? oder /`help` - Listet alle Installationsbefehle und -eigenschaften auf.
- /`silent` - Deaktiviert Installationsdialogfelder und Eingabeaufforderungen während der Installation.
- /`noreboot` - Unterdrückt die Aufforderungen zum Neustart des Dialogfelds während der Installation. Wenn Sie die Neustartaufforderung unterdrücken, werden USB-Geräte, die im ausgesetzten Zustand sind, erst nach dem Neustart des Benutzergeräts von der Citrix Workspace-App erkannt.
- /`includeSSON` - Erfordert die Installation mit Administratorrechten. Gibt an, dass die Citrix Workspace-App mit der Single Sign-On-Komponente installiert wird. Weitere Informationen finden Sie unter Domänen-Passthrough-Authentifizierung.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- /rcu - Dieser Switch ist nur wirksam, wenn ein Upgrade von einer nicht unterstützten Version der Software durchgeführt wird. Gibt an, dass die Citrix Workspace-App durch Deinstallation der vorhandenen Version installiert oder aktualisiert wird. Dadurch werden auch vorhandene Einstellungen bereinigt.

  > Hinweis:
  >
  > Die Befehlszeilenoption /rcu ist ab Version 1909 veraltet. Weitere Informationen finden Sie unter Einstellung von Features und Plattformen.

- /forceinstall Diese Option ist wirksam, wenn vorhandene Konfigurationen oder Einträge der Citrix Workspace-App in einem der folgenden Szenarios bereinigt werden:
  - Sie führen ein Upgrade von einer nicht unterstützten Citrix Workspace-App-Version aus.
  - Die Installation oder das Upgrade schlägt fehl.

Installationsparameter

/AutoUpdateCheck

Gibt an, dass Citrix Workspace für Windows erkennt, wenn ein Update verfügbar ist.

- Auto - Sie werden benachrichtigt, wenn ein Update zur Verfügung steht. Beispiel: CitrixWorkspaceApp.exe /AutoUpdateCheck=auto.
- Manual - Sie werden nicht benachrichtigt, wenn ein Update verfügbar ist. Suchen Sie manuell nach Updates. Beispiel: CitrixWorkspaceApp.exe /AutoUpdateCheck=manual.
- Disabled - Das Feature für automatische Updates ist deaktiviert. Beispiel: CitrixWorkspaceApp.exe /AutoUpdateCheck=disabled.

/AutoUpdateStream

Wenn Sie die automatische Aktualisierung aktiviert haben, können Sie den Releasepfad für die Aktualisierung auswählen. Weitere Informationen finden Sie unter Lifecycle Milestones.

- LTSR - Die automatische Aktualisierung auf des Long Term Service Release erfolgt nur kumulativ. Beispiel: CitrixWorkspaceApp.exe /AutoUpdateStream=LTSR.
- Current - Die automatische Aktualisierung erfolgt auf die neueste Version der Citrix Workspace-App handelt. Beispiel: CitrixWorkspaceApp.exe /AutoUpdateStream=Current.

/DeferUpdateCount

Gibt an, wie oft Sie Updatebenachrichtigungen ignorieren können, wenn ein Update verfügbar ist. Weitere Informationen finden Sie unter Citrix Workspace-Updates.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- -1 (Standard) –Ermöglicht das Ignorieren von Benachrichtigungen beliebig oft. Beispiel: `CitrixWorkspaceApp.exe /DeferUpdateCount=-1`.
- 0 - Gibt an, dass Sie pro verfügbares Update nur eine Benachrichtigung erhalten. Sie werden nicht erneut an das Update erinnert. Beispiel: `CitrixWorkspaceApp.exe /DeferUpdateCount=0`.
- Jede andere Nummer "n"- Ermöglicht das Ignorieren von Updatebenachrichtigungen "n" Mal. Die Option **Später erinnern** wird gemäß der festgelegten Zahl "n"angezeigt. Beispiel: `CitrixWorkspaceApp.exe /DeferUpdateCount=<n>`.

/AURolloutPriority

Wenn eine neue App-Version veröffentlicht wird, stellt Citrix das Update während des Bereitstellungszeitraums bereit. Mit diesem Parameter können Sie steuern, zu welchem Zeitpunkt während des Bereitstellungszeitraums Sie das Update erhalten können.

- Auto (Standard) - Sie erhalten Updates während des Bereitstellungszeitraums wie von Citrix konfiguriert. Beispiel: `CitrixWorkspaceApp.exe /AURolloutPriority=Auto`.
- Fast –Sie erhalten Updates zu Beginn des Bereitstellungszeitraums. Beispiel: `CitrixWorkspaceApp.exe /AURolloutPriority=Fast`.
- Medium - Sie erhalten Updates nach Ablauf der Hälfte des Bereitstellungszeitraums. Beispiel: `CitrixWorkspaceApp.exe /AURolloutPriority=Medium`.
- Slow –Sie erhalten Updates gegen Ende des Bereitstellungszeitraums. Beispiel: `CitrixWorkspaceApp.exe /AURolloutPriority=Slow`.

/includeappprotection

Bietet mehr Sicherheit bei der Verwendung von Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service), da Clients besser vor Bildschirmerfassungs- und Keylogging-Malware geschützt sind.

- `CitrixWorkspaceApp.exe /includeappprotection`

Weitere Informationen finden Sie unter App Protection.

INSTALLDIR

Gibt das benutzerdefinierte Installationsverzeichnis für die Installation der Citrix Workspace-App an. Der Standardpfad ist `C:\Program Files\Citrix`. Beispiel: `CitrixWorkspaceApp.exe INSTALLDIR=C:\Program Files\Citrix`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ADDLOCAL

Installiert die angegebenen Komponenten. Beispiel: `CitrixWorkspaceapp.exe ADDLOCAL =ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopViewer,Flash,Vd3d, WebHelper,BrowserEngine,WorkspaceHub,USB`.

HDX-Parameter

ALLOW_BIDIRCONTENTREDIRECTION

Gibt an, dass die bidirektionale Inhaltsumleitung zwischen Client-zu-Host und Host-zu-Client aktiviert ist. Weitere Informationen finden Sie unter Richtlinieneinstellungen für die bidirektionale Inhaltsumleitung in der Dokumentation zu Citrix Virtual Apps and Desktops.

- 0 (Standard) –Die bidirektionale Inhaltsumleitung ist deaktiviert. Beispiel: `CitrixWorkspaceApp .exe ALLOW_BIDIRCONTENTREDIRECTION=0`.
- 1 –Die bidirektionale Inhaltsumleitung ist aktiviert. Beispiel: `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=1`.

FORCE_LAA

Gibt an, dass die Citrix Workspace-App mit der clientseitigen Komponente für den lokalen App-Zugriff installiert ist. Sie müssen die Citrix Workspace-App mit Administratorrechten installieren, damit diese Komponente funktioniert. Weitere Informationen finden Sie unter Lokaler App-Zugriff in der Dokumentation zu Citrix Virtual Apps and Desktops.

- 0 (Standard) –Die Komponente für den lokalen App-Zugriff ist nicht installiert. Beispiel: `CitrixWorkspaceApp.exe FORCE_LAA=0`.
- 1 –Die clientseitige Komponente für den lokalen App-Zugriff ist installiert. Beispiel: `CitrixWorkspaceApp.exe FORCE_LAA=1`.

LEGACYFTAICONS

Gibt an, ob Anwendungssymbole für Dokumente angezeigt werden, die Dateitypzuordnungen für abonnierte Anwendungen haben.

- False (Standard) –Die Anwendungssymbole werden für Dokumente oder Dateien angezeigt, die Dateitypzuordnungen für abonnierte Anwendungen aufweisen. Wenn dieser Wert auf "false" gesetzt ist, generiert das Betriebssystem ein Symbol für ein Dokument, dem kein bestimmtes Symbol zugewiesen ist. Das vom Betriebssystem generierte Symbol ist ein generisches

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Symbol, das mit einer kleineren Version des Anwendungssymbols überlagert wird. Beispiel: `CitrixWorkspaceApp.exe LEGACYFTAICONS=False`.
- True –Die Anwendungssymbole werden nicht für Dokumente oder Dateien angezeigt, die Dateitypzuordnungen für abonnierte Anwendungen aufweisen. Beispiel: `CitrixWorkspaceApp.exe LEGACYFTAICONS=True`.

ALLOW_CLIENTHOSTEDAPPSURL

Aktiviert die URL-Umleitung auf einem Benutzergerät. Weitere Informationen finden Sie unter Lokaler App-Zugriff in der Dokumentation zu Citrix Virtual Apps and Desktops.

- 0 (Standard) –Deaktiviert die URL-Umleitungsfunktion auf einem Benutzergerät. Beispiel: `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=0`.
- 1 –Aktiviert die URL-Umleitung auf einem Benutzergerät. Beispiel: `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=1`.

Parameter für Einstellungen und Benutzeroberfläche

ALLOWADDSTORE

Ermöglicht es Ihnen, die Stores (http oder https) basierend auf dem angegebenen Parameter zu konfigurieren.

- S (Standard) –Sie können nur sichere Stores (mit HTTPS konfiguriert) hinzufügen oder entfernen. Beispiel: `CitrixWorkspaceApp.exe ALLOWADDSTORE=S`.
- A - Sie können sichere (HTTPS) und nicht sichere (HTTP) Stores hinzufügen oder entfernen. Gilt nicht, wenn die Citrix Workspace-App pro Benutzer installiert ist. Beispiel: `CitrixWorkspaceApp.exe ALLOWADDSTORE=A`.
- N –Benutzer können nie einen eigenen Store hinzufügen. Beispiel: `CitrixWorkspaceApp.exe ALLOWADDSTORE=N`.

ALLOWSAVEPWD

Ermöglicht Ihnen, die Anmeldeinformationen für den Store lokal zu speichern. Dieser Parameter gilt nur für Stores, die das PNAgent-Protokoll verwenden.

- S (Standard) –Ermöglicht das Speichern von Kennwörtern nur für sichere Stores, die mit HTTPS konfiguriert sind. Beispiel: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=S`.
- N –Das Speichern von Kennwörtern ist nicht zulässig. Beispiel: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=N`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- A –Ermöglicht das Speichern von Kennwörtern für sichere Stores (HTTPS) und nicht sichere Stores (HTTP). Beispiel: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=A`.

STARTMENUDIR

Gibt den Ordner für die Verknüpfungen im Startmenü an.

- `<Directory Name>` –Standardmäßig werden Anwendungen unter **Start** > **Alle Programme** angezeigt. Sie können den relativen Pfad für die Verknüpfungen im Ordner `\Programs` angeben. Beispiel: Geben Sie `STARTMENUDIR=\Workspace` an, um Verknüpfungen unter Start > Alle Programme > Workspace zu platzieren.

DESKTOPDIR

Gibt den Ordner für Verknüpfungen auf dem Desktop an.

> **Hinweis:**
>
> Wenn Sie die Option DESKTOPDIR verwenden, legen Sie den Schlüssel `PutShortcutsOnDesktop` auf `True` fest.

- `<Directory Name>` –Sie können den relativen Pfad für Verknüpfungen angeben. Beispiel: Geben Sie `DESKTOPDIR=\Workspace` an, um Verknüpfungen unter Start > Alle Programme > Workspace zu platzieren.

SELFSERVICEMODE

Steuert den Zugriff auf die Self-Service-Benutzeroberfläche der Citrix Workspace-App.

- True –Der Benutzer hat Zugriff auf die Self-Service-Benutzeroberfläche. Beispiel: `CitrixWorkspaceApp.exe SELFSERVICEMODE=True`.
- False –Gibt an, dass der Benutzer keinen Zugriff auf die Self-Service-Benutzeroberfläche hat. Beispiel: `CitrixWorkspaceApp.exe SELFSERVICEMODE=False`.

ENABLEPRELAUNCH

Steuert den Vorabstart von Sitzungen. Weitere Informationen finden Sie unter Dauer des Anwendungsstarts.

- True - Gibt an, dass Sitzungsvorabstart aktiviert ist. Beispiel: `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True`.
- False - Gibt an, dass Sitzungsvorabstart deaktiviert ist. Beispiel: `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

DisableSetting

Ausblenden der Option **Verknüpfungen und Wiederverbinden** auf der Seite **Erweiterte Einstellungen**. Weitere Informationen finden Sie unter Ausblenden bestimmter Einstellungen auf der Seite "Erweiterte Einstellungen".

- 0 (Standard) –Die Optionen **Verknüpfungen** und **Wiederverbinden** werden auf der Seite "Erweiterte Einstellungen"angezeigt. Beispiel: `CitrixWorkspaceApp.exe DisableSetting=0`.
- 1 –Nur die Option **Wiederverbinden** wird auf der Seite "Erweiterte Einstellungen"angezeigt. Beispiel: `CitrixWorkspaceApp.exe DisableSetting=1`.
- 2 –Nur die Option **Verknüpfungen** wird auf der Seite "Erweiterte Einstellungen"angezeigt. Beispiel: `CitrixWorkspaceApp.exe DisableSetting=2`.
- 3 –Die Optionen **Verknüpfungen** und **Wiederverbinden** werden beide auf der Seite "Erweiterte Einstellungen"ausgeblendet. Beispiel: `CitrixWorkspaceApp.exe DisableSetting=3`.

EnableCEIP

Gibt an, dass Sie am Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) teilnehmen. Weitere Informationen finden Sie unter CEIP.

- True (Standard) - Teilnahme an CEIP. Beispiel: `CitrixWorkspaceApp.exe EnableCEIP=True`.
- False - Keine Teilnahme an CEIP. Beispiel: `CitrixWorkspaceApp.exe EnableCEIP=False`.

EnableTracing

Steuert die Funktion **Always-On-Ablaufverfolgung**.

- True (Standard) –Aktiviert die Funktion **Always-On-Ablaufverfolgung**. Beispiel: `CitrixWorkspaceApp.exe EnableTracing=true`.
- False –Deaktiviert die Funktion **Always-On-Ablaufverfolgung**. Beispiel: `CitrixWorkspaceApp.exe EnableTracing=false`.

CLIENT_NAME

Gibt den Namen an, mit dem das Benutzergerät beim Server identifiziert wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- <ClientName> - Gibt den Namen an, mit dem das Benutzergerät beim Server identifiziert wird. Der Standardname lautet %COMPUTERNAME%. Beispiel: `CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%`.

ENABLE_DYNAMIC_CLIENT_NAME

Ermöglicht, dass der Clientname mit dem Computernamen übereinstimmt. Wenn Sie den Computernamen ändern, ändert sich auch der Clientname.

- Yes (Standard) –Erlaubt, dass der Clientname mit dem Computernamen übereinstimmt. Beispiel: `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=Yes`.
- No –Erlaubt nicht, dass der Clientname mit dem Computernamen übereinstimmt. Sie müssen einen Wert für die Eigenschaft `CLIENT_NAME` angeben. Beispiel: `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No`.

Authentifizierungsparameter

ENABLE_SSON

Aktiviert Single Sign-On, wenn die Citrix Workspace-App mit dem Befehl `/includeSSON` installiert wird. Weitere Informationen finden Sie unter Domänen-Passthrough-Authentifizierung.

- Yes (Standard) –Gibt an, dass Single Sign-On aktiviert ist. Beispiel: `CitrixWorkspaceApp.exe /ENABLE_SSON=Yes`.
- No –Gibt an, dass Single Sign-On deaktiviert ist. Beispiel: `CitrixWorkspaceApp.exe /ENABLE_SSON=No`.

ENABLE_KERBEROS

Gibt an, ob die HDX-Engine Kerberos-Authentifizierung verwenden muss. Dies gilt nur, wenn die Single Sign-On-Authentifizierung aktiviert ist. Weitere Informationen finden Sie unter Domänen-Passthrough-Authentifizierung mit Kerberos.

- Yes –Gibt an, dass die HDX-Engine Kerberos-Authentifizierung verwendet. Beispiel: `CitrixWorkspaceApp.exe ENABLE_KERBEROS=Yes`.
- No –Gibt an, dass die HDX-Engine keine Kerberos-Authentifizierung verwendet. Beispiel: `CitrixWorkspaceApp.exe ENABLE_KERBEROS=No`.

Zusätzlich zu den oben genannten Eigenschaften können Sie auch die Store-URL angeben, die mit der Citrix Workspace-App verwendet wird. Sie können bis zu 10 Stores hinzufügen. Verwenden Sie dazu die folgende Eigenschaft:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[
On, Off]; [storedescription]"
```

Werte:

- x –Ganzzahlen von 0 bis 9 werden verwendet, um einen Store zu identifizieren.
- storename –Name des Stores. Dieser Wert muss mit dem auf dem StoreFront-Server konfigurierten Namen übereinstimmen.
- servername.domain –Vollqualifizierter Domänenname des Servers, der den Store hostet.
- IISLocation –Pfad zum Store in IIS. Die Store-URL muss mit der URL in der StoreFront-Provisioningdatei übereinstimmen. Die Store-URL hat das folgende Format: `/Citrix/store/discovery`. Um die URL zu erhalten, exportieren Sie eine Provisioningdatei von StoreFront, öffnen Sie die Datei im Editor und kopieren Sie die URL aus dem Element **Address**.
- [On, Off] –Die Option **Off** ermöglicht die Bereitstellung deaktivierter Stores. So können Benutzer entscheiden, ob sie darauf zugreifen oder nicht. Wenn der Status des Stores nicht angegeben ist, ist die Standardeinstellung **On**.
- storedescription - Beschreibung des Stores, z. B. `HR App Store`.

Beispiele für eine Installation über die Befehlszeile

Angeben der Citrix Gateway Store-URL:

```
CitrixWorkspaceApp.exe STORE0=HRStore;https://ag.mycompany.com#
Storename;On;Store
```

Dabei gibt *Storename* den Namen des Stores an, der konfiguriert werden muss.

> **Hinweis:**
>
> - Die mit dieser Methode konfigurierte Citrix Gateway Store-URL unterstützt keine PNA-Dienste-Sites, die Citrix Gateway verwenden.
> - Beim Konfigurieren mehrerer Stores muss die Citrix Gateway-Store-URL der erste Eintrag in der Liste sein. Die Konfiguration von Citrix Gateway-Store-URLs ist auf 1 beschränkt.

Installieren aller Komponenten ohne Benutzereingriffe und Angeben von zwei Anwendungsstores:

```
CitrixWorkspaceApp.exe /silent
STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;
HR App Store"
STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/
discovery;on;Backup HR App Store"
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> - Für eine erfolgreiche Passthrough-Authentifizierung ist es zwingend erforderlich, `/discovery` in die Store-URL aufzunehmen.
> - Die Citrix Gateway-Store-URL muss der erste Eintrag in der Liste der konfigurierten Store-URLs sein.

Deinstallieren

Verwenden des Windows-basierten Deinstallationsprogramms:

Sie können die Citrix Workspace-App für Windows mit dem Windows-Hilfsprogramm ‘‘Programme und Funktionen’’(Programme hinzufügen/entfernen) deinstallieren.

> **Hinweis:**
>
> Sie werden aufgefordert, das Citrix HDX RTME-Paket zu deinstallieren, bevor Sie mit der Installation der Citrix Workspace-App für Windows fortfahren. Klicken Sie auf OK, um mit der Deinstallation fortzufahren.

Installieren über die Befehlszeilenoberfläche:

Sie können die Citrix Workspace-App für Windows mit dem folgenden Befehl über die Befehlszeile deinstallieren.

```
CitrixWorkspaceApp.exe /uninstall
```

Führen Sie für die unbeaufsichtigte Deinstallation der Citrix Workspace-App für Windows den folgenden Befehl aus:

```
CitrixWorkspaceApp.exe /silent /uninstall
```

> **Hinweis:**
>
> - Die Registrierungsschlüssel, die von receiver.adm/receiver.adml oder receiver.admx erstellt wurden, verbleiben nach der Deinstallation.
> - Wenn Sie nach der Deinstallation Einträge im Registrierungs-Editor finden, löschen Sie diese manuell.

Bereitstellen

October 26, 2023

Sie können die Citrix Workspace-App mit den folgenden Methoden bereitstellen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Verwenden Sie Active Directory und Beispielstartskripts, um die Citrix Workspace-App für Windows bereitzustellen. Weitere Informationen über Active Directory finden Sie unter Verwenden von Active Directory und Beispielskripts.
- Verwenden von Workspace für Web, um sicherzustellen, dass Benutzer die Citrix Workspace-App für Windows installiert haben, bevor sie eine Anwendung in einem Browser starten. Weitere Informationen finden Sie unter Verwenden von Workspace für Web.
- Verwenden Sie ein ESD-Tool zur elektronischen Softwareverteilung wie Microsoft System Center Configuration Manager 2012 R2. Weitere Informationen finden Sie unter Verwenden von System Center Configuration Manager 2012 R2.

Verwenden von Active Directory und Beispielskripts

Sie können Active Directory-Gruppenrichtlinienskripts verwenden, um die Citrix Workspace-App für Windows auf Systemen basierend auf der Active Directory-Organisationsstruktur bereitzustellen. Citrix empfiehlt, die Skripts zu verwenden, anstatt die MSI-Dateien zu extrahieren. Allgemeine Informationen über Startskripts finden Sie in der Dokumentation von Microsoft.

Verwenden von Skripts mit Active Directory:

1. Erstellen Sie die Organisationseinheit (OU) für jedes Skript.
2. Erstellen Sie eine Gruppenrichtlinienobjekt (GPO) für die neu erstellte OU.

Skripts bearbeiten

Bearbeiten Sie die Skripts mit den folgenden Parametern im Kopfbereich jeder Datei:

- **Current Version of package** - Die angegebene Versionsnummer wird validiert und die Bereitstellung wird fortgesetzt, wenn die Nummer nicht vorhanden ist. Beispiel: set DesiredVersion= 3.3.0.XXXX, um genau der angegebenen Version zu entsprechen. Wenn Sie eine Teilversion angeben, beispielsweise 3.3.0, wird eine Übereinstimmung mit allen Versionen erkannt, die dieses Präfix haben (3.3.0.1111, 3.3.0.7777 usw.).
- **Package Location/Deployment directory** - Hiermit geben Sie die Netzwerkfreigabe an, die die Pakete enthält. Die Freigabe wird nicht durch das Skript authentifiziert. Für die Freigabe muss die Leseberechtigung auf JEDER eingestellt sein.
- **Script Logging Directory** - Hiermit geben Sie die Netzwerkfreigabe an, in die die Installationsprotokolle kopiert werden. Die Freigabe wird nicht durch das Skript authentifiziert. Für die Freigabe muss Schreib- und Leseberechtigung für JEDER eingestellt sein.
- **Package Installer Command Line Options** - Diese Befehlszeilenoptionen werden an den Installer weitergeleitet. Weitere Informationen zur Befehlszeilensyntax finden Sie unter Verwenden von Befehlszeilenparametern.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Skripts

Der Installer von Citrix Workspace-App bietet Beispiele für Pro-Computer- und Pro-Benutzer-Skripts, um die Citrix Workspace-App zu installieren und zu deinstallieren. Sie finden die Skripts auf der Download-Seite der Citrix Workspace-App für Windows.

Bereitstellungstyp	Bereitstellen	Entfernen
Pro Computer	CheckAndDeployWorkspacePerMachineStartupScript.bat	CheckAndRemoveWorkspacePerMachineSta
Pro Benutzer	CheckAndDeployWorkspacePerUserLogonScript.bat	CheckAndRemoveWorkspacePerUserLogonS

Hinzufügen von Startskripts:

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Wählen Sie **Computerkonfiguration** oder **Benutzerkonfiguration** > **Richtlinien** > **Windows-Einstellungen** > **Skripts**.
3. Wählen Sie im rechten Bereich der Gruppenrichtlinien-Verwaltungskonsole **Anmelden**.
4. Wählen Sie **Dateien anzeigen** und kopieren Sie das entsprechende Skript in den angezeigten Ordner.
5. Schließen Sie das Dialogfeld.
6. Klicken Sie in **Eigenschaften** auf **Hinzufügen** und **Durchsuchen**, um das soeben erstellte Skript zu finden und hinzuzufügen.

Bereitstellen der Citrix Workspace-App für Windows:

1. Verschieben Sie die Benutzergeräte, für die Sie diese Art der Bereitstellung verwenden möchten, in die von Ihnen erstellte Organisationseinheit (OU).
2. Starten Sie das Benutzergerät neu und melden Sie sich an.
3. Stellen Sie sicher, dass das neu installierte Paket unter **Programme und Funktionen** aufgeführt ist.

Entfernen der Citrix Workspace-App für Windows:

1. Verschieben Sie die Benutzergeräte, die entfernt werden sollen, in die von Ihnen erstellte Organisationseinheit (OU).
2. Starten Sie das Benutzergerät neu und melden Sie sich an.
3. Stellen Sie sicher, dass das neu installierte Paket nicht unter Programme und Funktionen aufgeführt ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verwenden von Workspace für Web

Sie können die Citrix Workspace-App für Windows über Workspace für Web bereitstellen, um sicherzustellen, dass die App vor der Herstellung einer Verbindung zu einer Anwendung über den Browser auf den Benutzergeräten installiert wird. Mit Workspace für Web können Sie über eine Webseite auf StoreFront-Stores zugreifen. Wenn Workspace für Web erkennt, dass ein Benutzer keine kompatible Version der Citrix Workspace-App für Windows hat, wird der Benutzer zum Download und zur Installation der Citrix Workspace-App für Windows aufgefordert.

Die e-mail-basierte Kontenermittlung wird nicht unterstützt, wenn die Citrix Workspace-App für Windows von Workspace für Web bereitgestellt wird. Wenn die e-mail-basierte Kontenermittlung konfiguriert ist und ein Erstbenutzer die Citrix Workspace-App für Windows von Citrix.com installiert, fordert die App den Benutzer zur Eingabe einer E-Mail- oder Serveradresse auf. Bei der Eingabe einer E-Mail-Adresse wird eine Fehlermeldung "Sie können kein Konto mit der E-Mail-Adresse hinzufügen" angezeigt.

Verwenden Sie die folgende Konfiguration, um nur zur Eingabe der Serveradresse aufzufordern.

1. Laden Sie `CitrixWorkspaceApp.exe` auf den lokalen Computer herunter.
2. Benennen Sie `CitrixWorkspaceApp.exe` in `CitrixWorkspaceAppWeb.exe` um.
3. Stellen Sie die umbenannte ausführbare Datei mit der normalen Bereitstellungsmethode bereit. Wenn Sie StoreFront verwenden, finden Sie weitere Informationen unter Konfigurieren von Workspace für Web mit Konfigurationsdateien in der StoreFront-Dokumentation.

Verwenden von System Center Configuration Manager 2012 R2

Sie können die Citrix Workspace-App über Microsoft System Center Configuration Manager (SCCM) bereitstellen.

> **Hinweis:**
>
> Die SCCM-Bereitstellung wird nur von Citrix Receiver für Windows ab Version 4.5 und höher unterstützt.

Die Bereitstellung der Citrix Workspace-App für Windows mit SCCM umfasst vier Teilschritte:

1. Hinzufügen der Citrix Workspace-App zur SCCM-Bereitstellung
2. Hinzufügen von Verteilungspunkten
3. Bereitstellen der Citrix Workspace-App im Softwarecenter
4. Erstellen von Gerätesammlungen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hinzufügen der Citrix Workspace-App zur SCCM-Bereitstellung

1. Kopieren Sie die heruntergeladene Citrix Workspace-App-Software in einen Ordner auf dem Configuration Manager-Server und starten Sie die Configuration Manager-Konsole.
2. Wählen Sie **Softwarebibliothek** > **Anwendungsverwaltung**. Klicken Sie mit der rechten Maustaste auf **Anwendung** und klicken Sie auf **Anwendung erstellen**.
   Der Assistent zum Erstellen von Anwendungen wird angezeigt.
3. Aktivieren Sie im Bereich **Allgemein** die Option **Anwendungsinformationen manuell angeben** und klicken Sie auf **Weiter**.
4. Im Bereich **Allgemeine Informationen** geben Sie Informationen zur Anwendung wie Name, Hersteller und Softwareversion ein.
5. Im Assistenten zum Anwendungskatalog geben Sie zusätzliche Informationen wie Sprache, Anwendungsname und Benutzerkategorie ein. Klicken Sie dann auf **Weiter**.

   > **Hinweis:**
   >
   > Benutzer können die Informationen sehen, die Sie hier angeben.

6. Im Bereich **Bereitstellungstyp** klicken Sie auf **Hinzufügen**, um den Bereitstellungstyp für die Citrix Workspace-App zu konfigurieren.

   Der Assistent zum Erstellen von Bereitstellungstypen wird angezeigt.
7. Bereich **Allgemein**: Wählen Sie Windows Installer (*.msi-Datei) als Bereitstellungstyp. Aktivieren Sie **Informationen zum Bereitstellungstyp manuell angeben** und klicken Sie auf **Weiter**.
8. Bereich **Allgemeine Informationen**: Legen Sie den Bereitstellungstyp fest (z. B.: Workspace-Bereitstellung) und klicken Sie auf **Weiter**.
9. Bereich **Inhalt**:

   a) Geben Sie den Pfad zum Verzeichnis mit der Citrix Workspace-App-Setupdatei an. Beispiel: Tools auf dem SCCM-Server.
   b) Geben Sie das **Installationsprogramm** an. Zur Auswahl stehen folgende Optionen:
      - `CitrixWorkspaceApp.exe /silent` für die standardmäßige automatische Installation.
      - `CitrixWorkspaceApp.exe /silent /includeSSON` zum Aktivieren von Domänen-Passthrough.
      - `CitrixWorkspaceApp.exe /silent SELFSERVICEMODE=false` zum Installieren der Citrix Workspace-App im Modus ohne Self-Service.
   c) Geben Sie für **Deinstallationsprogramm** den Befehl `CitrixWorkspaceApp.exe /uninstall` ein (zum Aktivieren der Deinstallation über SCCM).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

10. Bereich **Erkennungsmethode**: Wählen Sie **Regeln konfigurieren, um zu erkennen, ob dieser Bereitstellungstyp vorhanden ist**, und klicken Sie auf **Klausel hinzufügen**.
    Das Dialogfeld "Erkennungsregel"wird angezeigt.

    - Wählen Sie als **Einstellungstyp** die Option "Dateisystem".
    - Wählen Sie folgende Einstellungen unter **Geben Sie die Datei oder den Ordner an, um diese Anwendung zu erkennen**:
      - **Typ:** Wählen Sie im Dropdownmenü die Option **Datei**.
      - **Pfad**: `%ProgramFiles(x86)%\\Citrix\\ICA Client\\Receiver\`
      - **Datei- oder Ordnername**: `receiver.exe`
      - **Eigenschaft**: Wählen Sie im Dropdownmenü die Option **Version**.
      - **Operator**: Wählen Sie im Dropdownmenü **größer oder gleich**.
      - **Wert**: Geben Sie die Versionsnummer der Citrix Workspace-App ein, die Sie bereitstellen möchten.

    > **Hinweis:**
    >
    > Diese Regelkombination gilt auch für Upgrades der Citrix Workspace-App für Windows.

11. Wählen Sie im Bereich **Benutzererfahrung** folgende Einstellungen:

    - **Installationsverhalten**: Option "Für System installieren"
    - **Anmeldeanforderung**: Option "Unabhängig von Benutzeranmeldung"
    - **Sichtbarkeit des Installationsprogramms:** Normal
      Klicken Sie auf "Weiter".

    > **Hinweis:**
    >
    > Legen Sie keine Anforderungen und Abhängigkeiten für diesen Bereitstellungstyp fest.

12. Prüfen Sie im Bereich **Zusammenfassung** die gewählten Einstellungen für diesen Bereitstellungstyp. Klicken Sie auf **Weiter**.

    Es wird dann ein Erfolg gemeldet.

13. Im Abschlussfensterwird unter **Bereitstellungstypen** ein neuer Bereitstellungstyp (Workspace-Bereitstellung) aufgelistet.

14. Klicken Sie auf **Weiter** und klicken Sie auf **Schließen**.

Hinzufügen von Verteilungspunkten

1. Klicken Sie in der Configuration Manager-Konsole mit der rechten Maustaste auf "Citrix Workspace-App"und wählen Sie **Inhalt verteilen**.

   Der Assistent für die Verteilung von Inhalt wird angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Klicken Sie im Bereich "Inhaltsverteilung"auf **Hinzufügen > Verteilungspunkte**.

   Das Dialogfeld "Verteilungspunkte hinzufügen"wird angezeigt.

3. Navigieren Sie zum SCCM-Server, auf dem der Inhalt verfügbar ist, und klicken Sie auf **OK**.

   Im Abschlussfenster wird eine Erfolgsmeldung angezeigt.

4. Klicken Sie auf **Schließen**.

Bereitstellen der Citrix Workspace-App im Softwarecenter

1. Klicken Sie mit der rechten Maustaste in der Configuration Manager-Konsole auf "Citrix Workspace-App"und wählen Sie **Bereitstellen**.

   Der Assistent zur Softwarebereitstellung wird angezeigt.

2. Wählen Sie **Durchsuchen** für die Sammlung (Gerätesammlung oder Benutzersammlung), wo die Anwendung bereitgestellt werden soll, und klicken Sie auf **Weiter**.

3. Wählen Sie im Bereich **Bereitstellungseinstellungen** für **Aktion** die Einstellung "Installation" und für **Zweck** die Option "Erforderlich". Dies aktiviert die unbeaufsichtigte Installation. Klicken Sie auf **Weiter**.

4. Legen Sie im Bereich **Zeitplanung** den Zeitplan für die Bereitstellung der Software auf den Zielgeräten fest.

5. Legen Sie im Bereich **Benutzererfahrung** das Verhalten für **Benutzerbenachrichtigungen** fest: Wählen Sie **Änderungen zum Stichtag oder während eines Wartungsfensters ausführen (erfordert Neustart)** und klicken Sie auf **Weiter**, um den Assistenten zur Softwarebereitstellung zu schließen.

Im Abschlussfenster wird eine Erfolgsmeldung angezeigt.

Starten Sie die Ziel-Endpunktgeräte neu (nur für die sofortige Installation erforderlich).

Auf Endpunktgeräten wird die Citrix Workspace-App im Softwarecenter unter **Verfügbare Software** angezeigt. Die Installation wird automatisch auf der Basis des konfigurierten Zeitplans ausgelöst. Alternativ können Sie auch einen späteren Termin festlegen oder die Software bei Bedarf installieren. Der Installationsstatus wird nach dem Start der Installation im Softwarecenter angezeigt.

Erstellen von Gerätesammlungen

1. Starten Sie die Configuration Manager-Konsole und klicken Sie auf **Bestand und Kompatibilität** > **Überblick** > **Geräte**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Klicken Sie mit der rechten Maustaste auf **Gerätesammlungen** und wählen Sie **Gerätesammlung erstellen**.

   Der Assistent zum Erstellen von Gerätesammlungen wird angezeigt.

3. Geben Sie im Bereich **Allgemein** den Namen für das Gerät ein und klicken Sie auf **Durchsuchen**, um eine begrenzte Sammlung auszuwählen.

   Dies bestimmt den Geltungsbereich von Geräten. Es kann eine der von SCCM erstellten Standard-Gerätesammlungen verwendet werden.
   Klicken Sie auf **Weiter**.

4. Klicken Sie im Bereich "Mitgliedschaftsregeln"auf **Regel hinzufügen**. Diese wird dann zum Filtern der Geräte verwendet.

   Der Assistent zum Erstellen direkter Mitgliedschaftsregeln wird angezeigt.

   - Wählen Sie im Bereich **Ressourcen** suchen einen Attributnamen, der den gesuchten Geräten entspricht, und legen Sie einen Wert für den Attributnamen fest, der bei der Geräteauswahl verwendet werden soll.

5. Klicken Sie auf **Weiter**. Wählen Sie im Bereich "Ressourcen auswählen"die Geräte aus, die in der Gerätesammlung enthalten sein müssen.

   Im Abschlussfenster wird eine Erfolgsmeldung angezeigt.

6. Klicken Sie auf **Schließen**.

7. Im Bereich "Mitgliedschaftsregeln"wird eine neue Regel aufgelistet. Klicken Sie auf "Weiter".

8. Im Abschlussfenster wird eine Erfolgsmeldung angezeigt. Klicken Sie auf **Schließen**, um den Assistenten zum Erstellen von Gerätesammlungen schließen.

   Die neue Gerätesammlung ist nun unter **Gerätesammlungen** aufgeführt. Beim Navigieren im Assistenten zur Softwarebereitstellung wird die neue Gerätesammlung in den Gerätesammlungen angezeigt.

> **Hinweis:**
>
> Wenn Sie das Attribut **MSIRESTARTMANAGERCONTROL** auf **False** setzen, kann die Citrix Workspace-App für Windows mit SCCM möglicherweise nicht bereitgestellt werden.
> Gemäß unserer Analyse wird dieses Problem nicht durch die Citrix Workspace-App für Windows verursacht. Ein erneuter Versuch kann zudem zum Erfolg der Bereitstellung führen.

Aktualisieren

April 22, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Manuelle Aktualisierung

Wenn Sie die Citrix Workspace-App für Windows bereits installiert haben, laden Sie die neueste Version der App von der Citrix Downloadseite herunter und installieren Sie sie.

Automatisches Update

Ab Version 1912 Cumulative Update 4 (CU4) haben die Citrix Workspace Update-Protokolle neue Pfade. Die Workspace Update-Protokolle sind in C:\Program Files(x86)\Citrix\Logs bei maschinenweiten Updates. Bei benutzerweiten Updates sind sie im temporären Ordner des Benutzers.

Wenn eine neue Version der Citrix Workspace-App veröffentlicht wird, sendet Citrix das Update an das System, auf dem die Citrix Workspace-App installiert ist.

> **Hinweis:**
>
> - Wenn Sie einen ausgehenden Proxy mit SSL-Interception konfiguriert haben, fügen Sie eine Ausnahme zum Workspace-Server für automatische Updates `https://downloadplugins.citrix.com/` hinzu, damit Sie Updates von Citrix erhalten.
> - Automatische Updates sind für Versionen vor Citrix Workspace-App 2104 und Citrix Workspace-App 1912 LTSR CU4 nicht verfügbar.
> - Wenn Sie einen Outbound-Proxy mit SSL-Interception konfiguriert haben, fügen Sie eine Ausnahme zum Workspace-Signaturdienst für automatische Updates `https://citrixupdates.cloud.com/` und zum Downloadspeicherort `https://downloadplugins.citrix.com/` hinzu, damit Sie Updates von Citrix erhalten.
> - Ihr System muss über eine Internetverbindung verfügen, um Updates zu erhalten.
> - Standardmäßig sind Citrix Workspace-Updates auf dem VDA deaktiviert. Dies umfasst RDS-Server mit mehreren Benutzern, VDI- und Maschinen mit Remote-PC-Zugriff.
> - Citrix Workspace-Updates sind auf Maschinen deaktiviert, auf denen Desktop Lock installiert ist.
> - Workspace für Web-Benutzer können die StoreFront-Richtlinie nicht automatisch herunterladen.
> - Citrix Workspace-Updates können auf LTSR-Updates beschränkt werden.
> - Citrix HDX RTME für Windows ist in Citrix Workspace-Updates enthalten. Sie werden über verfügbare HDX RTME-Updates für das LTSR und das aktuelle Release der Citrix Workspace-App benachrichtigt.

Erweiterte Konfiguration für automatische Updates (Citrix Workspace-Updates)

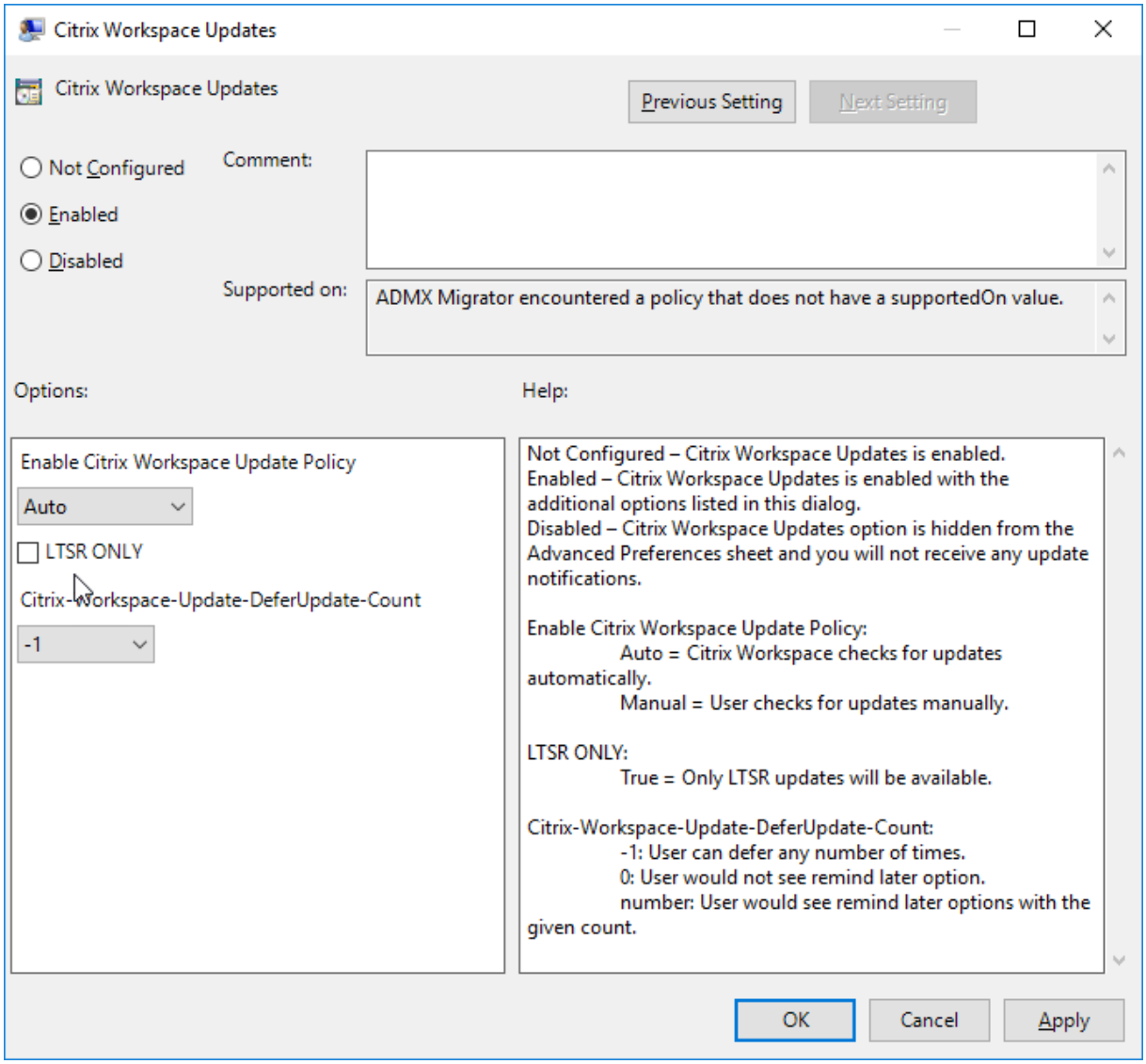
Sie können Citrix Workspace-Updates mit den folgenden Methoden konfigurieren:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Administrative Gruppenrichtlinienobjektvorlage
2. Befehlszeilenoberfläche
3. Grafische Benutzeroberfläche
4. StoreFront

Konfigurieren von Citrix Workspace-Updates mit der administrativen Gruppenrichtlinienobjektvorlage

Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App, indem Sie gpedit.msc ausführen und am Knoten "Computer Configuration"zu **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Workspace Updates** gehen.



1. **Updates aktivieren oder deaktivieren:** Wählen Sie **Aktiviert** oder **Deaktiviert** aus, um Workspace-Updates zu aktivieren oder zu deaktivieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Wenn Sie **Deaktiviert** auswählen, werden Sie nicht über neue Updates informiert. Dadurch wird auch die Option Citrix Workspace-Updates auf der Seite Erweiterte Einstellungen ausgeblendet.

2. **Updatebenachrichtigung:** Wenn ein Update verfügbar ist, können Sie wählen, ob Sie automatisch benachrichtigt werden möchten oder manuell danach suchen. Nachdem Sie Workspace-Updates aktiviert haben, wählen Sie eine der folgenden Optionen aus der Dropdown-Liste **Citrix Workspace-Updaterichtlinie aktivieren**:

    - Auto: Sie werden benachrichtigt, wenn ein Update zur Verfügung steht (Standardeinstellung).
    - Manual - Sie werden nicht benachrichtigt, wenn ein Update verfügbar ist. Suchen Sie manuell nach Updates.

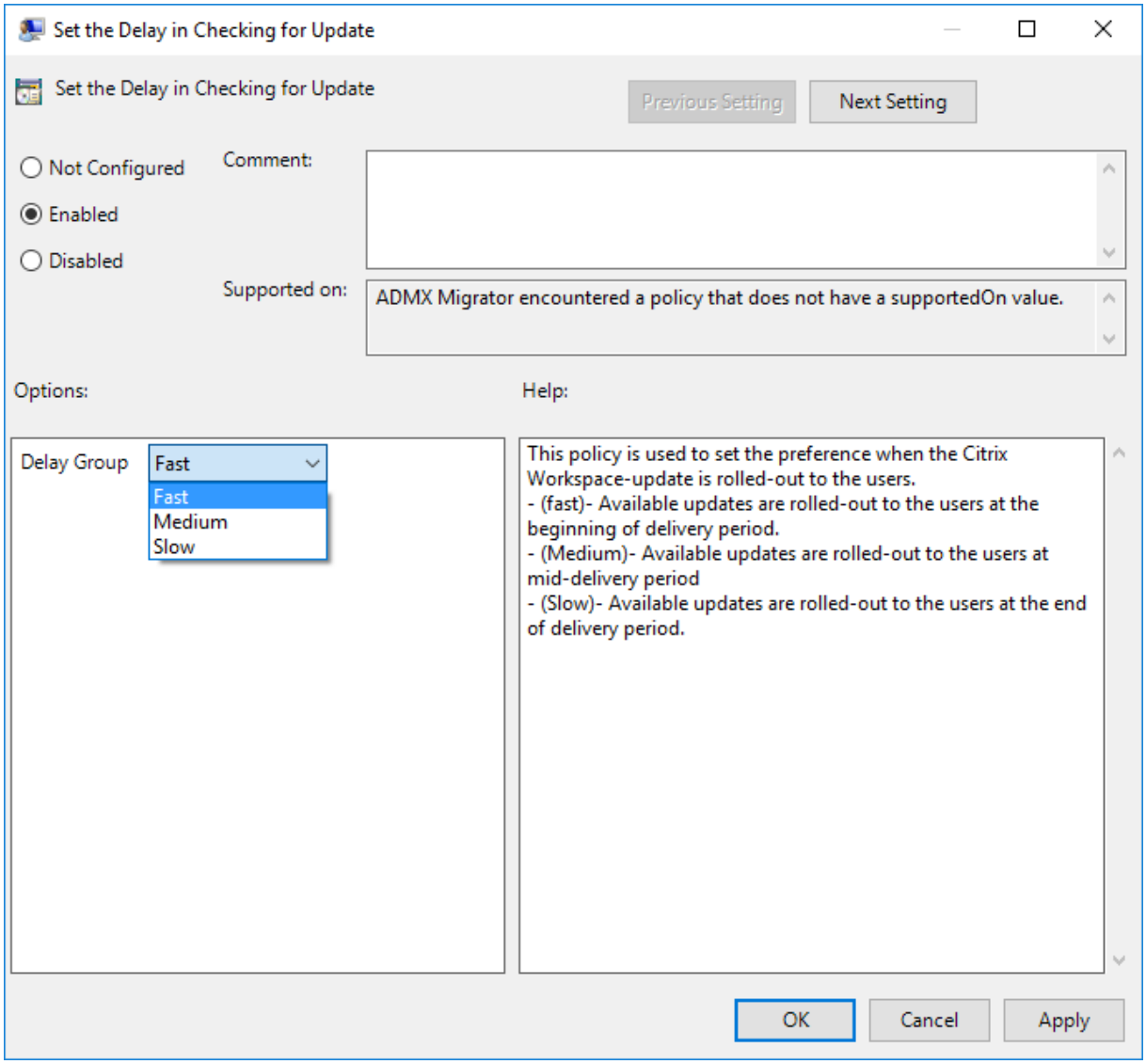
3. Aktivieren Sie **Nur LTSR**, um Updates nur für LTSR zu erhalten.
4. Wählen Sie im Dropdownmenü **Citrix-Workspace-Update-DeferUpdate-Count** einen Wert zwischen -1 und 30 aus:

    - -1 - Erlaubt das Ignorieren der Benachrichtigungen beliebig oft (Standard).
    - 0 - Sie erhalten nur eine Benachrichtigung für das Update.

Konfigurieren der Verzögerung bei der Suche nach Updates Wenn eine neue Version der Citrix Workspace-App verfügbar ist, stellt Citrix das Update während eines bestimmten Bereitstellungszeitraums bereit. Mit dieser Eigenschaft können Sie steuern, in welcher Phase des Bereitstellungszeitraums Sie das Update erhalten.

Führen Sie zum Konfigurieren des Bereitstellungszeitraums `gpedit.msc` aus, um die administrative Vorlage für Gruppenrichtlinienobjekte zu starten. Navigieren Sie unter "Computerkonfiguration"zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Verzögerung für Prüfung auf Updates festlegen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Wählen Sie **Aktiviert** und anschließend im Dropdownmenü neben **Für Gruppe aufschieben** eine der folgenden Optionen:

- Fast –Das Rollout des Updates erfolgt zu Beginn des Bereitstellungszeitraums.
- Medium –Das Rollout des Updates erfolgt in der Mitte des Bereitstellungszeitraums.
- Slow –Das Rollout des Updates erfolgt am Ende des Bereitstellungszeitraums.

> **Hinweis:**
>
> Wenn Sie **Deaktiviert** auswählen, werden Sie nicht über die verfügbaren Updates informiert. Dadurch wird auch die Option Citrix Workspace-Updates auf der Seite Erweiterte Einstellungen ausgeblendet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfigurieren von Citrix Workspace-Updates über die Befehlszeilenschnittstelle

Durch Angeben von Befehlszeilenparametern während der Installation der Citrix Workspace-App:

Sie können Workspace-Updates konfigurieren, indem Sie während der Installation der Citrix Workspace-App Befehlszeilenparameter angeben. Weitere Informationen finden Sie unter Installationsparameter.

Mit Befehlszeilenparametern nach der Installation der Citrix Workspace-App:

Citrix Workspace-Updates können auch nach der Installation der Citrix Workspace-App für Windows konfiguriert werden. Navigieren Sie mit der Windows-Befehlszeile zum Speicherort von CitrixReceiverUpdater.exe.

Normalerweise befindet sich CitrixWorkspaceUpdater.exe unter `CitrixWorkspaceInstallLocation\Citrix\Ica Client\Receiver`. Sie können diese Binärdatei zusammen mit den im Abschnitt Installationsparameter aufgeführten Befehlszeilenparametern ausführen.

Beispiel:

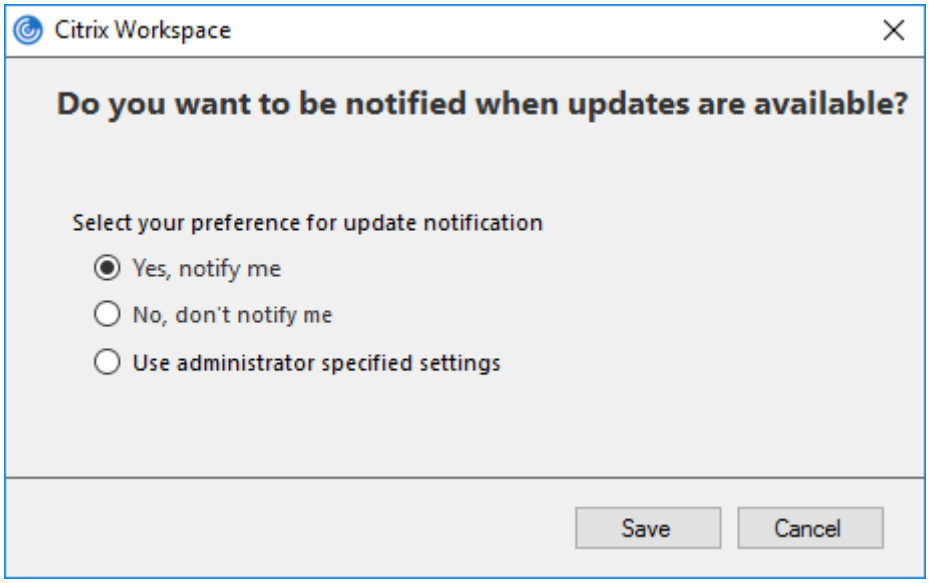
```
CitrixReceiverUpdater.exe /AutoUpdateCheck=auto /AutoUpdateStream=
Current /DeferUpdateCount=-1 /AURolloutPriority=fast
```

> **Hinweis:**
>
> `/AutoUpdateCheck` ist ein obligatorischer Parameter, den Sie festlegen müssen, um andere Parameter wie `/AutoUpdateStream`, `/DeferUpdateCount` und `/AURolloutPriority` zu konfigurieren.

Konfigurieren von Citrix Workspace-Updates über die grafische Benutzeroberfläche

Ein Benutzer kann die Einstellung für Citrix Workspace-Updates im Dialogfeld Erweiterte Einstellungen außer Kraft setzen. Diese Konfiguration gilt pro Benutzer und die Einstellungen werden nur für den aktuellen Benutzer angewendet. Klicken Sie mit der rechten Maustaste im Infobereich auf das Citrix Workspace-App-Symbol. Wählen Sie **Erweiterte Einstellungen** > **Citrix Workspace-Updates**. Wählen Sie die Benachrichtigungseinstellung aus und klicken Sie auf **Speichern**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Hinweis:**
>
> Sie können die über das Citrix Workspace-App-Symbol im Infobereich verfügbare Seite "Erweiterte Einstellungen"ganz oder teilweise ausblenden. Weitere Informationen finden Sie unter Erweiterte Einstellungen.

Konfigurieren von Citrix Workspace-Updates mit StoreFront

1. Öffnen Sie die Datei `web.config` mit einem Text-Editor. Die Datei ist normalerweise im Verzeichnis `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Suchen Sie das Benutzerkonto-Element in der Datei. Der Kontoname Ihrer Bereitstellung ist "Store".

   Beispiel: `<account id=... name="Store">`

   Vor dem Tag `</account>` navigieren Sie zu den Eigenschaften des Benutzerkontos:

   ```
   <properties>
          <clear/>
    </properties>
    <!--NeedCopy-->
   ```

3. Fügen Sie das Tag für automatische Updates nach dem Tag *<clear />* ein.

   ```
   <account>

       <clear />

       <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
           F84Store"

   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
7         description="" published="true" updaterType="Citrix"
              remoteAccessType="None">
8
9         <annotatedServices>
10
11          <clear />
12
13          <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
14
15            <metadata>
16
17              <plugins>
18
19                <clear />
20
21              </plugins>
22
23              <trustSettings>
24
25                <clear />
26
27              </trustSettings>
28
29              <properties>
30
31                <property name="Auto-Update-Check" value="auto" />
32
33                <property name="Auto-Update-DeferUpdate-Count" value
                      ="1" />
34
35                      <property name="Auto-Update-LTSR-Only" value
                          ="FALSE" />
36
37                <property name="Auto-Update-Rollout-Priority" value=
                      "fast" />
38
39                   </properties>
40
41            </metadata>
42
43          </annotatedServiceRecord>
44
45        </annotatedServices>
46
47        <metadata>
48
49          <plugins>
50
51            <clear />
52
53          </plugins>
54
55          <trustSettings>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
56
57            <clear />
58
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
70
71  <!--NeedCopy-->
```

Nachfolgend sind die Bedeutungen der Eigenschaften und ihre möglichen Werte aufgeführt:

- **Auto-update-Check:** Gibt an, dass die Citrix Workspace-App ein Update automatisch erkennt, wenn es verfügbar ist.
- **Auto-update-LTSR-only:** Gibt an, dass das Release-Update nur für LTSR gilt.
- **Auto-update-Rollout-Priority:** Gibt den Bereitstellungszeitraum an, in dem Sie das Update erhalten können.
- **Auto-update-DeferUpdate-Count:** Gibt an, wie oft Sie die Benachrichtigungen für die Release-Updates ignorieren können.

Erste Schritte

April 22, 2024

Dies ist ein Referenzdokument, mit dem Sie Ihre Umgebung nach der Installation der Citrix Workspace-App einrichten können.

Voraussetzungen:

Stellen Sie sicher, dass alle im Abschnitt Systemanforderungen aufgeführten Systemanforderungen erfüllt sind.

Bevor Sie die Citrix Workspace-App verwenden, müssen Sie Folgendes konfigurieren:

- Administrative Gruppenrichtlinienobjektvorlage
- StoreFront
- Citrix Gateway Store
- Store-URL zur Citrix Workspace-App hinzufügen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Clientlaufwerkzuordnung
- Domain Name Service-Namensauflösung

Administrative Gruppenrichtlinienobjektvorlage

Citrix empfiehlt Regeln für das Netzwerkrouting, für die Proxyserver und für die vertrauenswürdige Serverkonfiguration, für das Benutzerrouting, für die Remoteclientgeräte und die Benutzererfahrung mit dem Gruppenrichtlinienobjekt "Administrative Vorlagen"zu konfigurieren.
Sie können die Vorlagendateien receiver.admx bzw. receiver.adml für Domänenrichtlinien und lokale Computerrichtlinien verwenden. Importieren Sie die Vorlagendatei für Domänenrichtlinien mit der Gruppenrichtlinien-Verwaltungskonsole. Dies ist besonders nützlich, wenn Sie Citrix Workspace-App-Einstellungen auf mehrere verschiedene Benutzergeräte im Unternehmen anwenden möchten. Wenn Sie nur ein einziges Benutzergerät bearbeiten möchten, importieren Sie die Vorlagendatei mit dem lokalen Gruppenrichtlinien-Editor auf dem Gerät.

Citrix empfiehlt die Verwendung der administrativen Gruppenrichtlinienobjektvorlage von Windows für die Konfiguration der Citrix Workspace-App.

Ab Citrix Receiver für Windows 4.6 befinden sich im Installationsverzeichnis die Dateien `CitrixBase.admx` und `CitrixBase.adml` sowie administrative Vorlagendateien (receiver.adm oder receiver.admx\receiver.adml, je nach Betriebssystem).

> **Hinweis:**
>
> Die ADM-Datei ist nur zur Verwendung mit Windows XP Embedded-Plattformen. Die ADMX/ADML-Dateien sind zur Verwendung mit Windows Vista/Windows Server 2008 und allen höheren Versionen von Windows.

Wenn die Citrix Workspace-App mit dem VDA installiert wird, sind die ADMX/ADML-Dateien im Installationsverzeichnis der Citrix Workspace-App. Beispiel: <Installationsverzeichnis>\Online Plugin\Configuration.

Wird die Citrix Workspace-App ohne den VDA installiert, sind die ADMX/ADML-Dateien normalerweise im Verzeichnis `C:\Program Files\Citrix\ICA Client\Configuration`.

In der Tabelle unten finden Sie Informationen zu den Vorlagendateien der Citrix Workspace-App und deren Speicherorten.

> **Hinweis:**
>
> Citrix empfiehlt, dass Sie die GPO-Vorlagendateien verwenden, die mit der aktuellen Version der Citrix Workspace-App bereitgestellt werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dateityp	Dateispeicherort
receiver.adm	\ICA Client\Configuration
receiver.admx	\ICA Client\Configuration
receiver.adml	\ICA Client\Configuration\[MUIculture]
CitrixBase.admx	\ICA Client\Configuration
CitrixBase.adml	\ICA Client\Configuration\[MUIculture]

Hinweis:

- Wenn CitrixBase.admx\adml nicht dem lokalen Gruppenrichtlinienobjekt hinzugefügt wird, geht möglicherweise die Richtlinie **ICA-Dateisignierung aktivieren** verloren.
- Fügen Sie beim Upgrade der Citrix Workspace-App die neuesten Vorlagendateien dem lokalen Gruppenrichtlinienobjekt wie nachfolgend beschrieben hinzu. Beim Import der aktuellen Dateien werden die vorherigen Einstellungen beibehalten.

Hinzufügen der Vorlagendatei receiver.adm zum lokalen Gruppenrichtlinienobjekt (nur für Windows XP Embedded-Betriebssysteme):

Citrix empfiehlt die Verwendung von CitrixBase.admx und CitrixBase.adml um sicherzustellen, dass die Optionen im Gruppenrichtlinienobjekt-Editor richtig sortiert angezeigt werden.

Sie können ADM-Vorlagendateien zum Konfigurieren von lokalen und domänenbasierten Gruppenrichtlinienobjekten verwenden.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner **Administrative Vorlagen** aus.
3. Klicken Sie im Menü **Aktion** auf **Vorlagen hinzufügen/entfernen.**
4. Wählen Sie **Hinzufügen** aus und navigieren Sie zum Speicherort der Vorlagendatei `\<Installation Directory>\ICA Client\Configuration\receiver.adm`.
5. Klicken Sie auf **Öffnen** um die Vorlage hinzuzufügen, und klicken Sie dann auf "Schließen", um zum Gruppenrichtlinien-Editor zurückzukehren.

   Die Citrix Workspace-App-Vorlagendatei ist im lokalen Gruppenrichtlinienobjektverzeichnis in folgendem Pfad: **Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Workspace**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nachdem die ADM-Vorlagendateien dem lokalen Gruppenrichtlinienobjekt hinzugefügt wurden, wird die folgende Meldung angezeigt:

"Der folgende Eintrag im Abschnitt [strings] ist zu lang und wurde abgeschnitten:
Klicken Sie auf **OK**, um die Nachricht zu ignorieren."

Hinzufügen der Vorlagendateien receiver.admx/adml zum lokalen Gruppenrichtlinienobjekt (höhere Versionen des Windows-Betriebssystems):

Sie können ADM-Vorlagendateien zum Konfigurieren von lokalen und domänenbasierten Gruppenrichtlinienobjekten verwenden. Weitere Informationen zum Verwalten von ADMX-Dateien finden Sie in diesem Microsoft MSDN-Artikel.

Kopieren Sie nach der Installation der Citrix Workspace-App die Vorlagendateien gemäß folgender Tabelle:

Dateityp	Kopieren von	Kopieren nach
receiver.admx	\ICA Client\Configuration\receiver.admx	Nach: %system-root%\policyDefinitions
CitrixBase.admx	\ICA Client\Configuration\CitrixBase.admx	Nach: %system-root%\policyDefinitions
receiver.adml	\ICA Client\Configuration\[MUIculture]\receiver.adml	%systemroot%\policyDefinitions[MUIculture
CitrixBase.adml	\ICA Client\Configuration\[MUIculture]\CitrixBase.adml	%systemroot%\policyDefinitions[MUIculture

> **Hinweis:**
>
> Citrix Workspace-App-Vorlagendateien sind im lokalen Gruppenrichtlinienobjekt unter **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** nur dann verfügbar, wenn Sie die Dateien CitrixBase.admx/CitrixBase.adml dem Ordner `\PolicyDefinitions` hinzufügen.

StoreFront

Citrix StoreFront authentifiziert eine Verbindung mit Citrix Virtual Apps and Desktops, Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) und VDI-in-a-Box. Verfügbare Desktops und Anwendungen werden in Stores enumeriert und aggregiert und Sie greifen darauf über die Citrix Workspace-App zu.

Zusätzlich zu der Konfiguration, die in diesem Abschnitt zusammengefasst ist, müssen Sie außerdem Citrix Gateway konfigurieren, sodass Benutzer sich von außerhalb mit dem internen Netzwerk

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

verbinden können (z. B. Benutzer, die über das Internet oder von Remotestandorten eine Verbindung herstellen).

> **Hinweis:**
>
> Wenn Sie die Option zum Anzeigen aller Stores wählen, wird möglicherweise die alte StoreFront-Benutzeroberfläche angezeigt.

StoreFront konfigurieren:

Installieren und konfigurieren Sie StoreFront, wie in der StoreFront-Dokumentation beschrieben. Die Citrix Workspace-App benötigt eine HTTPS-Verbindung. Wenn der StoreFront-Server für HTTP konfiguriert ist, muss ein Registrierungsschlüssel auf dem Benutzergerät eingestellt werden. Eine Anleitung finden Sie unter Verwenden von Befehlszeilenparametern in der Beschreibung der Eigenschaft **ALLOWADDSTORE**.

> **Hinweis:**
>
> Administratoren, die mehr Kontrolle wünschen, können mit einer von Citrix bereitgestellten Vorlage eine Downloadsite für die Citrix Workspace-App für Windows erstellen.

Citrix Gateway Store

Hinzufügen oder Festlegen eines Citrix Gateways mit der administrativen Gruppenrichtlinienobjektvorlage:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Klassische administrative Vorlagen (ADM)** > **Citrix Komponenten** > **Citrix Workspace** > **StoreFront**.
3. Wählen Sie **Citrix Gateway-URL\StoreFront-Kontenliste**.
4. Bearbeiten Sie die Einstellungen.
    - Storename: der angezeigte Name des Stores
    - Store-URL: die URL des Stores
    - #Storename: der Name des Stores hinter dem Citrix Gateway
    - Storeaktivierungszustand: der Zustand des Stores, Ein/Aus
    - Storebeschreibung: eine Beschreibung des Stores
5. Fügen Sie die Citrix Gateway-URL hinzu oder geben Sie sie ein. Geben Sie den Namen der URL durch Semikolon getrennt ein:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Beispiel: `CitrixWorkspaceApp.exe STORE0= HRStore;https://ag.mycompany.com#Storename;On;Store`
Wobei #Store name der Name des Stores hinter dem Citrix Gateway ist.

Wird in früheren Versionen ein Konto über die Richtlinie **Citrix Gateway-URL\StoreFront-Kontenliste** dem Gruppenrichtlinienobjekt hinzugefügt oder daraus entfernt, muss Citrix Receiver zurückgesetzt werden, damit die Änderungen in Kraft treten.

Ab Version 1808 werden alle Änderungen an der Richtlinie **Citrix Gateway-URL\StoreFront-Kontenliste** in einer Sitzung angewendet, wenn Sie die Citrix Workspace-App neu starten. Ein Reset ist nicht erforderlich.

> **Hinweis:**
>
> Das Zurücksetzen der Citrix Workspace-App ist bei der Neuinstallationen der Citrix Workspace-App Version 1808 und höher nicht erforderlich. Bei Upgrades auf Version 1808 und höher setzen Sie die Citrix Workspace-App zurück, damit die Änderungen wirksam werden.

Einschränkungen:

- Die Citrix Gateway-URL muss als Erste aufgeführt werden, gefolgt von der/den StoreFront-URL(s).
- Mehrere Citrix Gateway-URLs werden nicht unterstützt.
- Eine mit dieser Methode konfigurierte Citrix Gateway-URL unterstützt keine PNA-Dienste-Site hinter Citrix Gateway.

Wiederverbindung über Workspace Control verwalten

Mit Workspace Control folgen Anwendungen dem Benutzer, wenn er das Gerät wechselt. So können etwa Krankenhausärzte von einer Arbeitsstation zu einer anderen wechseln, ohne ihre Anwendungen auf jedem einzelnen Gerät neu starten zu müssen. In der Citrix Workspace-App können Sie Workspace Control auf Clientgeräten durch Ändern der Registrierung verwalten. Für domänengebundene Clientgeräte können Sie dazu auch die Gruppenrichtlinie verwenden.

> **Achtung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Erstellen Sie **WSCReconnectModeUser** und ändern Sie den vorhandenen Registrierungsschlüssel **WSCReconnectMode** im Masterdesktopimage oder auf dem Citrix Virtual Apps-Server. Der veröffentlichte Desktop kann das Verhalten der Citrix Workspace-App ändern.

WSCReconnectMode-Schlüsseleinstellungen für die Citrix Workspace-App:

- 0 = keine Wiederverbindung mit vorhandenen Sitzungen
- 1 = Wiederverbindung bei Anwendungsstart
- 2 = Wiederverbindung bei Anwendungsaktualisierung
- 3 = Wiederverbindung bei Anwendungsstart oder Anwendungsaktualisierung
- 4 = Wiederverbindung beim Öffnen der Citrix Workspace-Benutzeroberfläche
- 8 = Wiederverbindung beim Anmelden an Windows
- 11 = Kombination von 3 und 8

Deaktivieren von Workspace Control für die Citrix Workspace-App Erstellen Sie den folgenden Schlüssel, um Workspace Control zu deaktivieren:

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle` (64 Bit)

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\\Dazzle` (32 Bit)

Name: **WSCReconnectModeUser**

Typ: REG_SZ

Wertdaten: 0

Ändern Sie den folgenden Schlüssel vom Standardwert 3 auf 0

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\\Dazzle` (64 Bit)

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\\Dazzle` (32 Bit)

Name: **WSCReconnectMode**

Typ: REG_SZ

Wertdaten: 0

> **Hinweis:**
>
> Wenn Sie keinen Schlüssel erstellen möchten, können Sie den REG_SZ-Wert WSCReconnectAll auf “false”festlegen.

Ändern des Timeouts der Statusanzeige

Sie können die Zeit ändern, die die Statusanzeige beim Start einer Sitzung durch einen Benutzer angezeigt wird. Zum Ändern des Timeoutzeitraums erstellen Sie einen REG_DWORD-Wert SI

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

INACTIVE MS in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\. Sie können den REG_DWORD-Wert auf 4 festlegen, wenn die Statusanzeige eher ausgeblendet werden soll.

Anpassen des Speicherorts für Anwendungsverknüpfungen über die Befehlszeile

Über die Integration in das Startmenü und den Nur-Verknüpfungsmodus können Sie Verknüpfungen für veröffentlichte Anwendungen im **Windows-Startmenü** oder auf dem Windows-Desktop platzieren. Benutzer müssen Anwendungen nicht über die Citrix Workspace-Benutzeroberfläche abonnieren. Die Integration in das Startmenü und die Verwaltung von Desktopverknüpfungen bieten eine nahtlose Desktoperfahrung für Benutzergruppen, die einen gleichförmigen Zugriff auf einen bestimmten Anwendungssatz benötigen.

Als Citrix Workspace-App-Administrator verwenden Sie Befehlszeilen-Installationsflags, Gruppenrichtlinienobjekte, Kontodienste oder Registrierungseinstellungen zum Deaktivieren der normalen Self-Service-Schnittstelle von Citrix Workspace-App und ersetzen diese mit einem vorkonfigurierten Startmenü. Das Flag heißt **SelfServiceMode** und ist standardmäßig auf "true"festgelegt. Wenn der Administrator das **SelfServiceMode**-Flag auf "false"festlegt, hat der Benutzer keinen Zugriff mehr auf die Self-Service-Benutzeroberfläche der Citrix Workspace-App. Der Zugriff auf abonnierte Apps ist stattdessen über das Startmenü und über Desktopverknüpfungen möglich. Dies wird hier als Nur-Verknüpfungsmodus bezeichnet.

Benutzer und Administratoren können eine Reihe von Registrierungseinstellungen zur Einrichtung der Verknüpfungen verwenden.

Arbeiten mit Verknüpfungen

- Benutzer können Apps nicht entfernen. Alle Apps sind verbindlich, wenn das Flag **SelfService-Mode** auf "false"festgelegt ist (= Nur-Verknüpfungsmodus). Wenn ein Benutzer ein Verknüpfungssymbol vom Desktop entfernt, wird das Symbol wieder angezeigt, wenn er über das Citrix Workspace-App-Symbol im Infobereich "Aktualisieren"auswählt.
- Benutzer können nur einen Store konfigurieren. Die Optionen Konto und Einstellungen sind nicht verfügbar. Auf diese Weise wird verhindert, dass Benutzer zusätzliche Stores konfigurieren. Der Administrator kann einem Benutzer besondere Privilegien zum Hinzufügen mehrerer Konten erteilen, indem er die Gruppenrichtlinienobjektvorlage verwendet oder den Registrierungsschlüssel HideEditStoresDialog auf dem Clientcomputer manuell hinzufügt. Wenn der Administrator einem Benutzer dieses Privileg erteilt, steht diesem die Option "Einstellungen"über das Infobereichsymbol zur Verfügung, mit der er Konten hinzufügen und entfernen kann.
- Die Benutzer können Apps nicht über die **Windows-Systemsteuerung** entfernen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Sie können Desktopverknüpfungen über eine anpassbare Registrierungseinstellung hinzufügen. Desktopverknüpfungen werden nicht standardmäßig hinzugefügt. Starten Sie nach jeder Änderung an Registrierungseinstellungen die Citrix Workspace-App neu.
- Verknüpfungen werden im Startmenü standardmäßig mit einem Kategoriepfad erstellt: UseCategoryAsStartMenuPath.

> **Hinweis:**
>
> In Windows 8/8.1 und Windows 10 ist die Erstellung von verschachtelten Ordnern im Startmenü nicht zulässig. Die Anwendungen werden einzeln oder im Stammordner angezeigt, jedoch nicht in mit Citrix Virtual Apps definierten Unterordnern für Kategorien.

- Sie können während der Installation das Flag [/DESKTOPDIR="Dir_name"] hinzufügen, um alle Verknüpfungen in einem Ordner zusammenzufassen. CategoryPath wird für Desktopverknüpfungen unterstützt.
- Die automatische Neuinstallation geänderter Apps ist ein Feature, das über den Registrierungsschlüssel AutoReInstallModifiedApps aktiviert werden kann. Wenn AutoReInstallModifiedApps aktiviert ist, werden alle auf dem Server durchgeführten Änderungen an Attributen veröffentlichter Anwendungen und Desktops auf dem Clientcomputer übernommen. Wenn AutoReInstallModifiedApps deaktiviert ist, werden Attribute von Anwendungen und Desktops nicht aktualisiert und Verknüpfungen werden nach dem Löschen bei einer Aktualisierung auf dem Client nicht wieder aufgeführt. Standardmäßig ist AutoReInstallModifiedApps aktiviert. Weitere Informationen finden Sie unter "Konfigurieren von Speicherorten für App-Verknüpfungen mit Registrierungsschlüsseln".

Anpassen des Speicherorts für Anwendungsverknüpfungen über den Registrierungs-Editor

> **Hinweis:**
>
> - Standardmäßig verwenden Registrierungsschlüssel das Format Zeichenfolge.
> - Sie müssen Änderungen an Registrierungsschlüsseln vor dem Konfigurieren eines Stores vornehmen. Möchten Sie oder ein Benutzer die Registrierungsschlüssel ändern, müssen er oder Sie die Citrix Workspace-App zurücksetzen, die Registrierungsschlüssel konfigurieren und dann den Store neu konfigurieren.

Registrierungsschlüssel für 32-Bit-Maschinen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Registry key	Value	Key path
WSCSupported	True	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver\ SR\Store\" + primaryStoreID +\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Citrix \Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\Dazzle
WSCReconnectAll	True	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID + \Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Policies \Citrix\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\Dazzle
WSCReconnectMode	3	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID +\Properties • HKLM\SOFTWARE\Policies\Citrix \Dazzle • HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectModeUser	Registry is not created during installation	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID+\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Policies \Citrix\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE \Citrix\Dazzle

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Registrierungsschlüssel für 64-Bit-Maschinen:

Registry key	Value	Key path
WSCSupported	True	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Dazzle • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\D
WSCReconnectAll	True	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\Citrix\D
WSCreconnectMode	3	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver\SR \Store\"+ primaryStoreID +"\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node \Policies\Citrix\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node \Citrix\Dazzle
WSCReconnectModeUser	Registry is not created during installation.	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver\SR \Store\"+ primaryStoreID+\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node \Citrix\Dazzle

Benutzerkonten

Sie können Benutzern wie folgt die Kontoinformationen mitteilen, die sie zum Zugriff auf die virtuellen Anwendungen und Desktops benötigen.

- Konfigurieren der e-mail-basierten Kontenermittlung
- Provisioningdatei
- Benutzerseitige manuelle Eingabe der bereitgestellten Informationen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Wichtig**
>
> Citrix empfiehlt, die Citrix Workspace-App nach der Installation neu zu starten. Damit wird sichergestellt, dass Benutzer Konten hinzufügen können, und dass die Citrix Workspace-App USB-Geräte erkennt, die während der Installation im ausgesetzten Zustand waren.

Die erfolgreiche Installation wird in einem Dialogfeld bestätigt. Danach wird der Bildschirm **Konto hinzufügen** angezeigt. Als Erstbenutzer müssen Sie im Dialogfeld **Konto hinzufügen** eine E-Mail- oder eine Serveradresse eingeben, um ein Konto einzurichten.

Unterdrücken des Dialogfelds "Konto hinzufügen"

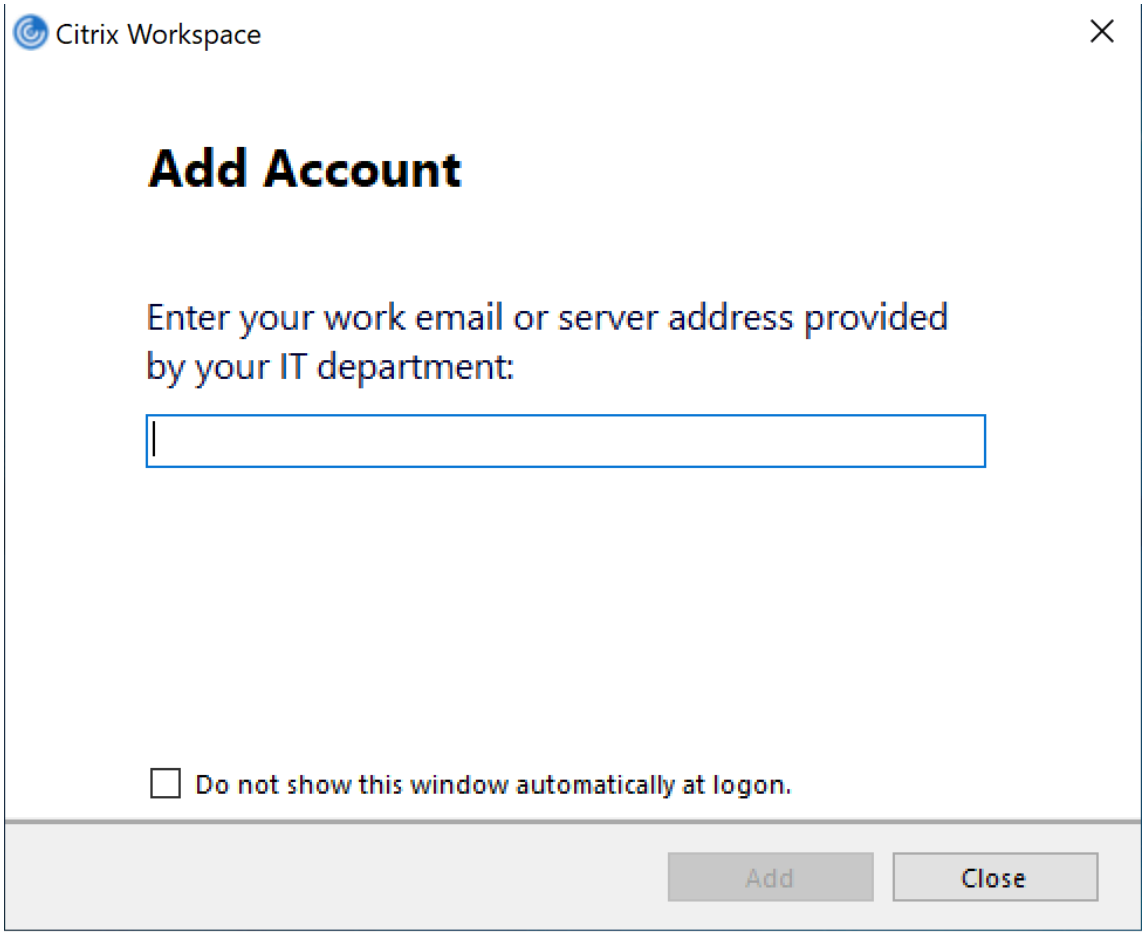
Das Dialogfeld **Konto hinzufügen** wird angezeigt, wenn der Store nicht konfiguriert ist. Mit dem Dialogfeld **Konto hinzufügen** können Sie ein Citrix Workspace-App-Konto durch Eingabe einer E-Mail-Adresse oder einer Server-URL einrichten.

Die Citrix Workspace-App ermittelt das Citrix Gateway, den StoreFront-Server oder das virtuelle App Controller-Gerät, das bzw. der der E-Mail-Adresse zugeordnet ist, und fordert den Benutzer dann zur Anmeldung auf, damit die Enumeration erfolgen kann.

Das Dialogfeld Konto hinzufügen kann wie folgt unterdrückt werden:

1. **Bei der Systemanmeldung**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Wählen Sie **Dieses Fenster bei der Anmeldung nicht automatisch anzeigen**, damit das Fenster **Konto hinzufügen** bei nachfolgenden Anmeldungen nicht angezeigt wird.
Diese Einstellung wird pro Benutzer festgelegt und wird beim Zurücksetzen der Citrix Workspace-App für Windows zurückgesetzt.

2. **Installation über die Befehlszeile**

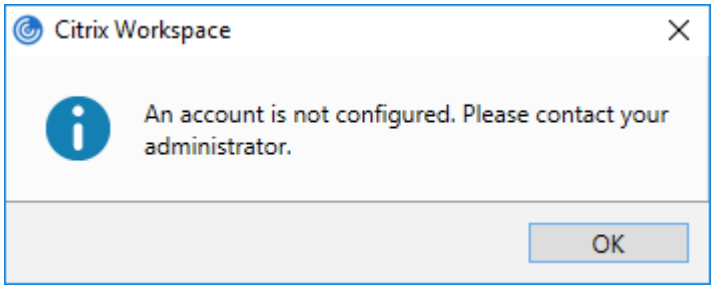
   Installieren Sie die Citrix Workspace-App für Windows als Administrator an der Befehlszeilenschnittstelle mit der folgenden Befehlszeilenoption.

   ```
   CitrixWorkspaceApp.exe /ALLOWADDSTORE=N
   ```

   Diese Einstellung gilt pro Maschine, daher ist das Verhalten für alle Benutzer gleich.

   Die folgende Meldung wird angezeigt, wenn kein Store konfiguriert ist.

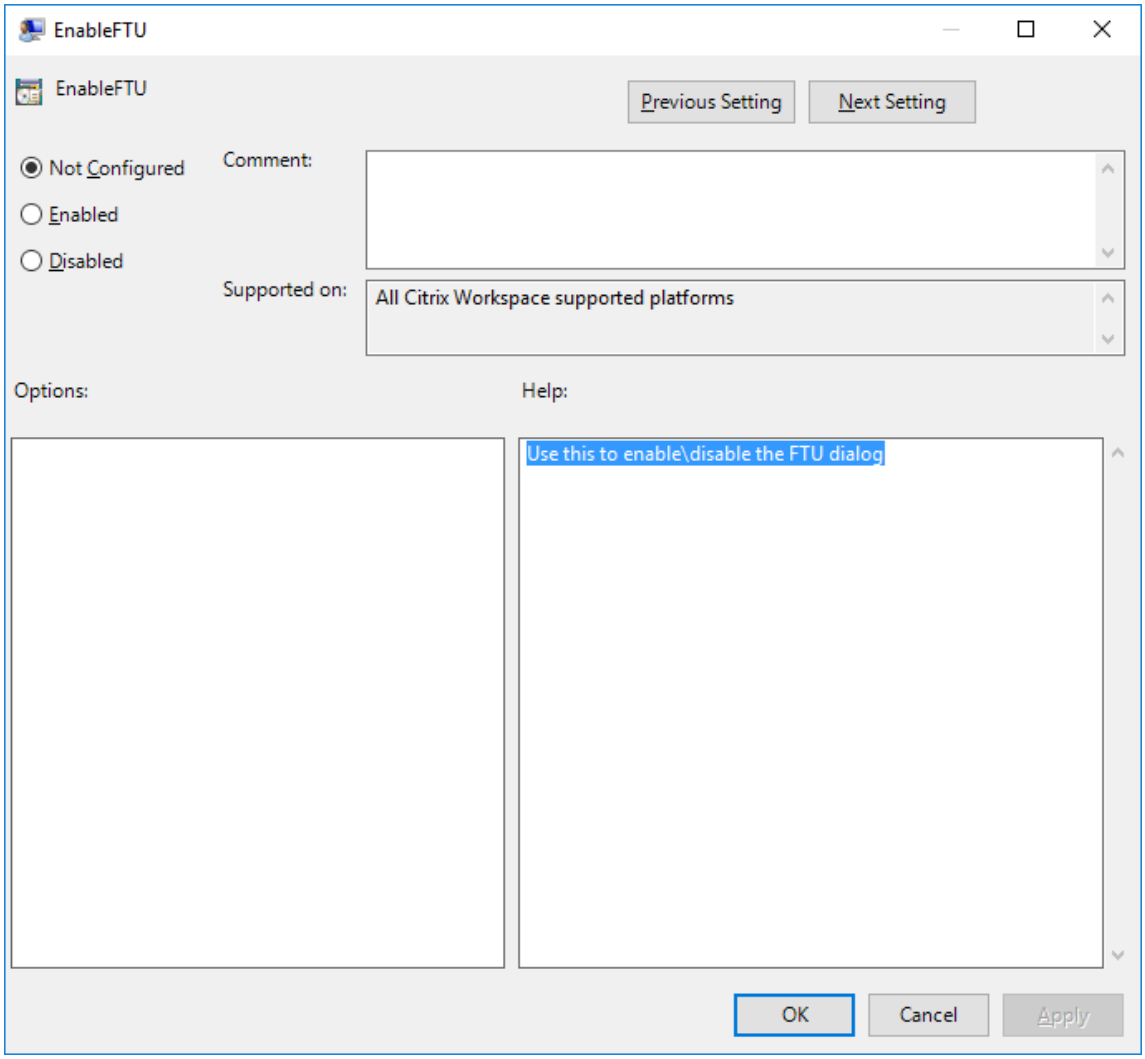
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Das Dialogfeld **Konto hinzufügen** kann wie folgt unterdrückt werden:

- **Umbenennen der ausführbaren Citrix Datei:**
  Benennen Sie die Datei **CitrixWorkspaceApp.exe** in **CitrixWorkspaceAppWeb.exe** um, um das Verhalten des Dialogfelds **Konto hinzufügen** zu ändern. Durch Umbenennen der Datei wird das Dialogfeld **Konto hinzufügen** nicht im Startmenü angezeigt.
- **Administrative Gruppenrichtlinienobjektvorlage:**
  Zum Ausblenden der Option **Konto hinzufügen** im Installationsassistenten der Citrix Workspace-App deaktivieren Sie **EnableFTUpolicy** im Knoten "Self-Service"in der lokalen administrativen Gruppenrichtlinienobjektvorlage (siehe unten).
  Diese Einstellung gilt pro Maschine, daher ist das Verhalten für alle Benutzer gleich.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Konfigurieren der e-mail-basierten Kontenermittlung

Wenn Sie die Citrix Workspace-App für die e-mail-basierte Kontenermittlung konfigurieren, geben Benutzer ihre E-Mail-Adresse statt einer Server-URL während der Erstinstallation und -konfiguration der Citrix Workspace-App ein. Die Citrix Workspace-App ermittelt den Citrix Gateway oder StoreFront-Server, der der E-Mail-Adresse auf der Basis von DNS-Dienstdatensätzen zugeordnet ist, und fordert den Benutzer dann zur Anmeldung auf, um auf virtuelle Desktops und Anwendungen zuzugreifen.

> **Hinweis:**
>
> Die e-mail-basierte Kontenermittlung wird nicht für die Bereitstellungen mit dem Webinterface unterstützt.

Weitere Informationen zum Konfigurieren der e-mail-basierten Kontenermittlung finden Sie unter Global App Configuration Service.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bereitstellen von Provisioningdateien für Benutzer

StoreFront bietet Provisioningdateien, die Benutzer für eine Verbindung mit Stores öffnen können.

Sie können mit StoreFront ein Provisioningdateien erstellen, die Verbindungsdetails für Konten enthalten. Stellen Sie diese Dateien den Benutzern zur Verfügung, um eine automatische Konfiguration der Citrix Workspace-App zu ermöglichen. Nach der Installation der Citrix Workspace-App öffnen Benutzer einfach die Datei, um die App zu konfigurieren. Wenn Sie Workspace für Website konfigurieren, können Benutzer auch Provisioningdateien für die Citrix Workspace-App von den Sites abrufen.

Weitere Informationen finden Sie unter Exportieren der Store-Provisioningdateien für Benutzer in der StoreFront-Dokumentation.

Bereitstellen der manuell einzugebenden Kontoinformationen für Benutzer

Stellen Sie sicher, dass Benutzer die nötigen Informationen zum Verbinden mit ihren virtuellen Desktops und Anwendungen haben, damit sie Konten manuell erstellen können.

- Für Verbindungen mit einem StoreFront-Store teilen Sie den Benutzern die URL für den betreffenden Server mit. Beispiel:`https://servername.company.com`.

  Für Webinterface-Bereitstellungen teilen Sie den Benutzern die URL für die Citrix DaaS-Site mit.

- Für Verbindungen über Citrix Gateway legen Sie fest, ob Benutzer alle konfigurierten Stores sehen oder nur den Store, für den der Remotezugriff auf einen bestimmten Citrix Gateway aktiviert ist.

  - Anzeigen aller konfigurierten Stores: Teilen Sie den Benutzern den FQDN für Citrix Gateway mit.
  - Beschränken des Zugriffs auf einen bestimmten Store: Teilen Sie den Benutzern den FQDN für Citrix Gateway und den Storenamen wie folgt mit:

CitrixGatewayFQDN?MyStoreName:

Wenn z. B. für Store “SalesApps”der Remotezugriff auf server1.com aktiviert ist und für Store “HRApps”Remotezugriff auf server2.com, muss ein Benutzer server1.com?SalesApps für den Zugriff auf SalesApps eingeben bzw. server2.com?HRApps für den Zugriff auf HRApps. Für dieses Feature muss ein Erstbenutzer ein Konto erstellen, indem er eine URL eingibt, und die e-mail-basierte Kontenermittlung ist nicht verfügbar.

Wenn ein Benutzer Angaben für ein neues Konto macht, versucht die Citrix Workspace-App, die Verbindung zu überprüfen. Im Erfolgsfall fordert die Citrix Workspace-App den Benutzer auf, sich bei dem Konto anzumelden.

Öffnen Sie zur Verwaltung von Konten die Homepage der Citrix Workspace-App, klicken Sie auf den ▾ und dann auf **Konten**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Automatisches Freigeben von mehreren Store-Konten

> **Warnung**
>
> Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Wenn Sie mehrere Store-Konten haben, können Sie die Citrix Workspace-App für Windows so konfigurieren, dass beim Erstellen einer Sitzung automatisch Verbindungen zu allen Konten hergestellt werden. Automatisches Anzeigen aller Konten beim Öffnen der Citrix Workspace-App:

Bei 32-Bit-Systemen: Erstellen Sie den Schlüssel "CurrentAccount":

Ort: HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

Schlüsselname: CurrentAccount

Wert: AllAccount

Typ: REG_SZ

Bei 64-Bit-Systemen: Erstellen Sie den Schlüssel "CurrentAccount":

Ort: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle

Schlüsselname: CurrentAccount

Wert: AllAccount

Typ: REG_SZ

Clientlaufwerkzuordnung

Die Citrix Workspace-App für Windows unterstützt das Zuordnen von Geräten auf Benutzergeräten, sodass sie in einer Sitzung zur Verfügung stehen. Benutzer haben folgende Möglichkeiten:

- Zugreifen auf lokale Laufwerke, Drucker und COM-Ports
- Ausschneiden und Einfügen zwischen der Sitzung und der lokalen Windows-Zwischenablage
- Wiedergeben von Audiodateien (Systemklänge und WAV-Dateien), die in der Sitzung abgespielt werden

Während der Anmeldung informiert die Citrix Workspace-App den Server über die verfügbaren Clientlaufwerke, COM- und LPT-Ports. Standardmäßig werden Clientlaufwerke Serverlaufwerksbuchstaben

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

zugeordnet. Für Clientdrucker werden Druckerwarteschlangen erstellt, sodass die Clientdrucker direkt mit der Sitzung verbunden zu sein scheinen. Diese Zuordnungen stehen nur dem aktuellen Benutzer während der aktuellen Sitzung zur Verfügung. Sie werden bei der Abmeldung des Benutzers gelöscht und bei seiner nächsten Anmeldung neu erstellt.

Mit den Einstellungen der Richtlinie für die Umleitung können Sie Benutzergeräte zuordnen, die nicht automatisch bei der Anmeldung zugeordnet werden. Weitere Informationen finden Sie in der Dokumentation zu Citrix Virtual Apps and Desktops.

Deaktivieren von Benutzergerätzuordnungen

Sie können die Benutzergerätzuordnung einschließlich Optionen für Laufwerke, Drucker und Ports mit dem **Windows-Servermanager** einstellen. Weitere Informationen über verfügbare Optionen finden Sie in der Dokumentation zu den Remotedesktopdiensten.

Umleiten von Clientordnern

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung. Wird auf dem Server nur die Clientlaufwerkzuordnung aktiviert, werden die clientseitigen vollständigen Volumes den Sitzungen automatisch als UNC-Link (Universal Naming Convention) zugeordnet. Wenn Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf dem Benutzergerät konfiguriert, wird der Teil des vom lokalen Benutzer angegebenen lokalen Volumes umgeleitet.

Nur die vom Benutzer angegebenen Ordner statt des kompletten Dateisystems auf dem Benutzergerät werden als UNC-Links in den Sitzungen angezeigt. Wenn Sie UNC-Links durch die Registrierung deaktivieren, werden Clientordner als zugeordnete Laufwerke in der Sitzung angezeigt. Weitere Informationen, u. a. zur Konfiguration der Umleitung von Clientordnern für Benutzergeräte, finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation.

Zuordnen von Clientlaufwerken zu serverseitigen Laufwerksbuchstaben

Die Clientlaufwerkzuordnung ermöglicht das Umleiten von Laufwerksbuchstaben auf der Hostseite auf Laufwerke, die auf dem Benutzergerät vorhanden sind. Beispiel: In einer Citrix Benutzersitzung kann das Laufwerk H dem Laufwerk C auf dem Benutzergerät, auf dem die Citrix Workspace-App für Windows ausgeführt wird, zugeordnet werden.

Die Clientlaufwerkzuordnung ist in die Standardfunktionen von Citrix zur Geräteumleitung integriert. Im Dateimanager, Windows Explorer und in den Anwendungen werden diese Zuordnungen genauso wie andere Netzwerkzuordnungen angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Der Server, auf dem virtuelle Desktops und Anwendungen ausgeführt werden, kann während der Installation so konfiguriert werden, dass Clientlaufwerke automatisch einem festgelegten Satz von Laufwerksbuchstaben zugeordnet werden. In der Standardinstallation werden Laufwerksbuchstaben angefangen mit V und dann absteigend Clientlaufwerksbuchstaben zugeordnet. Ein Laufwerksbuchstabe wird jeder Festplatte und jedem CD-ROM-Laufwerk zugeordnet. (Diskettenlaufwerken werden die vorhandenen Laufwerkbuchstaben zugewiesen.) Diese Methode ergibt die folgenden Laufwerkzuordnungen in einer Sitzung:

Clientlaufwerksbuchstabe	Der Server greift darauf wie folgt zu
A	A
B	B
C	V
D	U

Der Server kann so konfiguriert werden, dass zwischen den Laufwerksbuchstaben des Servers und des Clients keine Konflikte entstehen. Dazu werden die Laufwerksbuchstaben des Servers in höhere Laufwerksbuchstaben geändert. Werden beispielsweise die Serverlaufwerke C und D in M und N geändert, können die Clientgeräte direkt auf ihre Laufwerke C und D zugreifen. Diese Methode führt zu den folgenden Laufwerkszuordnungen in einer Sitzung:

Clientlaufwerksbuchstabe	Der Server greift darauf wie folgt zu
A	A
B	B
C	C
D	D

Der Laufwerksbuchstabe, durch den das Serverlaufwerk C ersetzt wird, wird während des Setups festgelegt. Alle anderen Festplatten- und CD-Laufwerksbuchstaben werden durch aufeinander folgende Laufwerksbuchstaben ersetzt (zum Beispiel: C > M, D > N, E > O). Bei diesen Laufwerksbuchstaben darf es keine Konflikte mit bereits existierenden Laufwerkszuordnungen im Netzwerk geben. Wenn ein Netzwerklaufwerk einem bereits vorhandenen Laufwerksbuchstaben eines Servers zugeordnet wird, ist die Netzlaufwerkszuordnung ungültig.

Wenn ein Benutzergerät eine Verbindung mit einem Server herstellt, werden die Clientzuordnungen wiederhergestellt, wenn die automatische Clientgerätzuordnung nicht deaktiviert ist. Die Clientlaufwerkzuordnung ist standardmäßig aktiviert. Sie können die Einstellungen mit dem Konfigurationstool

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

der Remotedesktopdienste (Terminaldienste) ändern. Außerdem können Sie mit Richtlinien genauer steuern, wie die Clientgerätzuordnung angewendet wird. Weitere Informationen zu Richtlinien finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation.

HDX Plug-n-Play-USB-Geräteumleitung

HDX Plug-n-Play USB-Geräteumleitung ermöglicht die dynamische Umleitung von Mediengeräten, einschließlich Kameras, Scannern, Medienplayern und POS-Geräten, zum Server. Sie oder der Benutzer können die Umleitung auf einige oder alle Geräte beschränken. Bearbeiten Sie die Richtlinien auf dem Server oder wenden Sie Gruppenrichtlinien auf dem Benutzergerät an, um die Einstellungen für die Umleitung zu konfigurieren. Weitere Informationen finden Sie unter Überlegungen zu USB und Clientlaufwerk in der Citrix Virtual Apps and Desktops-Dokumentation.

> **Wichtig**
>
> Wenn Sie die Plug-n-Play-USB-Geräteumleitung in einer Serverrichtlinie nicht zulassen, kann der Benutzer diese Richtlinieneinstellung nicht außer Kraft setzen.

Ein Benutzer kann Berechtigungen in der Citrix Workspace-App festlegen und die Geräteumleitung immer zulassen oder ablehnen oder bei jeder Verbindung eines Geräts gefragt werden. Diese Einstellung wirkt sich nur auf Geräte aus, die eingesteckt werden, nach dem der Benutzer die Einstellung geändert hat.

Zuordnen eines COM-Ports für Clients zu einem Server-COM-Port:

Mit der Client-COM-Portzuordnung können Geräte, die an COM-Ports des Benutzergeräts angeschlossen sind, in Sitzungen verwendet werden. Diese Zuordnungen können in gleicher Weise wie andere Netzwerkzuordnungen verwendet werden.

Sie können Client-COM-Ports von der Befehlszeile aus zuordnen. Sie können auch die Client-COM-Portzuordnung vom Remotedesktop-Konfigurationstool (Terminaldienste) oder mit Richtlinien steuern. Informationen zu Richtlinien finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation.

> **Wichtig**
>
> Die Zuordnung von COM-Ports ist nicht mit TAPI kompatibel.

1. Aktivieren Sie für Citrix Virtual Apps and Desktops-Bereitstellungen die Richtlinieneinstellung “Client-COM-Portumleitung”.
2. Melden Sie sich bei der Citrix Workspace-App an.
3. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   net use comx: \\\\\client\\comz:
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

wobei x die Nummer des COM-Ports auf dem Server ist (für die Zuordnung stehen die Ports 1 bis 9 zur Verfügung) und z die Nummer des Client-COM-Ports, den Sie zuordnen möchten.

4. Geben Sie zur Bestätigung des Vorgangs

   ```
   net use
   ```

   an der Eingabeaufforderung ein. Die angezeigte Liste enthält zugeordnete Laufwerke, LPT- und zugeordnete COM-Ports.

Installieren Sie das Gerät für den zugeordneten Namen, um diesen COM-Port in einem virtuellen Desktop oder einer Anwendung zu verwenden. Wenn Sie beispielsweise den Port COM1 auf dem Client dem Port COM5 auf dem Server zuordnen, installieren Sie das COM-Portgerät in der Sitzung auf COM5. Verwenden Sie diesen zugeordneten COM-Port dann wie einen COM-Port auf dem Benutzergerät.

DNS-Namensauflösung

Wenn die Citrix Workspace-App für Windows den Citrix XML-Dienst verwendet, kann sie einen DNS-Namen anstatt der IP-Adresse eines Servers anfordern.

> **Wichtig:**
>
> Wenn Ihre DNS-Umgebung nicht speziell für die Verwendung dieser Funktion konfiguriert ist, empfiehlt Citrix, die DNS-Namensauflösung in der Serverfarm nicht zu aktivieren.

Beim Herstellen einer Verbindung zu veröffentlichten Anwendungen über das Webinterface kann die Citrix Workspace-App ebenfalls den Citrix XML-Dienst verwenden. Damit die Citrix Workspace-App Verbindungen über das Webinterface herstellen kann, löst der Webserver den DNS-Namen für die App auf.

Die DNS-Namensauflösung ist auf dem Server standardmäßig deaktiviert und in der Citrix Workspace-App standardmäßig aktiviert. Wenn die DNS-Namensauflösung auf dem Server deaktiviert ist, wird bei jeder Citrix Workspace-App-Anfrage nach einem DNS-Namen eine IP-Adresse ausgegeben. Die DNS-Namensauflösung muss nicht in der Citrix Workspace-App deaktiviert werden.

Deaktivieren der DNS-Namensauflösung für bestimmte Benutzergeräte:

Wenn Sie in der Serverbereitstellung die DNS-Namensauflösung verwenden und Probleme mit bestimmten Benutzergeräten haben, können Sie die DNS-Namensauflösung für diese Geräte deaktivieren.

> **Achtung**
>
> Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

1. Fügen Sie eine Registrierungsschlüssel-Zeichenfolge **xmlAddressResolutionType** zu `HKEY\\_LOCAL\\_MACHINE\Software\\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing` hinzu.
2. Setzen Sie den Wert auf **IPv4-Port**.
3. Wiederholen Sie diesen Vorgang für alle Benutzer der Benutzergeräte.

Konfigurieren

May 23, 2024

App Protection

> **Haftungsausschluss**
>
> Die App Protection-Richtlinien filtern den Zugriff auf erforderliche Funktionen des zugrunde liegenden Betriebssystems (spezifische API-Aufrufe für die Bildschirmerfassung oder das Aufzeichnen von Tastenanschlägen). Damit schützen sie auch vor benutzerdefinierten und speziell entwickelten Hackertools. Die Weiterentwicklung von Betriebssystemen führt jedoch immer wieder zu neuen Einfallstoren für das Keylogging oder die Bildschirmerfassung. Darum ist kein hundertprozentiger Schutz möglich, auch wenn wir diese Schwachstellen kontinuierlich identifizieren und korrigieren.

App Protection (App-Schutz) ist ein Zusatzfeature, das erweiterte Sicherheit bei der Verwendung von Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) bietet. Die Funktion beschränkt die Möglichkeit, dass Clients durch Keylogging und Screenshot-Malware kompromittiert werden. App Protection verhindert das Exfiltrieren vertraulicher Informationen wie Benutzeranmeldeinformationen und sensible Informationen, die auf dem Bildschirm angezeigt werden. Die Funktion verhindert, dass Benutzer und Angreifer Screenshots erstellen und Keylogger verwenden, um vertrauliche Informationen zu lesen und zu nutzen.

Für App Protection müssen Sie eine Add-On-Lizenz auf dem Lizenzserver installieren. Eine Citrix Virtual Desktops-Lizenz muss ebenfalls vorhanden sein. Informationen zur Lizenzierung finden Sie unter Konfigurieren in der Dokumentation zu App Protection.

Anforderungen:

- Citrix Virtual Apps and Desktops Version 1912 oder höher.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- StoreFront Version 1912.
- Citrix Workspace-App Version 1912 oder höher

Voraussetzungen:

- App Protection muss auf dem Controller aktiviert sein. Weitere Informationen finden Sie in der Dokumentation zu App Protection.

Sie können App Protection mit einem der folgenden Verfahren in die Citrix Workspace-App integrieren:

- Bei der Installation der Citrix Workspace-App über die Befehlszeilenschnittstelle oder grafische Benutzeroberfläche. ODER
- Beim Starten einer App (Installation bei Bedarf).

> **Hinweis:**
>
> - Dieses Feature wird nur unter Microsoft Windows Desktop-Betriebssystemen wie Windows 10, Windows 8.1 und Windows 7 unterstützt.
> - Das Feature wird nicht über RDP (Remote Desktop Protocol) unterstützt.

Schutz von On-Premises-HDX-Sitzungen:

Zwei Richtlinien bieten Keylogging- und Screenshotschutz in einer Sitzung. Diese Richtlinien müssen über PowerShell konfiguriert werden. Es gibt keine grafische Benutzeroberfläche für diesen Zweck.

> **Hinweis:**
>
> Citrix DaaS unterstützt App Protection nicht.

Informationen zur Konfiguration von App Protection in Citrix Virtual Apps and Desktops finden Sie in der Dokumentation zu App Protection.

App Protection - Konfiguration in der Citrix Workspace-App

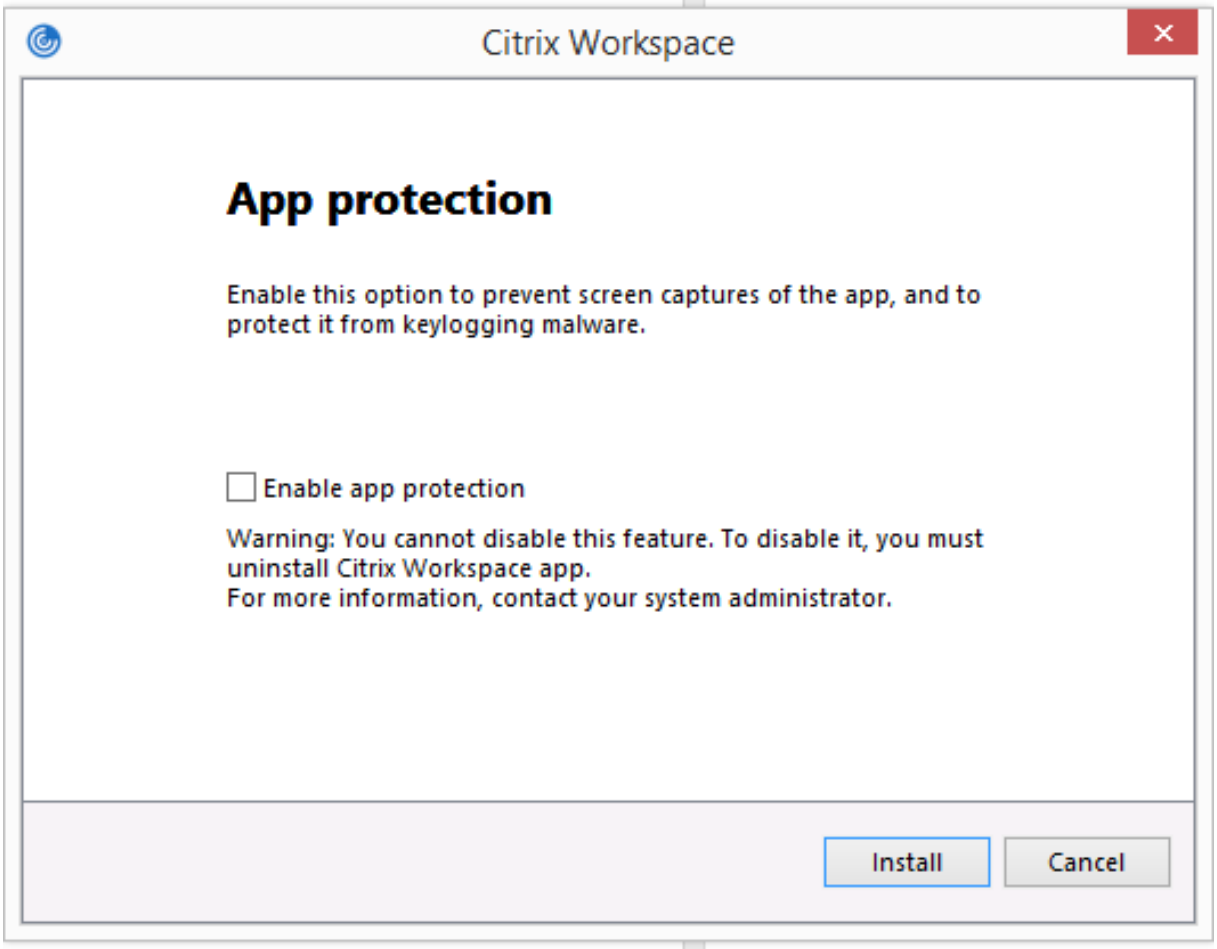
> **Hinweis:**
>
> - Integrieren Sie App Protection nur dann in die Citrix Workspace-App, wenn Sie dazu vom Administrator aufgefordert werden.
> - App Protection kann das Erstellen von Screenshots auf dem Gerät erschweren.

Bei der Installation der Citrix Workspace-App können Sie App Protection über eines der folgenden Verfahren integrieren:

- Grafische Benutzeroberfläche
- Befehlszeilenoberfläche

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Grafische Benutzeroberfläche Bei der Installation der Citrix Workspace-App können Sie die App Protection-Komponente im folgenden Dialogfeld hinzufügen. Aktivieren Sie **App Protection aktivieren** und klicken Sie auf **Installieren**, um mit der Installation fortzufahren.



> **Hinweis:**
>
> Wenn Sie App Protection nicht bei der Installation aktivieren, werden Sie beim Starten einer geschützten App dazu aufgefordert. Installieren Sie dann die App Protection-Komponente.

Befehlszeilenoberfläche Mit der Befehlszeilenoption `/includeappprotection` fügen Sie während der Installation der Citrix Workspace-App die App Protection-Komponente hinzu.

Die folgende Tabelle enthält Informationen zu Bildschirmen, die je nach Bereitstellung geschützt sind:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

App Protection bereitstellen	Geschützte Bildschirme	Nicht geschützte Bildschirme
In der Citrix Workspace-App enthalten	Self-Service-Plug-In und Authentifizierungsmanager / Dialogfeld "Benutzeranmelde-informationen"	Connection Center, Geräte, alle Fehlermeldungen der Citrix Workspace-App, Automatische Wiederverbindung von Clients, Konto hinzufügen
Auf dem Controller konfiguriert	ICA-Sitzungsbildschirm (für Apps und Desktops)	Connection Center, Geräte, alle Fehlermeldungen der Citrix Workspace-App, Automatische Wiederverbindung von Clients, Konto hinzufügen

Erwartetes Verhalten:

Das erwartete Verhalten hängt davon ab, wie Benutzer auf den StoreFront-Store zugreifen, der geschützte Ressourcen enthält.

> **Hinweis:**
>
> - Citrix empfiehlt, nur die native Citrix Workspace-App zum Starten einer geschützten Sitzung zu verwenden.

- **Verhalten in Workspace für Web:**

  App Protection wird nicht in Konfigurationen mit Workspace für Web unterstützt. Anwendungen, die durch App Protection-Richtlinien geschützt sind, werden nicht aufgelistet. Weitere Informationen zu den zugewiesenen Ressourcen erhalten Sie von Ihrem Systemadministrator.

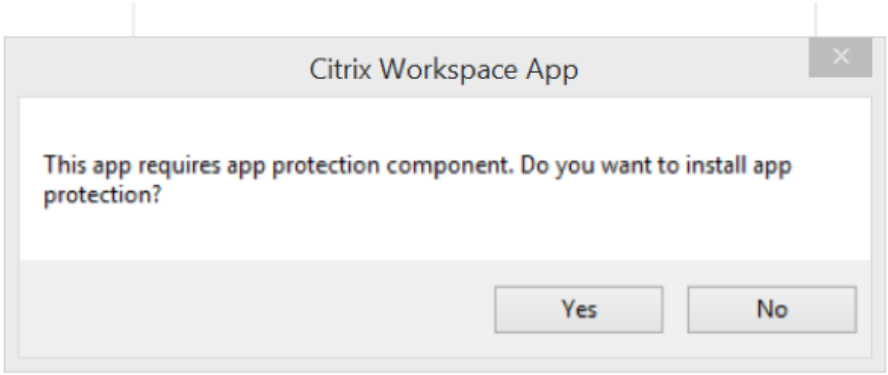
- **Verhalten in Versionen der Citrix Workspace-App, die App Protection nicht unterstützen:**

  In der Citrix Workspace-App bis Version 1911 werden Anwendungen, die durch App Protection-Richtlinien geschützt sind, in StoreFront nicht aufgelistet.

- **Verhalten von Apps, wenn App Protection auf dem Controller konfiguriert ist:**

  Wenn App Protection auf dem Controller konfiguriert ist und Sie eine geschützte Anwendung starten, wird App Protection zunächst installiert. Das folgende Dialogfeld wird angezeigt:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Klicken Sie auf **Ja**. App Protection wird installiert und der Benutzer kann die geschützte App starten.

- **Verhalten von geschützten Sitzungen mit Remotedesktopverbindung (RDP)**
  - Die aktive geschützte Sitzung wird getrennt, sobald Sie eine RDP-Sitzung starten.
  - Der Start einer geschützten Sitzung in einer Sitzung mit Remotedesktopverbindung ist nicht möglich.

App Protection-Fehlerprotokolle:

Die Protokolle von App Protection werden in der Debug-Ausgabe registriert. Führen Sie folgende Schritte aus, um diese Protokolle zu erfassen:

1. Laden Sie die App DebugView von der Microsoft-Website herunter und installieren Sie sie.
2. Starten Sie die Eingabeaufforderung, und führen Sie folgenden Befehl aus:

   ```
   Dbgview.exe /t /k /v /l C:\logs.txt
   ```

   Im obigen Beispiel können Sie die Protokolle in der Datei log.txt anzeigen.

Der Befehl gibt Folgendes an:

- `/t` –Die DebugView-App ist beim Start im Infobereich minimiert.
- `/k` –Kernel-Erfassung aktivieren.
- `/v` –Ausführliche Kernel-Erfassung aktivieren.
- `/l` –Ausgabe in spezieller Datei protokollieren.

App Protection deinstallieren:

Um App Protection zu deinstallieren, müssen Sie die Citrix Workspace-App von Ihrem System deinstallieren. Starten Sie das System neu, damit die Änderungen wirksam werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> App Protection wird nur bei einem Upgrade auf Version 1912 und höher unterstützt.

Bekannte Probleme oder Einschränkungen:

- Keine Unterstützung des Features unter Microsoft Server-Betriebssystemen wie Windows Server 2012 R2 oder Windows Server 2016.
- Um einen Screenshot auf dem lokalen Gerät zu erstellen, müssen die Fenster der Citrix Workspace-App minimiert werden. Andernfalls ist keine Bildschirmaufnahme auf dem lokalen Gerät möglich.
- Keine Unterstützung des Features in Double-Hop-Szenarios.
- Damit das Feature ordnungsgemäß funktioniert, müssen Sie auf dem VDA die Citrix-Richtlinie zur **Zwischenablagenumleitung** deaktivieren.

Geschätzte Codierungsleistung von Endpunkten in Microsoft Teams

Beim Start von HDxTeams.exe (der in die Citrix Workspace-App eingebetteten WebRTC-Medienengine für die Microsoft Teams-Umleitung) wird die optimale Codierungsauflösung geschätzt, die ohne Überlastung der Endpunkt-CPU aufrechterhalten werden kann. Mögliche Werte sind 240p, 360p, 720p und 1080p.

Diese Schätzung der Endpunktleistung (auch `webrtcapi.EndpointPerformance` genannt) läuft, wenn HdxTeams.exe initialisiert wird. Der Macroblock-Code bestimmt die beste Auflösung, die bei dem jeweiligen Endpunkt erzielt werden kann. Die höchstmögliche Auflösung fließt dann in die Codec-Aushandlung zwischen Peers oder zwischen Peer und Konferenzserver ein.

Es gibt vier Leistungskategorien für Endpunkte, jeweils mit eigener maximal verfügbarer Auflösung:

Endpunktleistung	Maximale Auflösung	Registrierungsschlüsselwert
Schnell	1080p	3
Mittel	720p	2
Langsam	360p	1
Sehr langsam	240p	0

Vorhandene Konfigurationsflags können den VP9- oder H264-Codec deaktivieren.
H264 benötigt weniger CPU-Leistung, verbraucht aber mehr Bandbreite. Im Gegensatz dazu verbraucht VP9 mehr CPU-Leistung, aber weniger Bandbreite.

Registrierungspfad in der Citrix Workspace-App:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Navigieren Sie zum Registrierungspfad HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream, und erstellen Sie folgende Schlüssel:\

Name	Typ	Werte	Beschreibung
DisableVP9	DWORD	1; 0	1 - VP9-Codec deaktivieren; 0 - aktivieren
DisableH264	DWORD	1;0	1 - H.264-Codec deaktivieren; 0 - aktivieren
OverridePerformance	DWORD	0;1;2;3	Erzwingen Sie die gewünschte Leistung. Der Wert muss zwischen 0 und 3 liegen, wobei 0 für “Sehr langsam”und 3 für “Schnell”steht.

Weitere Informationen zur Optimierung von Microsoft Teams finden Sie unter Optimierung für Microsoft Teams.

Adaptiver Transport

Adaptiver Transport ist eine Datenübertragungsmethode für Citrix Virtual Apps and Desktops und Citrix DaaS. Sie ist schneller, passt sich an, verbessert die Anwendungsinteraktivität und ist bei schwierigen Langstrecken-WAN- und Internetverbindungen interaktiver. Adaptiver Transport bietet eine hohe Serverskalierbarkeit und eine effiziente Bandbreitennutzung. Bei Verwendung des adaptiven Transports reagieren virtuelle ICA-Kanäle automatisch auf veränderliche Netzwerkbedingungen. Sie wechseln automatisch zwischen dem Citrix Protokoll Enlightened Data Transport (EDT) und TCP, um die beste Leistung zu erzielen. Dadurch wird der Datendurchsatz für alle virtuellen ICA-Kanäle, darunter Thinwire-Anzeigeremoting, Dateiübertragung (Clientlaufwerkzuordnung), Drucken und Multimedia-Umleitung verbessert. Dieselbe Einstellung gilt für LAN- und WAN-Bedingungen.

Wenn **HDXoverUDP** in älteren Releases auf **Bevorzugt** festgelegt ist, erfolgt der Datentransport wenn möglich über EDT. Wenn dies nicht möglich ist, erfolgt er über TCP.

Wenn Sie die Sitzungszuverlässigkeit aktivieren, werden EDT und TCP bei einer Sitzungszuverlässigkeitswiederverbindung und einer automatischen Wiederverbindung von Clients parallel versucht. Wenn EDT bevorzugt wird, aber der erforderliche zugrunde liegende UDP-Transport nicht verfügbar ist und TCP verwendet werden muss, wird durch diese Verbesserung die Verbindungszeit verkürzt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nach dem Fallback auf TCP sucht der adaptive Transport standardmäßig alle fünf Minuten nach EDT.

Anforderungen:

- Citrix Virtual Apps and Desktops 7.12 oder höher
- StoreFront 3.8
- Nur IPv4 VDAs; IPv6- sowie heterogene Konfigurationen mit IPv6 und IPv4 werden nicht unterstützt.
- Firewallregel zum Zulassen von eingehendem Datenverkehr an den UDP-Ports 1494 und 2598 des VDAs

> **Hinweis:**
>
> TCP-Ports 1494 und 2598 sind erforderlich und werden automatisch geöffnet, wenn Sie den VDA installieren. Die UDP-Ports 1494 und 2598 werden jedoch nicht automatisch geöffnet. Legen Sie sie auf **Aktiviert** fest.

Die Citrix Workspace-App lässt den adaptiven Transport standardmäßig zu. Ebenfalls standardmäßig versucht der Client die Verwendung des adaptiven Transports nur dann, wenn der VDA auf dem Delivery Controller für **Bevorzugt** konfiguriert ist und die Einstellung auf dem VDA angewendet wurde.

Sie können den adaptiven Transport mit der Einstellung **Adaptiver HDX-Transport** aktivieren. Legen Sie diese neue Richtlinieneinstellung auf **Bevorzugt** fest, damit der adaptive Transport verwendet wird, sofern dies möglich ist. Wo dies nicht möglich ist, wird TCP verwendet.

Verwenden Sie die administrative Gruppenrichtlinienobjektvorlage, um den adaptiven Transport auf dem Client zu deaktivieren.

Konfigurieren des adaptiven Transports mit der administrativen Gruppenrichtlinienobjektvorlage für die Citrix Workspace-App

Die folgenden Konfigurationsschritte sind optional und dienen zum Anpassen der Umgebung. Sie können das Feature beispielsweise aus Sicherheitsgründen für einen bestimmten Client deaktivieren.

> **Hinweis:**
>
> Standardmäßig ist adaptiver Transport deaktiviert (Aus) und TCP wird immer verwendet.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Netzwerkrouting**.
3. Legen Sie die Richtlinie **Transportprotokoll für Citrix Workspace** auf **Aktiviert** fest.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Wählen Sie nach Bedarf **Kommunikationsprotokoll für Citrix Workspace**.

    - **Aus** –Gibt an, dass TCP zur Datenübertragung verwendet wird.
    - **Bevorzugt** –Gibt an, dass der Client versucht, zuerst über UDP eine Verbindung zum Server herzustellen. Wenn UDP nicht verfügbar ist, wird TCP zum Verbindungsaufbau verwendet.
    - **Ein** –Gibt an, dass Citrix Workspace-App für Windows ausschließlich über UDP eine Verbindung mit dem Server herstellt. Bei dieser Option erfolgt kein Fallback auf TCP.

5. Klicken Sie auf **Anwenden** und **OK**.
6. Führen Sie an der Befehlszeile den Befehl `gpupdate /force` aus.

Zum Verwenden des adaptiven Transports fügen Sie die Citrix Workspace-App-Vorlagen dem Ordner **Policy Definitions** hinzu. Informationen über das Hinzufügen von Vorlagendateien zum lokalen Gruppenrichtlinienobjekt finden Sie unter Gruppenrichtlinienobjektvorlage.

Prüfen, ob die Richtlinieneinstellung in Kraft gesetzt wurde

Navigieren Sie zu `HKEY\\_LOCAL\\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT` und vergewissern Sie sich, dass der Schlüssel **HDXOverUDP** enthalten ist.

Weitere Informationen finden Sie unter Adaptiver Transport in der Citrix Virtual Apps and Desktops-Dokumentation.

Seite “Erweiterte Einstellungen”

Sie können die Verfügbarkeit und den Inhalt der Seite **Erweiterte Einstellungen** anpassen. Die Seite ist im Kontextmenü des Citrix Workspace-App-Symbols im Infobereich zu finden. Auf diese Weise wird sichergestellt, dass Benutzer nur vom Administrator festgelegte Einstellungen auf ihren Systemen anwenden können. Optionen:

- Ausblenden der gesamten Seite “Erweiterte Einstellungen”
- Ausblenden der folgenden Einstellungen auf der Seite:
    - Datensammlung
    - Connection Center
    - Konfigurationsprüfung
    - Tastatur und Sprachenleiste
    - Hoher DPI-Wert
    - Supportinformationen
    - Verknüpfungen und Wiederverbinden
    - Citrix Casting

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Erweiterte Einstellungen aus dem Kontextmenü ausblenden

Sie können die Seite "Erweiterte Einstellungen"über die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App ausblenden:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Self-Service** > **Erweiterte Einstellungen - Optionen**.
3. Wählen Sie die Richtlinie **Erweiterte Einstellungen deaktivieren**.
4. Wählen Sie **Aktiviert** aus, um die Option "Erweiterte Einstellungen"im Kontextmenü des Citrix Workspace-App-Symbols im Infobereich auszublenden.

> **Hinweis:**
>
> Standardmäßig ist die Option **Nicht konfiguriert** ausgewählt.

Ausblenden bestimmter Einstellungen auf der Seite "Erweiterte Einstellungen"über die administrative Gruppenrichtlinienobjektvorlage

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Self-Service** > **Erweiterte Einstellungen - Optionen**.
3. Wählen Sie die Richtlinie für die Einstellung, die Sie ausblenden möchten.

Die folgende Tabelle listet die Optionen auf, die Sie auswählen können, und deren Wirkung:

Optionen	Aktion
Nicht konfiguriert	Anzeigen der Einstellung
Aktiviert	Ausblenden der Einstellung
Deaktiviert	Anzeigen der Einstellung

Sie können die folgenden bestimmten Einstellungen auf der Seite "Erweiterte Einstellungen" ausblenden:

- Konfigurationsprüfung
- Connection Center
- Hoher DPI-Wert
- Datensammlung

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Gespeicherte Kennwörter löschen
- Tastatur und Sprachenleiste
- Verknüpfungen und Wiederverbinden
- Supportinformationen
- Citrix Casting

Ausblenden der Option zum Zurücksetzen von Workspace auf der Seite "Erweiterte Einstellungen"mit dem Registrierungs-Editor

Sie können die Option **Workspace zurücksetzen** auf der Seite "Erweiterte Einstellungen"nur mit dem Registrierungs-Editor ausblenden.

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`.
3. Erstellen Sie einen Schlüsselzeichenfolgewert **EnableFactoryReset** und legen Sie ihn auf eine der folgenden Optionen fest:
    - True: zeigt die Option "Workspace zurücksetzen"auf der Seite "Erweiterte Einstellungen" an.
    - False: blendet die Option "Workspace zurücksetzen"auf der Seite "Erweiterte Einstellungen"aus.

Ausblenden der Option "Citrix Workspace-Updates"auf der Seite "Erweiterte Einstellungen"

> **Hinweis:**
>
> Der Richtlinienpfad für die Option "Citrix Workspace-Updates"ist anders als der Richtlinienpfad der anderen Optionen auf der Seite "Erweiterte Einstellungen".

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Citrix Workspace-Updates**.
3. Wählen Sie die Richtlinie **Citrix Workspace-Updates** aus.
4. Wählen Sie **Deaktiviert**, um die Einstellungen für automatische Updates auf der Seite **Erweiterte Einstellungen** auszublenden.

Anwendungsbereitstellung

Mit den folgenden Optionen können Sie die Benutzererfahrung bei der Bereitstellung von Anwendungen mit Citrix Virtual Apps and Desktops und Citrix DaaS verbessern.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Webzugriffsmodus: Ohne jegliche Konfiguration ermöglicht die Citrix Workspace-App browserbasierten Zugriff auf Anwendungen und Desktops. Sie wählen und verwenden die gewünschten Anwendungen einfach über Workspace für Web oder eine Webinterface-Site. In diesem Modus werden keine Verknüpfungen auf dem Desktop der Benutzer platziert.
- Self-Service-Modus: Sie konfigurieren den *Self-Service-Modus* durch Hinzufügen eines StoreFront-Kontos zur Citrix Workspace-App oder durch Verweisen der Citrix Workspace-App auf eine StoreFront-Website und können so Anwendungen über die Benutzeroberfläche der Citrix Workspace-App abonnieren. Diese verbesserte Benutzererfahrung ähnelt der eines mobilen App-Stores. Im Self-Service-Modus können Sie nach Bedarf Schlüsselworteinstellungen für obligatorische, automatisch bereitgestellte und Highlight-Apps konfigurieren.

> **Hinweis:**
>
> Standardmäßig können Sie in der Citrix Workspace-App Anwendungen zur Anzeige im Startmenü auswählen.

- Nur-Verknüpfungsmodus: Mit der Citrix Workspace-App können Anwendungs- und Desktopverknüpfungen automatisch direkt in das Startmenü oder auf dem Desktop platziert werden. Mit dem neuen *Nur-Verknüpfungsmodus* werden die veröffentlichten Anwendungen entsprechend dem gewohnten Windows-Navigationsschema angezeigt.

Weitere Informationen finden Sie unter Bereitstellungsgruppe erstellen in der Dokumentation zu Citrix Virtual Apps and Desktops.

Konfigurieren des Self-Service-Modus

Um den Self-Service-Modus zu verwenden, fügen Sie der Citrix Workspace-App ein StoreFront-Konto hinzu, oder Sie legen fest, dass die Citrix Workspace-App auf eine StoreFront-Site verweist. Mit Self-Service können Benutzer die Anwendungen über die Citrix Workspace-Benutzeroberfläche abonnieren. Diese verbesserte Benutzererfahrung ähnelt der eines mobilen App-Stores.

> **Hinweis:**
>
> Standardmäßig können Benutzer der Citrix Workspace-App Anwendungen zur Anzeige im Startmenü auswählen.

Im Self-Service-Modus können Sie nach Bedarf Schlüsselworteinstellungen für obligatorische, automatisch bereitgestellte und Highlight-Apps konfigurieren.

Fügen Sie den Beschreibungen, die Sie für Bereitstellungsgruppenanwendungen eingeben, Schlüsselwörter hinzu:

- Um eine App verbindlich zu machen, sodass sie nicht aus der Citrix Workspace-App entfernt werden kann, hängen Sie die Zeichenfolge “KEYWORDS: Mandatory”an die Anwendungsbeschreibung an. Benutzer haben keine Option zum Kündigen des Abonnements verbindlicher Apps.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Sie können automatisch eine Anwendung für alle Benutzer eines Stores abonnieren, wenn Sie die Zeichenfolge "KEYWORDS: Auto"der Beschreibung anhängen. Wenn Benutzer sich an dem Store anmelden, wird die Anwendung automatisch bereitgestellt, ohne dass die Benutzer sie manuell abonnieren müssen.
- Hängen Sie die Zeichenfolge "KEYWORDS: Featured"der Anwendungsbeschreibung an, um den Benutzern Anwendungen anzukündigen oder häufig verwendete Anwendungen in der Highlightliste von Citrix Workspace anzuzeigen.

Speicherort für App-Verknüpfung mit Gruppenrichtlinienobjektvorlage konfigurieren

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Self-Service**.
3. Wählen Sie die Richtlinie **Self-Service-Modus verwalten** aus.
    a) Wählen Sie **Aktiviert**, um die Self-Service-Benutzeroberfläche anzuzeigen.
    b) Wählen Sie **Deaktiviert**, um Apps manuell zu abonnieren. Diese Option blendet die Self-Service-Benutzeroberfläche aus.
4. Wählen Sie die Richtlinie **App-Verknüpfung verwalten** aus.
5. Wählen Sie die gewünschten Optionen aus.
6. Klicken Sie auf **Anwenden und OK**.
7. Starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.

Speicherorte für App-Verknüpfungen mit StoreFront-Kontoeinstellungen anpassen

Sie können Verknüpfungen im Startmenü und auf dem Desktop von der StoreFront-Site aus einrichten. Die folgenden Einstellungen können im Abschnitt **<annotatedServices>** der Datei web.config in `C:\inetpub\wwwroot\Citrix\Roaming` hinzugefügt werden:

- Zum Einfügen von Verknüpfungen auf dem Desktop verwenden Sie PutShortcutsOnDesktop. Einstellungen: "true"oder "false"(Standardwert ist "false").
- Zum Einfügen von Verknüpfungen im Startmenü verwenden Sie PutShortcutsInStartMenu. Einstellungen: "true"oder "false"(Standardwert ist "true").
- Zum Verwenden eines Kategoriepfads im Startmenü verwenden Sie UseCategoryAsStartMenuPath. Einstellungen: "true"oder "false"(Standardwert ist "true").

> **Hinweis:**
>
> In Windows 8, 8.1 und Windows 10 ist die Erstellung von verschachtelten Ordnern im Startmenü

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> nicht zulässig. Die Anwendungen werden einzeln oder im Stammordner angezeigt, jedoch nicht in mit Citrix Virtual Apps and Desktops definierten Unterordnern für Kategorien.

- Zum Festlegen eines einzelnen Verzeichnisses für alle Verknüpfungen im Startmenü verwenden Sie StartMenuDir. Einstellung: Zeichenfolgewert, der Name des Ordners, in dem die Verknüpfungen gespeichert werden.
- Zum Neuinstallieren modifizierter Apps verwenden Sie AutoReinstallModifiedApps. Einstellungen: "true"oder "false"(Standardwert ist "true").
- Zum Anzeigen eines einzelnen Verzeichnisses für alle Verknüpfungen auf dem Desktop verwenden Sie DesktopDir. Einstellung: Zeichenfolgewert, der Name des Ordners, in dem die Verknüpfungen gespeichert werden.
- Zum Vermeiden eines Eintrags unter "Programme hinzufügen/entfernen"verwenden Sie DontCreateAddRemoveEntry. Einstellungen: "true"oder "false"(Standardwert ist "false").
- Zum Entfernen von Verknüpfungen und des Citrix Workspace-Symbols einer Anwendung, die nicht mehr im Store verfügbar ist, verwenden Sie SilentlyUninstallRemovedResources. Einstellungen: "true"oder "false"(Standardwert ist "false").

Fügen Sie die Änderungen in der Datei web.config im **XML**-Abschnitt für das Konto hinzu. Sie finden diesen Abschnitt durch Suchen des Starttags:

```
<account id=... name="Store"
```

Der Abschnitt endet mit dem Tag </account>.

Vor dem Ende des Abschnitts "account"ist der Abschnitt "properties"mit den Eigenschaften:

```
<properties> <clear> <properties>
```

Eigenschaften können in diesen Abschnitt nach dem Tag <clear /> unter Angabe des Namens und Werts (eine Eigenschaft pro Zeile) eingefügt werden. Beispiel:

```
<property name="PutShortcutsOnDesktop"value="True"/>
```

> **Hinweis:**
>
> Wenn Eigenschaftenelemente vor dem Tag <clear /> hinzugefügt werden, sind sie u. U. ungültig. Sie können das Tag <clear /> entfernen, wenn Sie einen Eigenschaftsnamen und -wert hinzufügen.

Ausführliches Beispiel für diesen Abschnitt:

```
<properties <property name="PutShortcutsOnDesktop"value="True"<
property name="DesktopDir"value="Citrix Applications">
```

> **Wichtig**
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden. Weitere Informationen finden Sie in der StoreFront-Dokumentation.

Konfigurieren von Speicherorten für App-Verknüpfungen mit Einstellungen pro App in Citrix Virtual Apps and Desktops 7.x

Mit der Citrix Workspace-App können Anwendungs- und Desktopverknüpfungen direkt in das Startmenü oder auf dem Desktop platziert werden. Ältere Versionen von Workspace für Windows enthielten eine ähnliche Funktionalität, ab Release 4.2.100 kann jedoch die Platzierung von App-Verknüpfungen in Citrix Virtual Apps über Einstellungen pro App gesteuert werden. Diese Funktionalität ist in Umgebungen mit nur einer Handvoll Anwendungen nützlich, die immer am gleichen Ort angezeigt werden sollen.

Wenn Sie die Speicherorte der Verknüpfungen für alle Benutzer gleich festlegen möchten, verwenden Sie die Citrix Virtual Apps-Einstellungen pro App:

Wenn Sie unabhängig vom Modus mit den Einstellungen pro App festlegen möchten, wo Anwendungen platziert werden …	Konfigurieren Sie die Citrix Workspace-App für Windows mit **PutShortcutsInStartMenu=false** und aktivieren Sie die Einstellungen pro App. Hinweis: Diese Einstellung gilt nur für die Webinterface-Site.

> **Hinweis:**
>
> Die Einstellung **PutShortcutsInStartMenu=false** gilt für XenApp 6.5 und XenDesktop 7.x.

Einstellungen pro App in XenApp 6.5 konfigurieren

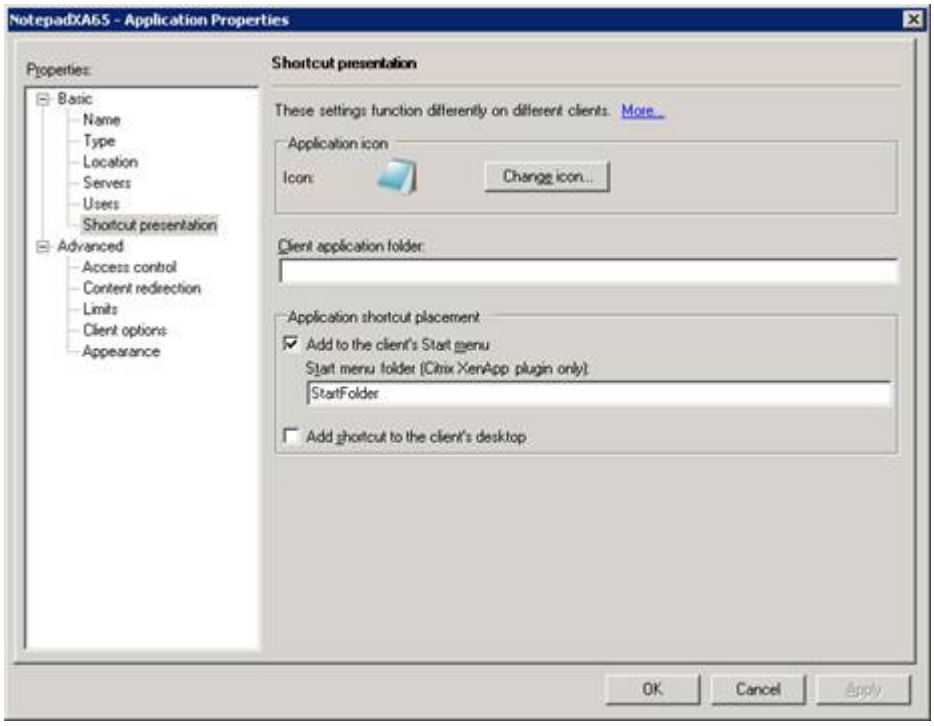
Konfigurieren einer Veröffentlichungsverknüpfung pro App in XenApp 6.5:

1. Öffnen Sie in XenApp im Bildschirm **Anwendungseigenschaften** das Eigenschaftendialogfeld **Grundlagen**.
2. Wählen Sie die Option Verknüpfungsdarstellung.
3. Aktivieren Sie im Bildschirm "Verknüpfungsdarstellung"im Bereich **Anwendungsverknüpfung festlegen** das Kontrollkästchen **Zu Startmenü von Client hinzufügen**. Geben Sie

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

anschließend den Namen des Ordners ein, in dem die Verknüpfung platziert werden soll. Wenn Sie keinen Ordnernamen angeben, platziert XenApp die Verknüpfung im Startmenü und nicht in einem Ordner des Startmenüs.

4. Aktivieren Sie Verknüpfung dem Clientdesktop hinzufügen, damit eine Verknüpfung auch auf dem Desktop der Clientmaschine erstellt wird.
5. Klicken Sie auf **Anwenden**.
6. Klicken Sie auf **OK**.



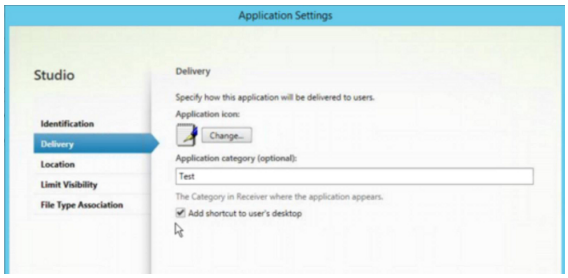
Speicherorte für App-Verknüpfungen mit Einstellungen pro App in XenApp 7.6 konfigurieren

Konfigurieren einer Veröffentlichungsverknüpfung pro App in XenApp 7.6:

1. Navigieren Sie in Citrix Studio zum Bildschirm **Anwendungseinstellungen**.
2. Wählen Sie im Bildschirm **Anwendungseinstellungen** die Option **Bereitstellung**. In diesem Bildschirm legen Sie fest, wie Anwendungen Benutzern bereitgestellt werden.
3. Wählen Sie das entsprechende Symbol für die Anwendung. Klicken Sie auf **Ändern**, um zum Speicherort des gewünschten Symbols zu navigieren.
4. Im Feld **Anwendungskategorie** können Sie optional für die Anwendung eine Kategorie in der Citrix Workspace-App angeben. Wenn Sie beispielsweise Verknüpfungen für Microsoft Office-Anwendungen hinzufügen, geben Sie Microsoft Office ein.
5. Aktivieren Sie das Kontrollkästchen "Verknüpfung auf Benutzerdesktop hinzufügen".

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Klicken Sie auf OK.



Reduzieren von Enumerationsverzögerungen oder digitales Signieren von Anwendungsstubs

Wenn die App-Enumeration bei jeder Anmeldung langsam ist oder Anwendungsstubs digital signiert werden müssen, können Sie mit der Citrix Workspace-App die EXE-Stubs von einer Netzwerkfreigabe kopieren.

Diese Funktionalität umfasst mehrere Schritte:

1. Erstellen Sie die Anwendungsstubs auf der Clientmaschine.
2. Kopieren Sie die Anwendungsstubs an einen allgemeinen Speicherort, der von einer Netzwerkfreigabe aus verfügbar ist.
3. Bereiten Sie bei Bedarf eine Positivliste vor oder signieren Sie die Stubs mit einem Unternehmenszertifikat.
4. Fügen Sie einen Registrierungsschlüssel hinzu, damit Workspace für Windows die Stubs durch Kopieren von der Netzwerkfreigabe erstellen kann.

Wenn **RemoveappsOnLogoff** und **RemoveAppsonExit** aktiviert sind und die App-Enumeration bei jeder Anmeldung langsam ist, lösen Sie das Problem mit dem folgenden Workaround:

1. Öffnen Sie den Registrierungs-Editor (regedit) und fügen Sie HKEY_CURRENT_USER\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d “true”hinzu.
2. Öffnen Sie den Registrierungs-Editor (regedit) und fügen Sie HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d “true”hinzu. HKEY_CURRENT_USER hat Vorrang vor HKEY_LOCAL_MACHINE.

> **Achtung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Ermöglichen Sie die Verwendung zuvor erstellter und in einer Netzwerkfreigabe gespeicherter EXE-Stubdateien durch den Computer:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Erstellen Sie auf einer Clientmaschine EXE-Stubdateien für alle Apps. Fügen Sie hierfür mit der Citrix Workspace-App alle Anwendungen der Maschine hinzu. Die Citrix Workspace-App generiert die EXE-Dateien.
2. Verwenden Sie die EXE-Stubdateien aus %APPDATA%\Citrix\SelfService. Sie benötigen nur die Dateien mit der Erweiterung .exe.
3. Kopieren Sie die EXE-Dateien in eine Netzwerkfreigabe.
4. Legen Sie für jeden Clientcomputer, der gesperrt werden soll, folgende Registrierungsschlüssel fest:

    a) Fügen Sie mit dem Registrierungs-Editor HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\WorkspaceStubs"hinzu.
    b) Fügen Sie mit dem Registrierungs-Editor HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v hinzu.
    c) CopyStubsFromCommonStubDirectory /t REG_SZ /d "true"hinzu. Diese Einstellungen sind auch über HKEY_CURRENT_USER möglich. HKEY_CURRENT_USER hat Vorrang vor HKEY_LOCAL_MACHINE.
    d) Beenden Sie die Citrix Workspace-App und starten Sie sie erneut, um die Einstellungen zu testen.

Anwendungsbeispiele:

In diesem Abschnitt finden Sie Anwendungsfälle für App-Verknüpfungen.

Benutzer wählen die gewünschten Apps für das Startmenü selbst aus (Self-Service)

Wenn Sie Dutzende oder sogar Hunderte von Apps haben, ist es am besten, wenn Benutzer ihre Lieblings-Apps selbst auswählen und dem Startmenü hinzufügen können:

Wenn Benutzer Apps selbst auswählen und dem Startmenü hinzufügen sollen …	…konfigurieren Sie die Citrix Workspace-App im Self-Service-Modus. In diesem Modus können Sie nach Bedarf Schlüsselworteinstellungen für *obligatorische* und *automatisch bereitgestellte* Apps konfigurieren.
Wenn Benutzer die Apps für das Startmenü selbst auswählen aber auch bestimmte App-Verknüpfungen auf dem Desktop platziert werden sollen …	…konfigurieren Sie die Citrix Workspace-App ohne Optionen und legen Sie die Einstellungen für die wenigen Apps, die auf dem Desktop platziert werden, einzeln fest. Verwenden Sie *automatisch bereitgestellte* und *obligatorische* Apps nach Bedarf.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Keine App-Verknüpfungen im Startmenü

Wenn ein Benutzer einen Familiencomputer verwendet, sind App-Verknüpfungen möglicherweise nicht erwünscht oder erforderlich. In solchen Fällen ist die einfachste Lösung der Zugriff über einen Browser. Installieren Sie die Citrix Workspace-App hierfür ohne Konfiguration und navigieren Sie zu Workspace für Web und Webinterface. Sie können für die Citrix Workspace-App auch Self-Service-Zugriff konfigurieren, ohne Verknüpfungen zu erstellen.

Wenn die Citrix Workspace-App nicht automatisch Anwendungsverknüpfungen im Startmenü platzieren soll …	…konfigurieren Sie die Citrix Workspace-App mit PutShortcutsInStartMenu=False. Die Citrix Workspace-App platziert keine App-Verknüpfungen im Startmenü, selbst wenn der Self-Service-Modus aktiviert ist. Sie können App-Verknüpfungen pro App über die Einstellungen festlegen.

Alle App-Verknüpfungen im Startmenü oder auf dem Desktop

Wenn Benutzer nur wenige Apps haben, können Sie alle Apps im Startmenü oder auf dem Desktop oder in einem Ordner auf dem Desktop platzieren.

Wenn die Citrix Workspace-App automatisch alle Anwendungsverknüpfungen im Startmenü platzieren soll…	…konfigurieren Sie die Citrix Workspace-App mit SelfServiceMode=False. Alle verfügbaren Apps werden dann im Startmenü angezeigt.
Wenn alle Anwendungsverknüpfungen auf dem Desktop platziert werden sollen…	…konfigurieren Sie die Citrix Workspace-App mit PutShortcutsOnDesktop=true. Alle verfügbaren Apps werden dann auf dem Desktop angezeigt.
Wenn alle Verknüpfungen auf dem Desktop in einem Ordner platziert werden sollen…	…konfigurieren Sie die Citrix Workspace-App mit DesktopDir=Name des Desktopordners, in dem die Anwendungen platziert werden sollen.

Einstellungen pro App in XenApp 6.5 oder 7.x

Wenn Sie die Speicherorte der Verknüpfungen für alle Benutzer gleich festlegen möchten, verwenden Sie die XenApp-Einstellungen pro App:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenn Sie unabhängig vom Modus mit den Einstellungen pro App festlegen möchten, wo Anwendungen platziert werden …	…konfigurieren Sie die Citrix Workspace-App mit PutShortcutsInStartMenu=false und aktivieren Sie die Einstellungen pro App.

Apps in Kategorieordnern oder in bestimmten Ordnern

Wenn Anwendungen in bestimmten Ordnern angezeigt werden sollen, verwenden Sie die folgenden Optionen:

Wenn die von der Citrix Workspace-App im Startmenü platzierten Anwendungsverknüpfungen in den zugeordneten Kategorieordnern angezeigt werden sollen…	…konfigurieren Sie die Citrix Workspace-App mit UseCategoryAsStartMenuPath=True.
Wenn die von der Citrix Workspace-App im Startmenü platzierten Anwendungsverknüpfungen in einem bestimmten Ordner angezeigt werden sollen…	…konfigurieren Sie die Citrix Workspace-App mit StartMenuDir=Startmenü-Ordnername.

Apps beim Abmelden oder Beenden entfernen

Wenn der Endpunkt von mehreren Benutzern verwendet wird und andere Benutzer die Apps nicht sehen sollen, stellen Sie sicher, dass die Apps beim Abmelden und Beenden des Benutzers entfernt werden.

Wenn die Citrix Workspace-App alle Apps beim Abmelden entfernen soll…	…konfigurieren Sie die Citrix Workspace-App mit RemoveAppsOnLogoff=True.
Wenn die Citrix Workspace-App alle Apps beim Beenden entfernen soll…	…konfigurieren Sie die Citrix Workspace-App mit RemoveAppsOnExit=True.

Konfigurieren von lokalem App-Zugriff für Anwendungen

Lokalen App-Zugriff für Anwendungen konfigurieren:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Wenn eine lokal installierte Anwendung statt einer in der Citrix Workspace-App verfügbaren Anwendung verwendet werden soll, hängen Sie die Zeichenfolge KEYWORDS:prefer=”pattern”an. Dieses Feature wird als lokaler App-Zugriff bezeichnet.

  Bevor die Citrix Workspace-App eine Anwendung auf dem Computer des Benutzers installiert, erfolgt eine Suche nach den angegebenen Mustern, um zu erkennen, ob die Anwendung lokal installiert ist. Wenn dies der Fall ist, abonniert die Citrix Workspace-App die Anwendung und erstellt keine Verknüpfung. Wenn der Benutzer die Anwendung vom Citrix Workspace-App-Fenster aus startet, startet die App die lokal installierte (bevorzugte) Anwendung.

  Wenn ein Benutzer eine bevorzugte Anwendung außerhalb der Citrix Workspace-App deinstalliert, wird das Abonnement für die Anwendung bei der nächsten Citrix Workspace-App-Aktualisierung gekündigt. Wenn ein Benutzer eine bevorzugte Anwendung über das Citrix Workspace-App-Dialogfeld deinstalliert, kündigt die Citrix Workspace-App das Anwendungsabonnement; die Anwendung wird jedoch nicht deinstalliert.

> **Hinweis:**
>
> Das Schlüsselwort “prefer”wird angewendet, wenn die Citrix Workspace-App eine Anwendung abonniert. Das Hinzufügen des Schlüsselworts, nach dem die Anwendung abonniert ist, hat keine Auswirkung.

Sie können das Schlüsselwort “prefer”mehrmals für eine Anwendung angeben. Nur eine Übereinstimmung wird benötigt, damit das Schlüsselwort auf eine Anwendung angewendet wird. Die folgenden Muster können in beliebiger Kombination verwendet werden:

- Wenn eine lokal installierte Anwendung statt einer in der Citrix Workspace-App verfügbaren Anwendung verwendet werden soll, hängen Sie die Textzeichenfolge KEYWORDS:prefer=”pattern” an. Dieses Feature wird als lokaler App-Zugriff bezeichnet.

  Bevor die Citrix Workspace-App eine Anwendung auf dem Computer des Benutzers installiert, erfolgt eine Suche nach den angegebenen Mustern, um zu erkennen, ob die Anwendung lokal installiert ist. Wenn dies der Fall ist, abonniert die Citrix Workspace-App die Anwendung und erstellt keine Verknüpfung. Wenn der Benutzer die Anwendung über das Citrix Workspace-App-Dialogfeld startet, startet die App die lokal installierte (bevorzugte) Anwendung.

  Wenn ein Benutzer eine bevorzugte Anwendung außerhalb der Citrix Workspace-App deinstalliert, wird das Abonnement für die Anwendung bei der nächsten Citrix Workspace-App-Aktualisierung gekündigt. Wenn ein Benutzer eine bevorzugte Anwendung über die Citrix Workspace-App deinstalliert, kündigt die App das Anwendungsabonnement; die Anwendung wird jedoch nicht deinstalliert.

Ab Version 1912 können Sie das Verhalten der automatischen Aktualisierung in der Citrix Workspace-App mit dem Registrierungs-Editor konfigurieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

In früheren Versionen wurde die Citrix Workspace-App beim Neustart auch bei vorhandenen Cache-Daten automatisch aktualisiert.

> **Hinweis:**
>
> Sie können diese Option nicht für X1-Store-fremde Konten konfigurieren.

Konfigurieren der automatischen Aktualisierung mit dem Registrierungs-Editor:

1. Starten Sie den Registrierungs-Editor und navigieren Sie zum Verzeichnis HKEY_LOCAL_MACHINE\SOFTWARE
2. Erstellen Sie die folgenden Zeichenfolgenwertschlüssel:

Registrierungsschlüssel	Wert
InitialRefreshMinMs	10000 (10 Sekunden)
InitialRefreshMaxMs	15000 (15 Sekunden)
SuppressRefreshMs	1000 (1 Sekunde)

3. Speichern Sie die Eingaben und schließen Sie den Editor.

> **Hinweis:**
>
> Das Schlüsselwort "prefer"wird angewendet, wenn die Citrix Workspace-App eine Anwendung abonniert. Das Hinzufügen des Schlüsselworts, nach dem die Anwendung abonniert ist, hat keine Auswirkung.

Sie können das Schlüsselwort "prefer"mehrmals für eine Anwendung angeben. Nur eine Übereinstimmung wird benötigt, damit das Schlüsselwort auf eine Anwendung angewendet wird. Die folgenden Muster können in beliebiger Kombination verwendet werden:

- prefer="ApplicationName"

  Das Anwendungsnamenmuster stimmt mit jeder Anwendung überein, die den angegebenen Anwendungsnamen im Verknüpfungsdateinamen hat. Der Anwendungsname kann ein Wort oder ein Satz sein. Für Sätze sind Anführungszeichen erforderlich. Die Übereinstimmung ist nicht für Teilworte oder Dateipfade zulässig; die Groß- und Kleinschreibung wird beachtet. Das Übereinstimmungsmuster für den Anwendungsnamen ist nützlich, wenn ein Administrator manuelle Überschreibungen ausführt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
Word	\Microsoft Office\Microsoft Word 2010	Ja
Microsoft Word	\Microsoft Office\Microsoft Word 2010	Ja
Konsole	McAfee\VirusScan Console	Ja
Virus	McAfee\VirusScan Console	Nein
Konsole	McAfee\VirusScan Console	Ja

- prefer="\\Folder1\Folder2\…\ApplicationName"

  Das Muster des absoluten Pfads stimmt mit dem gesamten Pfad der Verknüpfungsdatei und dem ganzen Anwendungsnamen unter dem Startmenü überein. Der Ordner "Programme"ist ein Unterordner des Startmenüverzeichnisses und muss daher im absoluten Pfad für die Zielanwendung in diesem Ordner enthalten sein. Anführungszeichen sind erforderlich, wenn der Pfad Leerstellen enthält. Für die Übereinstimmung wird die Groß-/Kleinschreibung beachtet. Das Übereinstimmungsmuster für den absoluten Pfad ist für Überschreibungen nützlich, die programmatisch in Citrix Virtual Apps and Desktops implementiert werden.

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
\Programme\Microsoft Office\Microsoft Word 2010	\Programme\Microsoft Office\Microsoft Word 2010	Ja
\Microsoft Office	\Programme\Microsoft Office\Microsoft Word 2010	Nein
\Microsoft Word 2010	\Programme\Microsoft Office\Microsoft Word 2010	Nein
\Programme\Microsoft Word 2010	\Programme\Microsoft Word 2010	Ja

- prefer="\Folder1\Folder2\…\ApplicationName"

  Das Muster des absoluten Pfads stimmt mit dem relativen Pfad unter dem Startmenü überein. Der angegebene relative Pfad muss den Anwendungsnamen enthalten und (optional) den Ordner, in dem die Verknüpfung gespeichert ist. Die Übereinstimmung ist erfolgreich, wenn am Ende des Pfads der Verknüpfungsdatei der angegebene relativen Pfad steht. Anführungszeichen sind erforderlich, wenn der Pfad Leerstellen enthält. Für die Übereinstimmung wird die Groß-/Kleinschreibung beachtet. Das Übereinstimmungsmuster für den relativen Pfad ist für Überschreibungen nützlich, die programmatisch implementiert werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
\Microsoft Office\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Ja
\Microsoft Office	\Microsoft Office\Microsoft Word 2010	Nein
\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Ja
\Microsoft Word	\Microsoft Word 2010	Nein

Informationen zu anderen Schlüsselwörtern finden Sie im Abschnitt "Zusätzliche Empfehlungen" unter Optimieren der Benutzererfahrung in der StoreFront-Dokumentation.

Dauer des Anwendungsstarts

Verwenden Sie das Feature zum Sitzungsvorabstart, um den Anwendungsstart in Zeiten mit normalem oder hohem Netzwerkverkehr zu verkürzen und die Benutzererfahrung dadurch zu verbessern. Mit dem Vorabstart-Feature kann eine Vorabstartsitzung bei der Benutzeranmeldung bei der Citrix Workspace-App oder zu einem bestimmten Zeitpunkt (wenn der Benutzer bereits angemeldet ist) erstellt werden.

Diese Vorabstartsitzung verkürzt die Startzeit der ersten Anwendung. Wenn ein Benutzer eine neue Kontoverbindung in der Citrix Workspace-App für Windows hinzufügt, findet der Sitzungsvorabstart erst in der nächsten Sitzung statt. Die Standardanwendung ctxprelaunch.exe wird in der Sitzung ausgeführt, ist jedoch für Sie unsichtbar.

Der Sitzungsvorabstart wird bei StoreFront-Bereitstellungen unterstützt. Stellen Sie bei Webinterfacebereitstellungen sicher, dass die Option **Kennwort speichern** aktiviert ist, um Anmeldeaufforderungen zu vermeiden. Sitzungsvorabstart wird nicht für Citrix Virtual Apps and Desktops-Bereitstellungen unterstützt.

Weitere Informationen finden Sie unter Sitzungsvorabstart und Sitzungsfortbestehen in einer Bereitstellungsgruppe in der Dokumentation zu Citrix Virtual Apps and Desktops.

Vorabstartsitzungen sind in der Standardeinstellung deaktiviert. Geben Sie zum Aktivieren vom Vorabstart von Sitzungen den Parameter `ENABLEPRELAUNCH=true` an der Workspace-Befehlszeile an oder legen Sie den Registrierungsschlüssel `EnablePreLaunch` auf "true"fest. Die Standardeinstellung "Null"bedeutet, dass der Vorabstart deaktiviert ist.

> **Hinweis:**
>
> Wenn der Client zur Unterstützung der Domänen-Passthrough-Authentifizierung (SSON)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> konfiguriert wurde, ist Vorabstart automatisch aktiviert. Wenn Sie die Domänen-Passthrough-Authentifizierung (SSON) ohne Vorabstart verwenden möchten, legen Sie den Registrierungsschlüssel **EnablePreLaunch** auf
> “false”fest.

Die Registrierungsverzeichnisse sind:

- HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Dazzle

Es gibt zwei Arten von Vorabstart:

- **Just-In-Time-Vorabstart:** Der Vorabstart wird direkt nach dem Authentifizieren der Anmeldeinformationen des Benutzers gestartet, unabhängig davon, ob es sich um eine Zeit mit hohem Netzwerkverkehr handelt. Diese Option wird normalerweise für Zeiten mit normalen Datenverkehr verwendet. Ein Benutzer kann den Just-In-Time-Vorabstart durch einen Neustart der Citrix Workspace-App auslösen.
- **Geplanter Vorabstart:** Der Vorabstart wird nach einem Zeitplan gestartet. Geplanter Vorabstart startet nur, wenn das Benutzergerät bereits ausgeführt wird und authentifiziert wurde. Wenn diese beiden Bedingungen zur geplanten Vorabstartzeit nicht erfüllt, wird keine Sitzung gestartet. Um Netzwerk- und Serverlast zu verteilen, wird die geplante Sitzung innerhalb eines Zeitfensters gestartet. Wenn beispielsweise Vorabstart für 13:45 geplant ist, wird die Sitzung tatsächlich irgendwann zwischen 13:15 und 13:45 gestartet. Normalerweise für Zeiten mit hohem Datenverkehr verwendet.

Zur Vorabstart-Konfiguration auf dem Citrix Virtual Apps-Server gehört das Erstellen, Bearbeiten oder Löschen von Vorabstartanwendungen sowie das Aktualisieren der Benutzerrichtlinien, die die Vorabstartanwendung steuern.

Sie können die Vorabstartfunktion nicht mit der Datei receiver.admx anpassen. Sie können aber die Vorabstartkonfiguration ändern, indem Sie während oder nach der Installation der Citrix Workspace-App für Windows die Registrierungswerte ändern.

- Die HKEY_LOCAL_MACHINE-Werte werden während der Clientinstallation geschrieben.
- Mit den HKEY_CURRENT_USER-Werten können Sie verschiedenen Benutzern auf derselben Maschine unterschiedliche Einstellungen bereitstellen. Die Benutzer können die HKEY_CURRENT_USER-Werte ohne Administratorrechte ändern. Sie können Skripts bereitstellen, mit denen die Benutzer diese Konfigurationsänderungen vornehmen können.

Registrierungswerte für HKEY_LOCAL_MACHINE:

Für 64-Bit-Windows-Betriebssysteme: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Für 32-Bit-Windows-Betriebssysteme: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch

Name: **UserOverride**

Werte:

0 - Wert unter HKEY_LOCAL_MACHINE verwenden, selbst wenn unter HKEY_CURRENT_USER Werte vorhanden sind.

1 - Werte unter HKEY_CURRENT_USER verwenden, wenn vorhanden, sonst den Wert unter HKEY_LOCAL_MACHINE.

Name: **State**

Werte:

0 - Vorabstart deaktivieren.

1 - Just-In-Time-Vorabstart aktivieren. (Vorabstart wird gestartet, nachdem die Anmeldeinformationen des Benutzers authentifiziert wurden.)

2 - Geplanten Vorabstart aktivieren. (Vorabstart startet zu der Zeit, die unter Schedule angegeben wurde.)

Name: **Schedule**

Wert:

Uhrzeit (24-Stunden-Format) und Wochentage für geplanten Vorabstart in folgendem Format:

`HH:MM|M:T:W:TH:F:S:SU` - dabei stehen `HH` und `MM` für Stunden und Minuten und `M:T:W:TH:F:S:SU` für den Wochentag. Um beispielsweise den Vorabstart montags, mittwochs und freitags um 13:45 zu aktivieren, stellen Sie Folgendes ein: Schedule=13:45	1:0:1:0:1:0:0. Die Sitzung wird irgendwann zwischen 13:15 und 13.45 gestartet.

Registrierungswerte für HKEY_CURRENT_USER:

HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

Die Schlüssel State und Schedule haben dieselben Werte wie für HKEY_LOCAL_MACHINE.

Bidirektionale Inhaltsumleitung

Die bidirektionale Inhaltsumleitung ermöglicht das Aktivieren und Deaktivieren der Client-zu-Host- und der Host-zu-Client-URL-Umleitung. Serverrichtlinien werden in Studio festgelegt und Clientrichtlinien werden in der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App festgelegt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix bietet zwar auch Host-zu-Client-Umleitung und lokalen App-Zugriff für die Client-zu-URL-Umleitung an, es wird jedoch die Verwendung der bidirektionalen Inhaltsumleitung für in die Domäne eingebundene Windows-Clients empfohlen.

Sie können die bidirektionale Inhaltsumleitung auf folgende Weise aktivieren:

1. Administrative Gruppenrichtlinienobjektvorlage
2. Registrierungs-Editor

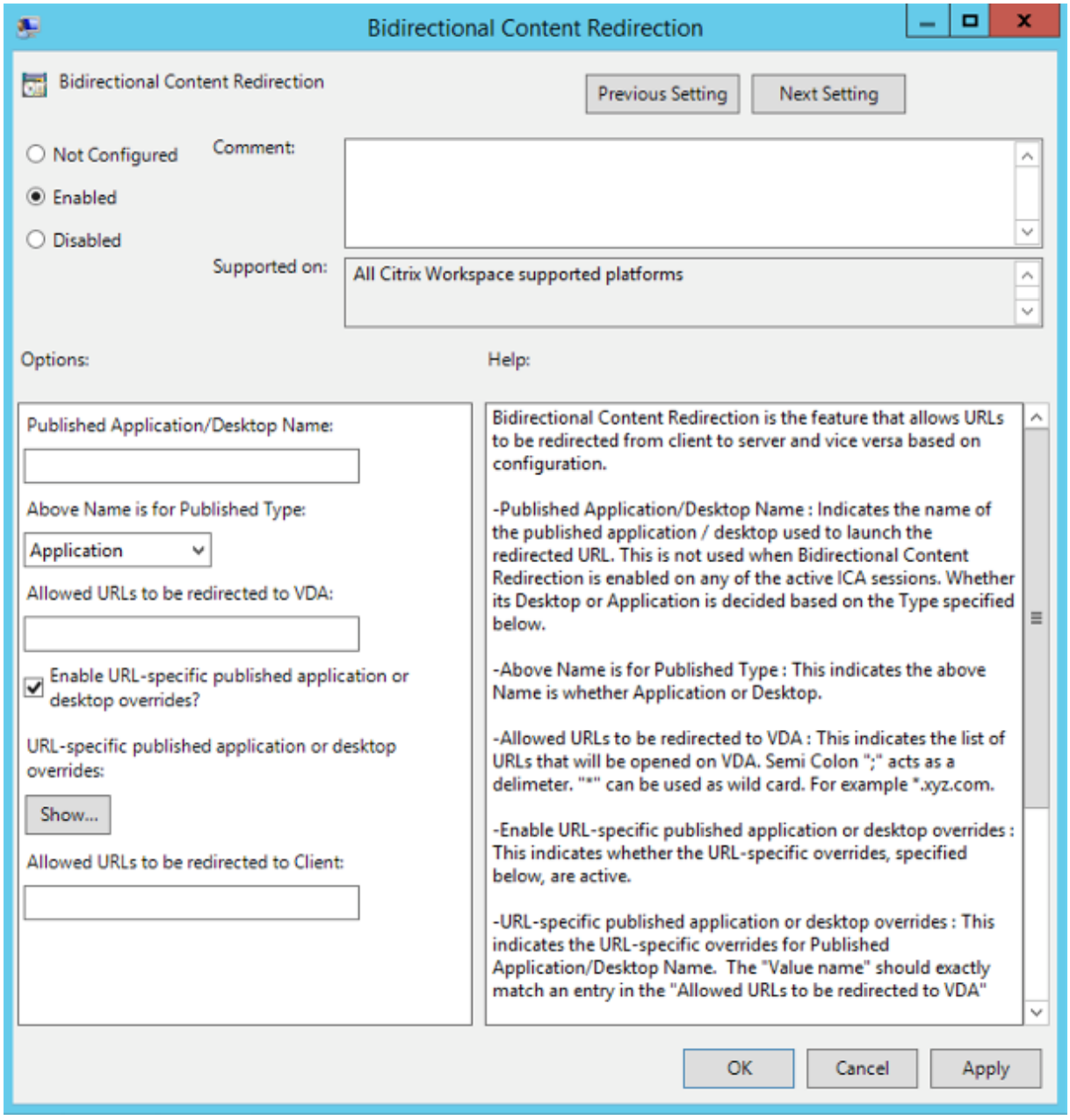
> **Hinweis:**
>
> - Die bidirektionale Inhaltsumleitung funktioniert nicht in einer Sitzung, in der **Lokaler App-Zugriff** aktiviert ist.
> - Die bidirektionale Inhaltsumleitung muss auf dem Server und dem Client aktiviert sein. Wenn sie auf dem Server oder auf dem Client deaktiviert ist, ist die Funktion deaktiviert.
> - Wenn Sie URLs einschließen, können Sie eine URL angeben oder eine durch Semikolon getrennte Liste von URLs. Sie können ein Sternchen (*) als Platzhalter verwenden.

Aktivieren der bidirektionalen Inhaltsumleitung mit der administrativen Gruppenrichtlinienobjektvorlage:

Verwenden Sie die Konfiguration mit der administrativen Gruppenrichtlinienobjektvorlage nur für die Erstinstallation der Citrix Workspace-App für Windows.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Benutzerkonfiguration** zu **Administrative Vorlagen** > **Klassische administrative Vorlagen (ADM)** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzererfahrung**.
3. Wählen Sie die Richtlinie **Bidirektionale Inhaltsumleitung**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



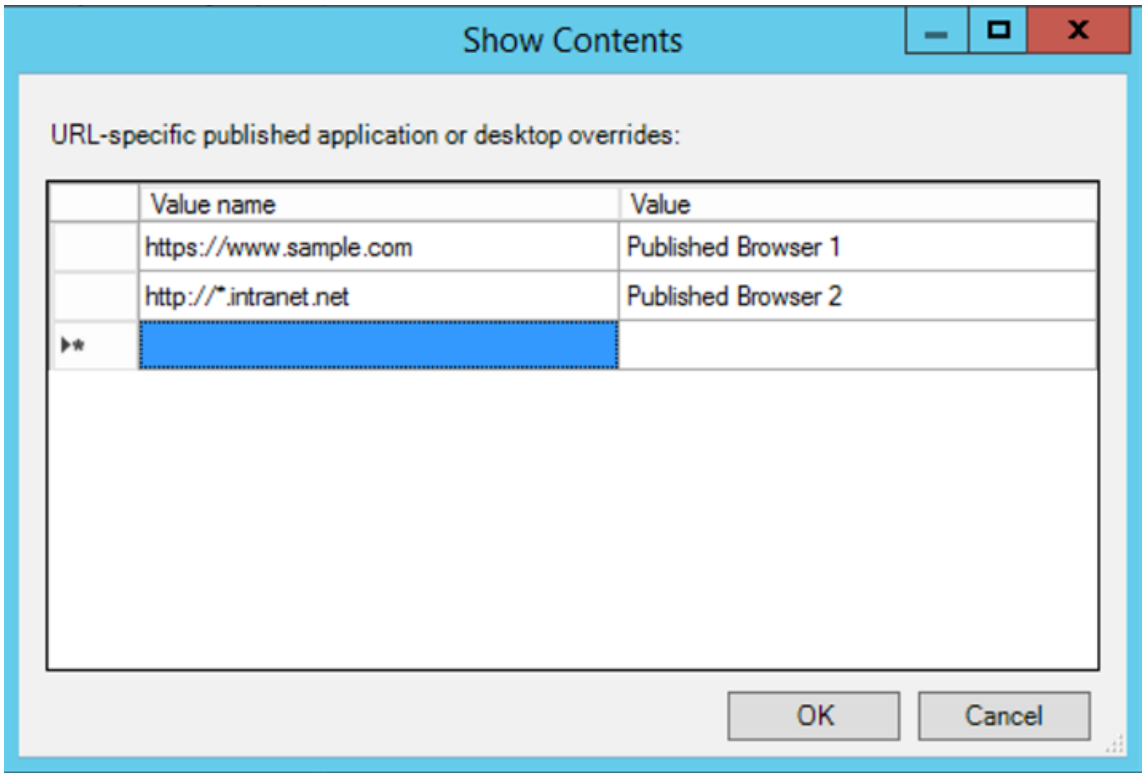
1. Geben Sie im Feld **Veröffentlichte(r) Anwendung/Desktop:** den Namen der Ressource ein, die zum Starten der umgeleiteten URL verwendet wird.

   > **Hinweis:**
   >
   > Wenn Sie URLs einschließen, geben Sie eine URL oder eine durch Semikola getrennte Liste der URLs an. Sie können ein Sternchen (*) als Platzhalter verwenden.

2. Wählen Sie unter **Veröffentlicht als** die Option **Anwendung** oder **Desktop** aus.
3. Geben Sie im Feld **Für Umleitung an VDA zulässige URLs** die URL ein, die umgeleitet werden soll. Trennen Sie die Listeneinträge durch Semikola voneinander.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Wählen Sie **URL-spezifische Außerkraftsetzungen für veröffentlichte Anwendungen oder Desktops aktivieren?**, wenn für eine URL eine Außerkraftsetzung gelten soll.
5. Klicken Sie auf **Anzeigen**, um eine Liste anzuzeigen, in der der Wertname mit einer der URLs im Feld **Für Umleitung an VDA zulässige URLs** übereinstimmen muss. Der Wert muss mit dem Namen einer veröffentlichten Anwendung übereinstimmen.



6. Geben Sie im Feld **Für Umleitung an Client zulässige URLs** die URL ein, die vom Server an den Client umgeleitet werden soll. Trennen Sie die Listeneinträge durch Semikola voneinander.

> **Hinweis:**
>
> Wenn Sie URLs einschließen, geben Sie eine URL oder eine durch Semikola getrennte Liste der URLs an. Sie können ein Sternchen (*) als Platzhalter verwenden.

7. Klicken Sie auf **Anwenden** und **OK**.
8. Führen Sie an der Befehlszeile den Befehl `gpupdate /force` aus.

Aktivieren der bidirektionalen Inhaltsumleitung mit der Registrierung:

Zum Aktivieren der bidirektionalen Inhaltsumleitung führen Sie den Befehl `redirector.exe /RegIE` im Installationsordner der Citrix Workspace-App aus (`C:\Program Files (x86)\Citrix\ICA Client`).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wichtig:

- Stellen Sie sicher, dass Umleitungsregeln keine Schleifenkonfiguration ergeben. Eine Schleifenkonfiguration entsteht zum Beispiel, wenn VDA-Regeln so festgelegt sind, dass eine URL wie `https://www.my\\_company.com` an den Client und an den VDA umgeleitet wird.
- Die URL-Umleitung unterstützt nur explizite URLs, d. h. solche, die in der Adressleiste des Browsers angezeigt werden oder die mit der browserinternen Suchfunktion gefunden wurden (je nach Browser).
- Wenn zwei Anwendungen mit demselben Anzeigenamen mehrere StoreFront-Konten verwenden, wird der Anzeigename im primären StoreFront-Konto für den Start der Anwendung oder einer Desktopsitzung verwendet.
- Ein neues Browserfenster wird nur geöffnet, wenn die URL zum Client umgeleitet wird. Wenn die URL zum VDA umgeleitet wird, und der Browser bereits geöffnet ist, wird die umgeleitete URL auf einer neuen Registerkarte geöffnet.
- Eingebettete Links in Dateien wie Dokumente, E-Mails, PDFs werden unterstützt.
- Stellen Sie sicher, dass auf einer Maschine nur entweder die Richtlinie für Serverdateitypzuordnung oder die für die Hostinhaltsumleitung aktiviert ist. Citrix empfiehlt, entweder das Serverdateitypzuordnungsfeature oder das URL-Umleitungsfeature zu deaktivieren, um sicherzustellen, dass die URL-Umleitung ordnungsgemäß funktioniert.

Einschränkung:

Kein Fallbackmechanismus ist vorhanden, wenn die Umleitung aufgrund von Problemen mit dem Sitzungsstart fehlschlägt.

Bloomberg-Tastaturen

Die Citrix Workspace-App unterstützt die Verwendung einer Bloomberg-Tastatur in Sitzungen mit virtuellen Apps und Desktops. Die erforderlichen Komponenten werden mit dem Plug-In installiert. Sie können das Feature für Bloomberg-Tastaturen zusammen mit der Citrix Workspace-App für Windows installieren oder über die Registrierung aktivieren.

Mehrere Sitzungen mit Bloomberg-Tastaturen sind nicht empfehlenswert. Die Tastatur funktioniert nur in Einzelsitzungen.

Konfigurieren einer Bloomberg-Tastatur:

Achtung

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übern-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> immt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

1. Gehen Sie zu folgendem Schlüssel in der Registrierung:

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

2. Führen Sie einen der folgenden Schritte aus:

   - Zum Aktivieren dieses Features müssen Sie den Eintrag mit Typ DWORD und dem Namen **EnableBloombergHID** auf den Wert 1 setzen.
   - Zum Deaktivieren dieses Features setzen Sie den Wert auf 0.

Weitere Informationen zum Konfigurieren von Bloomberg-Tastaturen finden Sie im Knowledge Center-Artikel CTX122615.

Abblenden des Desktop Viewer-Fensters verhindern:

Wenn Sie mehrere Desktop Viewer-Fenster verwenden, sind die nicht aktiven Desktops in der Standardeinstellung abgeblendet. Wenn Benutzer mehrere Desktops gleichzeitig anzeigen möchten, können die Informationen auf den Desktops unlesbar sein. Sie können das Standardverhalten deaktivieren und das Abblenden des Desktop Viewer-Fensters durch Bearbeiten der Registrierung verhindern.

> **Achtung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall eine Sicherungskopie der Registrierung, bevor Sie sie bearbeiten.

- Erstellen Sie auf dem Benutzergerät einen REG_DWORD-Eintrag mit dem Namen **DisableDimming** in einem der folgenden Registrierungsschlüssel, abhängig davon, ob Sie ein Abblenden für den aktuellen Benutzer des Geräts oder für das Gerät selbst einstellen möchten. Ein Eintrag ist bereits vorhanden, wenn Desktop Viewer auf dem Gerät verwendet wurde:
  - `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`
  - `HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop\DesktopViewer`

Sie können das Abblenden steuern oder auch eine lokale Richtlinie festlegen, indem Sie denselben REG_WORD-Eintrag in einem der folgenden Schlüssel erstellen:

- `HKEY_CURRENT_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer`

Überprüfen Sie vor der Verwendung dieser Schlüssel, ob der Administrator von Citrix Virtual Apps and Desktops und Citrix DaaS eine Richtlinie für dieses Feature festgelegt hat.

Stellen Sie den Eintrag auf einen Wert ungleich Null ein, z. B. 1 oder true.

Wenn keine Einträge angegeben sind, oder der Eintrag auf 0 gesetzt ist, wird das Desktop Viewer-Fenster abgeblendet. Bei Angabe mehrerer Einträge wird die folgende Priorität verwendet. Der erste Eintrag und Wert in der Liste legen fest, ob das Fenster abgeblendet wird:

1. HKEY_CURRENT_USER\Software\Policies\Citrix\…
2. HKEY_LOCAL_MACHINE\Software\Policies\Citrix\…
3. HKEY_CURRENT_USER\Software\Citrix\…
4. HKEY_LOCAL_MACHINE\Software\Citrix\…

Citrix Casting

Der Citrix Ready Workspace Hub verbindet die digitale und die physische Umgebung zur Bereitstellung von Apps und Daten in einem sicheren, intelligenten Bereich. Das System verbindet Geräte (oder auch Dinge, z. B. mobile Apps und Sensoren) zur Schaffung einer intelligenten und reaktionsfähigen Umgebung.

Citrix Ready Workspace Hub baut auf der Raspberry Pi 3-Plattform auf. Das Gerät, auf dem die Citrix Workspace-App ausgeführt wird, stellt eine Verbindung zum Citrix Ready Workspace Hub her und ermöglicht die Anzeige von Apps und Desktops auf einem größeren Display. Citrix Casting wird nur unter Microsoft Windows 10 Version 1607 und höher oder auf Windows Server 2016 unterstützt.

Citrix Casting ist ein Feature, mit dem Sie sofort und sicher auf jede App auf einem Mobilgerät zugreifen sie und auf einem großen Bildschirm anzeigen können.

> **Hinweis:**
>
> - Citrix Casting für Windows unterstützt Citrix Ready Workspace Hub Version 2.40.3839 und höher. Frühere Versionen werden möglicherweise nicht erkannt oder verursachen einen Castingfehler.
> - Citrix Casting wird in der Citrix Workspace-App für Windows (Store) nicht unterstützt.

Voraussetzungen:

- Bluetooth ist zur Hub-Erkennung auf dem Gerät aktiviert.
- Citrix Ready Workspace Hub und Citrix Workspace-App müssen sich im selben Netzwerk befinden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Port 55555 darf zwischen dem Gerät mit ausgeführter Citrix Workspace-App und dem Citrix Ready Workspace Hub nicht blockiert sein.
- Port 1494 darf für Citrix Casting nicht blockiert sein.
- Port 55556 ist der Standardport für SSL-Verbindungen zwischen Mobilgeräten und dem Citrix Ready Workspace Hub. Sie können in den Einstellungen von Raspberry Pi einen anderen SSL-Port konfigurieren. Wenn der SSL-Port blockiert ist, können die Benutzer keine SSL-Verbindungen zum Workspace Hub herstellen.
- Citrix Casting wird nur unter Microsoft Windows 10 Version 1607 und höher oder auf Windows Server 2016 unterstützt.

Konfigurieren des Citrix Casting-Starts

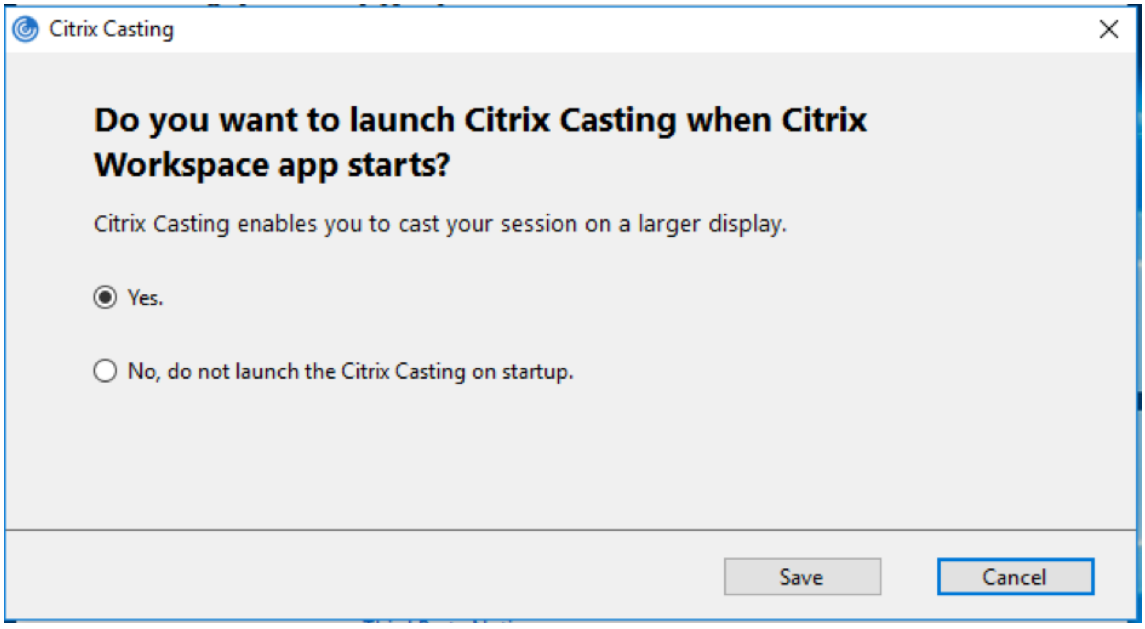
> **Hinweis:**
>
> Sie können die über das Citrix Workspace-App-Symbol im Infobereich verfügbare Seite "Erweiterte Einstellungen"ganz oder teilweise ausblenden. Weitere Informationen finden Sie unter Erweiterte Einstellungen.

1. Klicken Sie im Infobereich mit der rechten Maustaste auf das Symbol der Citrix Workspace-App und wählen Sie **Erweiterte Einstellungen**.

   Das Dialogfeld **Erweiterte Einstellungen** wird angezeigt.

2. Wählen Sie **Citrix Casting**.

   Das Dialogfeld **Citrix Casting** wird angezeigt.



3. Wählen Sie eine dieser Optionen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Ja –Citrix Casting wird beim Start der Citrix Workspace-App ebenfalls gestartet.
- Nein, Citrix Casting beim Start nicht starten –Gibt an, dass Citrix Casting beim Start der Citrix Workspace-App nicht gestartet wird.

> **Hinweis:**
>
> Bei Auswahl der Option **Nein** wird die aktuelle Bildschirmcastingsitzung nicht beendet. Die Einstellung wird erst beim nächsten Start der Citrix Workspace-App wirksam.

4. Klicken Sie auf **Speichern**, um die Änderung zu übernehmen.

Citrix Casting mit der Citrix Workspace-App verwenden

1. Melden Sie sich an der Citrix Workspace-App an und aktivieren Sie Bluetooth auf Ihrem Gerät.

   Die Liste der verfügbaren Hubs wird angezeigt. Die Liste ist nach dem RSSI-Wert des Beaconpakets der Workspace Hubs sortiert.

2. Wählen Sie den Workspace Hub aus, an den Sie Ihre Anzeige übertragen möchten, und wählen Sie eine der folgenden Optionen:

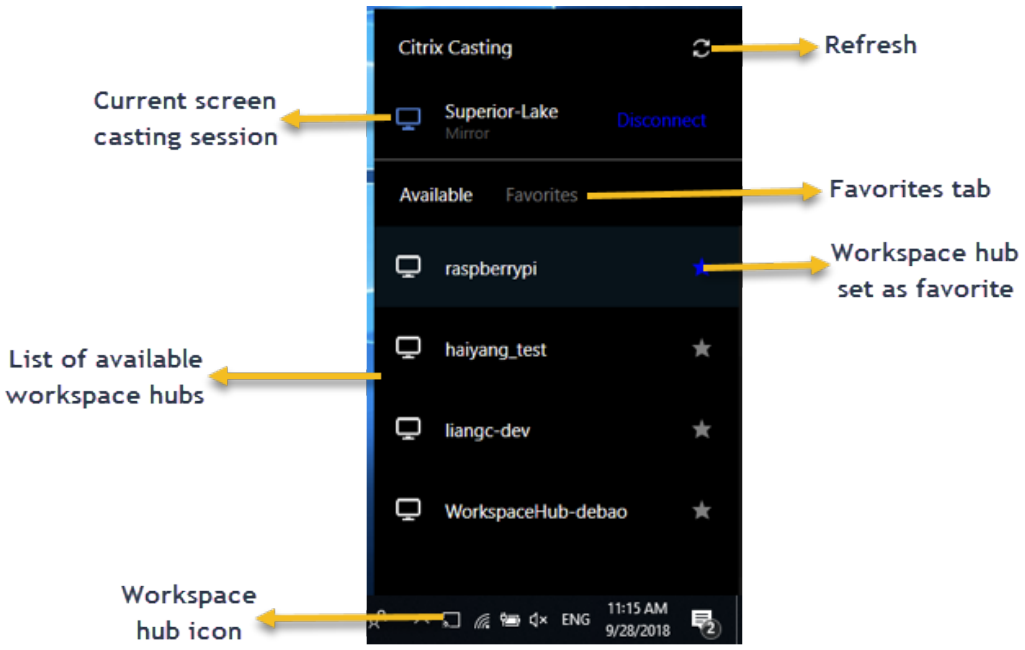
   - Mit **Spiegeln** können Sie den primären Bildschirm duplizieren und die Anzeige an das verbundene Workspace Hub-Gerät übertragen.
   - Mit **Erweitern** können Sie den Bildschirm des Workspace Hub-Geräts als sekundären Bildschirm verwenden.

> **Hinweis:**
>
> Beim Beenden der Citrix Workspace-App wird Citrix Casting nicht beendet.

Im Infobereich von **Citrix Casting** sind folgende Optionen verfügbar:

1. Die aktuelle Bildschirmcastingsitzung wird oben angezeigt.
2. Symbol **Aktualisieren**.
3. Wählen Sie **Trennen**, um die aktuelle Bildschirmcastingsitzung auf dem Workspace Hub zu beenden.
4. Mit dem Stern fügen Sie den Workspace Hub zu **Favoriten** hinzu.
5. Klicken Sie mit der rechten Maustaste auf das Workspace Hub-Symbol im Infobereich und wählen Sie **Beenden**, um die Bildschirmcastingsitzung zu trennen und den Citrix Ready Workspace Hub zu beenden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Checkliste bei Problemen

Prüfen Sie folgende Faktoren, wenn die Citrix Workspace-App keine verfügbaren Workspace Hubs im Umfeld erkennt oder mit ihnen nicht kommunizieren kann:

1. Citrix Workspace-App und Citrix Ready Workspace Hub sind mit demselben Netzwerk verbunden.
2. Bluetooth ist aktiviert und funktioniert ordnungsgemäß auf dem Gerät, auf dem die Citrix Workspace-App ausgeführt wird.
3. Das Gerät, auf dem die Citrix Workspace-App ausgeführt wird, liegt in Reichweite des Citrix Ready Workspace Hub, also weniger als 10 Meter entfernt und nicht hinter einer Wand oder einem anderen Hindernis.
4. Öffnen Sie einen Browser in der Citrix Workspace-App und geben Sie `http://<hub_ip>:55555/device-details.xml` ein, um zu überprüfen, ob die Workspace Hub-Gerätedetails angezeigt werden.
5. Klicken Sie in Citrix Ready Workspace Hub auf **Aktualisieren** und versuchen Sie erneut, eine Verbindung zum Workspace Hub herzustellen.

Bekannte Probleme und Einschränkungen

1. Citrix Casting funktioniert nur, wenn das Gerät mit demselben Netzwerk wie der Citrix Ready Workspace Hub verbunden ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Bei Netzwerkproblemen kann es zu einer verzögerten Anzeige auf dem Workspace Hub-Gerät kommen.
3. Bei Auswahl von **Erweitern** blinkt der primäre Bildschirm, auf dem die Citrix Ready Workspace-App gestartet wird, mehrmals.
4. Im Modus **Erweitern** können Sie die sekundäre Anzeige nicht als primäre Anzeige festlegen.
5. Die Bildschirmcastingsitzung wird automatisch beendet, wenn die Anzeigeeinstellungen auf dem Gerät geändert werden. Dies kann beispielsweise auftreten, wenn Sie die Bildschirmauflösung oder Bildschirmausrichtung ändern.
6. Wenn das Gerät, auf dem die Citrix Workspace-App ausgeführt wird, während der Bildschirmcastingsitzung gesperrt, inaktiviert oder in den Ruhezustand versetzt wird, wird beim Anmelden ein Fehler angezeigt.
7. Mehrere Bildschirmcastingsitzungen werden nicht unterstützt.
8. Die von Citrix Casting unterstützte maximale Bildschirmauflösung beträgt 1920 x 1440.
9. Citrix Casting unterstützt Citrix Ready Workspace Hub Version 2.40.3839 und höher. Frühere Versionen werden möglicherweise nicht erkannt oder verursachen einen Castingfehler.
10. Das Feature wird in der Citrix Workspace-App für Windows (Store) nicht unterstützt.
11. Unter Windows 10, Build 1607 wird Citrix Casting im Modus **Erweitert** u. U. nicht richtig positioniert.

Umleitung von USB-Verbundgeräten

Konfigurieren der Umleitung von USB-Verbundgeräten:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Remoting von Clientgeräten** > **Generisches USB-Remoting**.
3. Wählen Sie die Richtlinie **SplitDevices** (Geräte teilen).
4. Wählen Sie **Aktiviert**.
5. Klicken Sie auf **Anwenden** und auf **OK**, um die Richtlinie zu speichern.

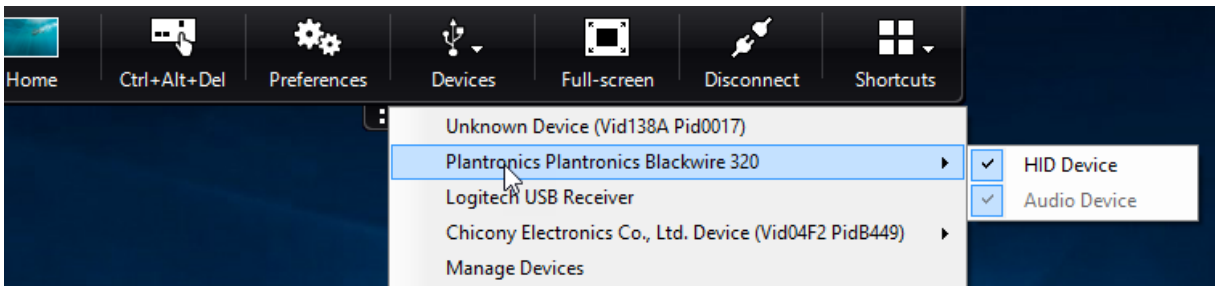
Zulassen oder Ablehnen einer Schnittstelle:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Benutzerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Remoting von Clientgeräten** > **Generisches USB-Remoting**.
3. Wählen Sie die Richtlinie **USB-Geräteregeln**.
4. Wählen Sie **Aktiviert**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

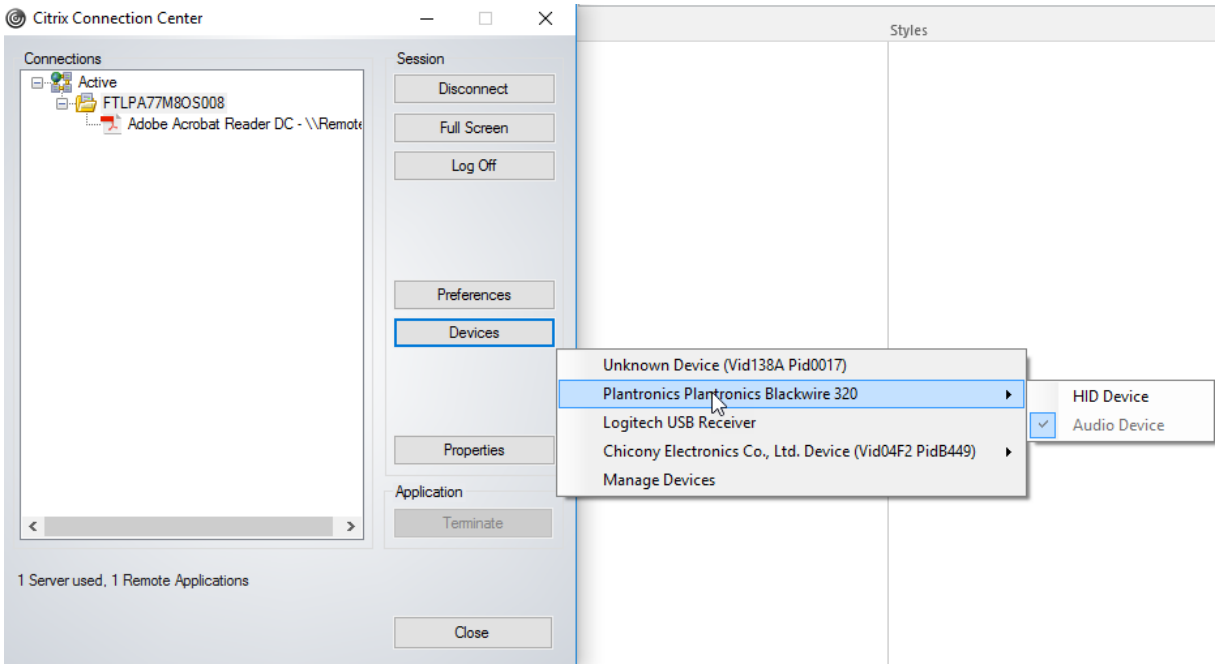
5. Fügen Sie im Textfeld **USB-Geräteregeln** das USB-Gerät hinzu, das zugelassen oder abgelehnt werden soll.
   Beispiel: `ALLOW: vid=047F pid= C039 split=01 intf=00,03`: Schnittstellen 00 und 03 sind zugelassen, andere werden beschränkt.
6. Klicken Sie auf **Anwenden** und **OK**.

In einer Desktopsitzung werden per Splitting aufgeteilte USB-Geräte im Desktop Viewer unter **Geräte** angezeigt. Darüber hinaus werden aufgeteilte USB-Geräte unter **Einstellungen** > **Geräte** angezeigt.



> **Hinweis:**
>
> Wenn Sie ein USB-Verbundgeräte für die generische USB-Umleitung aufteilen, müssen Sie das Gerät im Desktop Viewer oder Connection Center auswählen, um das Gerät umzuleiten.

In einer Anwendungssitzung werden per Splitting aufgeteilte USB-Geräte im **Connection Center** angezeigt.



In der folgenden Tabelle werden Verhaltensszenarien erläutert, wenn eine USB-Schnittstelle zugelassen oder abgelehnt wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Zulassen einer Schnittstelle:

Split	Schnittstelle	Aktion
TRUE	Gültige Zahl 0 -n	Angegebene Schnittstelle zulassen
TRUE	Ungültige Zahl	Alle Schnittstellen zulassen
FALSE	Beliebiger Wert	Generisches USB von übergeordnetem Gerät zulassen
Nicht angegeben	Beliebiger Wert	Generisches USB von übergeordnetem Gerät zulassen

Beispielsweise gibt SplitDevices - *true* an, dass alle Geräte durch Splitting aufgeteilt sind.

Ablehnen einer Schnittstelle:

Split	Schnittstelle	Aktion
TRUE	Gültige Zahl 0 -n	Angegebene Schnittstelle ablehnen
TRUE	Ungültige Zahl	Alle Schnittstellen ablehnen
FALSE	Beliebiger Wert	Generisches USB von übergeordnetem Gerät ablehnen
Nicht angegeben	Beliebiger Wert	Generisches USB von übergeordnetem Gerät ablehnen

Beispielsweise gibt SplitDevices - *false* an, dass Geräte nicht mit der angegebenen Schnittstellenzahl aufgeteilt sind.

Beispiel: *MyPlantronics* headset

Schnittstellenzahl:

- Schnittstellenklasse für Audio - 0
- Schnittstellenklasse für HID - 3

Beispielregeln für *MyPlantronics* headset:

- ALLOW: `vid=047F pid= C039 split=01 intf=00,03 /Allowed 00 and 03 interface, restrict others`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- DENY: `vid=047F pid= C039 split=01 intf=00,03 / deny 00 and 03`

Einschränkung:

Citrix empfiehlt, Schnittstellen für eine Webcam nicht per Splitting aufzuteilen. Als Workaround können Sie das Gerät über die generische USB-Umleitung an ein einzelnes Gerät weiterleiten. Verwenden Sie zur Leistungsverbesserung den optimierten virtuellen Kanal.

DPI-Skalierung

Die Citrix Workspace-App gestattet die Steuerung der Sitzungsauflösung durch das Betriebssystem.

Sie können in einer Sitzung einen hohen DPI-Wert anwenden. Dieses Feature ist jedoch standardmäßig deaktiviert. Das bedeutet, dass die Sitzungsskalierung der Auflösung des Betriebssystems folgt.

Sie können die DPI-Skalierung mit den folgenden Optionen konfigurieren:

1. Administrative Gruppenrichtlinienobjektvorlage (Konfiguration pro Maschine)
2. Erweiterte Einstellungen (Konfiguration pro Benutzer)

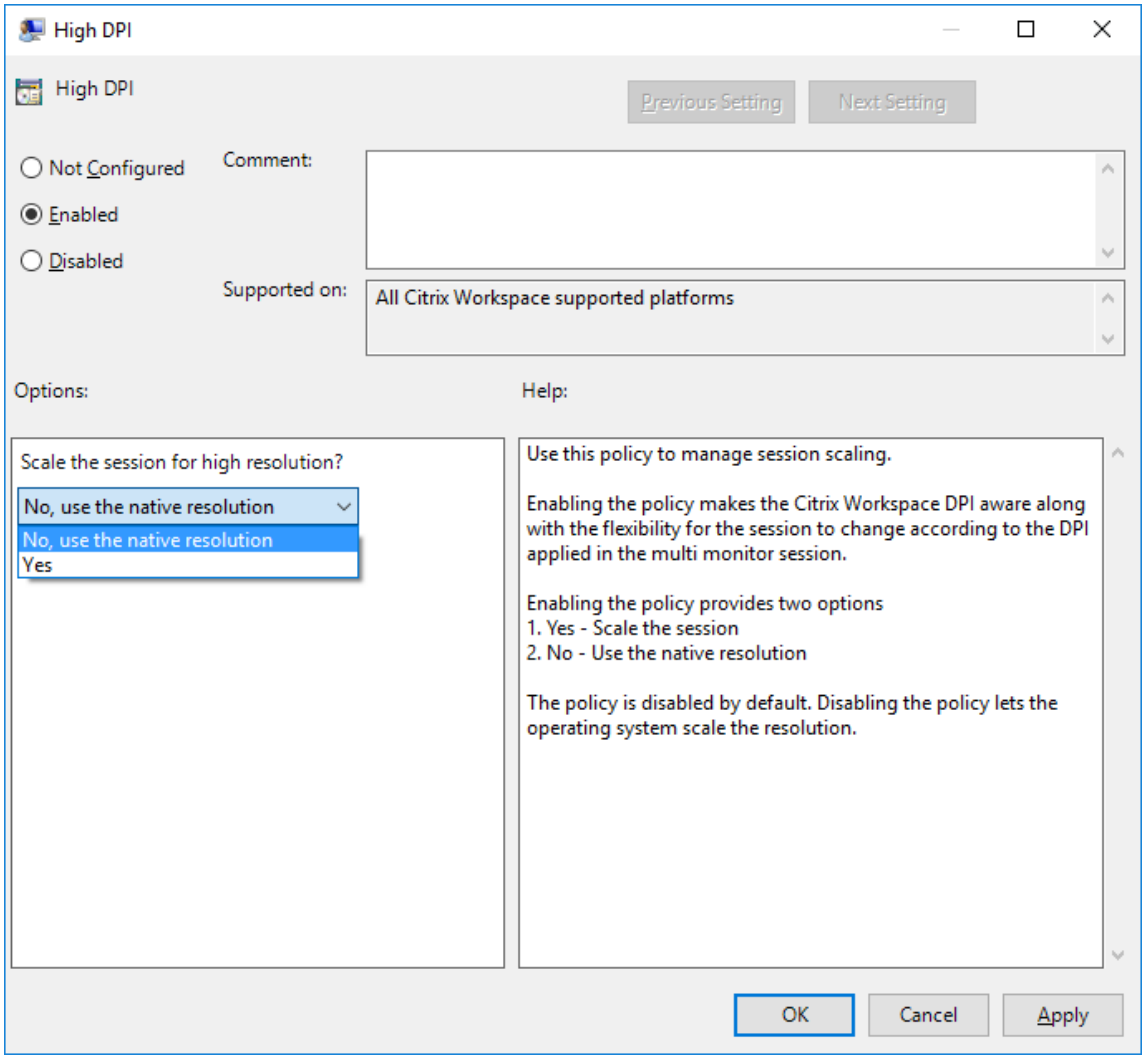
Einschränkungen:

- Auch wenn dieses Feature aktiviert ist, wurde eine leichte Unschärfe im Desktop Viewer beobachtet.
- Wenn Sie in einer Sitzung die DPI-Einstellungen ändern und die Sitzung neu starten, ist die Größe des Sitzungsfensters möglicherweise nicht angemessen. Um das Problem zu umgehen, ändern Sie die Größe des Sitzungsfensters.

DPI-Skalierung mit der administrativen Gruppenrichtlinienobjektvorlage konfigurieren:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen**> **Citrix Komponenten** > **Citrix Workspace** > **DPI**
3. Wählen Sie die Richtlinie **Hoher DPI-Wert** aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Wählen Sie eine der folgenden Optionen:

   a) Ja - Gibt an, dass ein hoher DPI-Wert in einer Sitzung angewendet wird.
   b) Nein, native Auflösung verwenden - Gibt an, dass die Auflösung vom Betriebssystem festgelegt wird.

5. Klicken Sie auf **Anwenden und OK**.
6. Führen Sie an der Befehlszeile den Befehl `gpupdate /force` aus, um die Änderungen anzuwenden.

Konfiguration von DPI-Skalierung über die grafische Benutzeroberfläche:

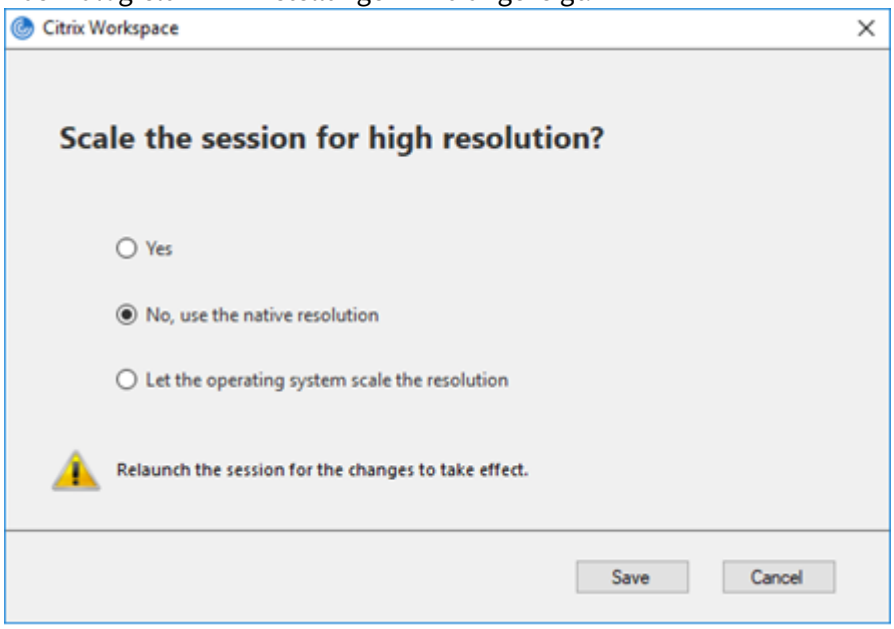
> **Hinweis:**
>
> Sie können die Seite "Erweiterte Einstellungen", die über das Symbol der Citrix Workspace-App für Windows im Infobereich verfügbar ist, ganz oder teilweise ausblenden. Weitere Informatio-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> nen finden Sie unter Erweiterte Einstellungen.

1. Klicken Sie mit der rechten Maustaste im Infobereich auf das Citrix Workspace-App-Symbol.
2. Wählen Sie **Erweiterte Einstellungen** und klicken Sie auf **DPI-Einstellungen**.

   Das Dialogfeld DPI-Einstellungen wird angezeigt.



3. Wählen Sie eine der folgenden Optionen:

   a) Ja - Gibt an, dass ein hoher DPI-Wert in einer Sitzung angewendet wird.
   b) Nein, native Auflösung verwenden - Gibt an, dass die Citrix Workspace-App den DPI-Wert auf dem VDA erkennt und ihn anwendet.
   c) Betriebssystem die Auflösung skalieren lassen − Standardmäßig ist diese Option ausgewählt. Damit kann Windows die DPI-Skalierung verarbeiten. Diese Option bedeutet auch, dass die Richtlinie “Hoher DPI-Wert”deaktiviert ist.

4. Klicken Sie auf **Speichern**.
5. Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

DPI-Skalierungsoptionen

Es gibt drei mögliche Einstellungen für die DPI-Skalierung in der Citrix Workspace-App: Skaliert, Nicht skaliert und Betriebssystemskalierung. Die Anwendungsfälle für die verschiedenen Einstellungen sind wie folgt.

Skaliert:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bei aktivierter Skalierung wird die Auflösung im VDA ähnlich wie bei der Betriebssystemskalierung skaliert. Diese Einstellung unterstützt jedoch gemischte DPI-Szenarien. Dies entspricht der Benutzeroberflächeneinstellung "Ja"oder der Aktivierung der Richtlinie "Hoher DPI-Wert"in der Gruppenrichtlinienobjektvorlage. Diese Einstellung eignet sich gut für gemischte DPI-Szenarien, wenn Sie eine Verbindung zu modernen VDAs herstellen. Dies ist die einzige Möglichkeit, Seamlesssitzungen zu skalieren. Die Skalierung kann zu Unschärfe in Bildern führen, insbesondere bei Text. Bei der Verbindung zu älteren VDAs (6.5 oder für Legacygrafiken konfigurierte VDAs) kann die Leistung beeinträchtigt sein. Lokaler App-Zugriff, RTOP und andere Plug-Ins, die APIs für die Bildschirmpositionierung verwenden, sind mit der Skalierung nicht kompatibel. In diesem Modus wechseln Seamless-Apps zwischen den Bildschirmen, um die korrekte Skalierung beizubehalten.
Diese Einstellung wird für Benutzer unter Windows 10 empfohlen, die eine Verbindung zu modernen VDAs herstellen. Sie unterstützt gemischte DPI-Werte ohne zusätzliche Auswirkungen auf die Serverressourcen.

Nicht skaliert:

Bei der nicht skalierten Einstellung wird die volle Auflösung aller Bildschirme in der Sitzung übermittelt. Diese Auflösungen sind nicht skaliert und können zu kleinem Text und kleinen Symbolen in Apps und Desktops führen. Dies entspricht der Benutzeroberflächeneinstellung "Nein"bei aktivierter Richtlinie "Hoher DPI-Wert"in der Gruppenrichtlinienobjektvorlage. Diese Einstellung verursacht keine Unschärfe aufgrund der Skalierung, kann jedoch zu kleinem Text und kleinen Symbolen führen. Wenn Sie eine Verbindung zu einer Desktopsitzung herstellen, kann der DPI-Wert im VDA eingestellt werden, was zur gewünschten Skalierung führt. Dies ist auf RDS-Desktops oder bei Seamlessanwendungen nicht möglich. Durch Aktivieren dieser Einstellung haben Sitzungen eine höhere Auflösung, was die Serverleistung und Skalierbarkeit beeinträchtigen kann.
Diese Einstellung wird für Desktopsitzungen empfohlen, bei denen die beste Bildqualität erforderlich ist und für die zusätzliche Serverressourcen verfügbar sind. Sie kann auch verwendet werden, wenn kleiner Text und kleine Symbole für den Benutzer kein Problem darstellen.

Betriebssystemskalierung:

Betriebssystemskalierung ist die Standardeinstellung und entspricht der Benutzeroberflächeneinstellung "Betriebssystem die Auflösung skalieren lassen". In diesem Szenario wird für die Richtlinie "Hoher DPI-Wert"die Option "Deaktiviert"festgelegt. Dadurch übernimmt das Windows-Betriebssystem die DPI-Skalierung für eine Sitzung. Die Auflösung wird auf dem VDA basierend auf dem DPI-Wert skaliert, was zu einer geringeren Auflösung als auf dem Clientgerät führt. Dies funktioniert gut für Sitzungen mit einem Bildschirm und ist effizient, wenn Sie eine Verbindung zu 6.5-VDAs oder VDAs herstellen, die für Legacygrafiken konfiguriert sind. Diese Methode unterstützt keine gemischten DPI-Werte. Alle Bildschirme müssen dieselben DPI-Werte haben, oder die Sitzung funktioniert nicht. Skalierung kann insbesondere bei Text zu unscharfer Darstellung führen. Bei Windows 10-Betriebssystemen können auch Probleme mit der Cursorgröße auftreten.
Diese Einstellung wird für Benutzer mit Windows 7-Endpunkten oder für Benutzer empfohlen, die

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

eine Verbindung zu Legacy-VDAs herstellen. Sie kann auch unter Windows 10 verwendet werden, wenn keine gemischten DPI-Werte vorliegen.

Virtuelles Anzeigelayout

Mit diesem Feature können Sie ein virtuelles Anzeigelayout für den Remotedesktop festlegen, mit dem ein Clientbildschirm virtuell in bis zu acht Bildschirme aufgeteilt werden kann. Sie können die virtuellen Bildschirme auf der Registerkarte **Bildschirmlayout** im Desktop Viewer konfigurieren. Dort können Sie horizontale oder vertikale Linien ziehen, um den Bildschirm in virtuelle Bildschirme zu unterteilen. Der Bildschirm wird entsprechend den angegebenen Prozentsätzen der Auflösung des Clientbildschirms aufgeteilt.

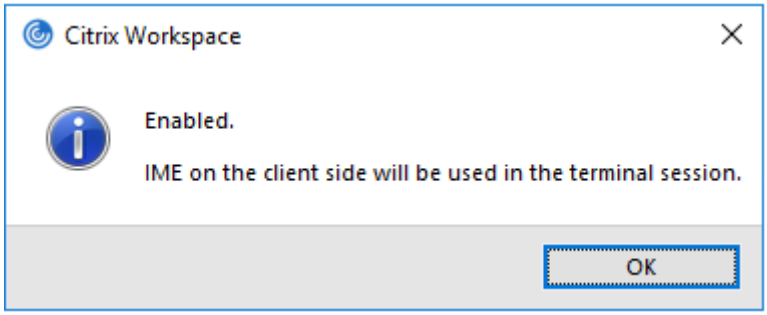
Sie können für die virtuellen Bildschirme eine DPI festlegen, die für die DPI-Skalierung bzw. DPI-Anpassung verwendet wird. Ändern Sie nach dem Anwenden eines virtuellen Bildschirmlayouts die Größe der Sitzung oder stellen Sie erneut eine Verbindung her.

Die Konfiguration gilt nur für Desktopsitzungen mit einem Bildschirm im Vollbildmodus. Sie hat keine Auswirkungen auf veröffentlichte Anwendungen. Diese Konfiguration gilt für alle nachfolgenden Verbindungen von diesem Client.

Generischer Client-IME (Eingabemethoden-Editor)

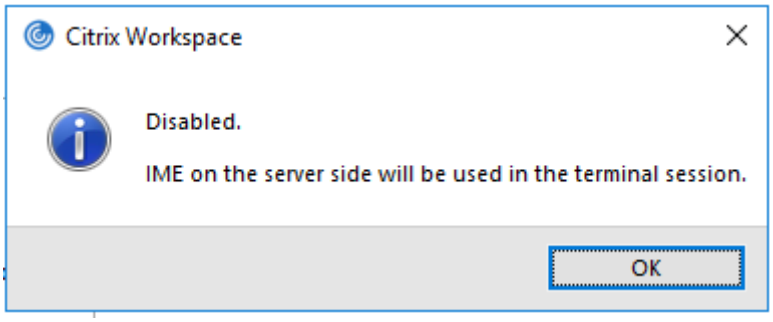
Konfigurieren eines generischen Client-IME über die Befehlszeilenschnittstelle:

- Führen Sie den Befehl `wfica32.exe /localime:on` im Citrix Workspace-App-Installationsordner `C:\Program Files (x86)\Citrix\ICA Client` aus, um den generischen Client-IME zu aktivieren.



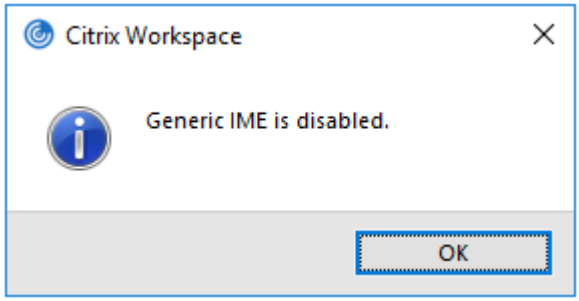
- Führen Sie den Befehl `wfica32.exe /localime:off` im Citrix Workspace-App-Installationsordner `C:\Program Files (x86)\Citrix\ICA Client` aus, um den generischen Client-IME zu deaktivieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

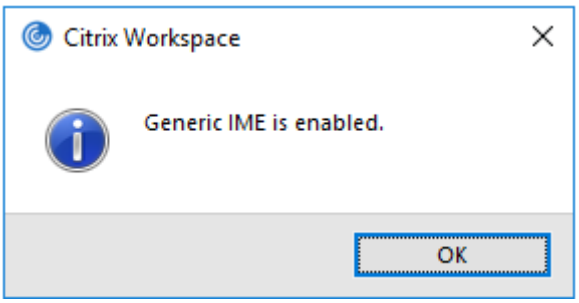


> **Hinweis:**
>
> Sie können mit der Befehlszeilenoption `wfica32.exe /localime:on` den generischen Client-IME und die Tastaturlayoutsynchronisierung aktivieren.

- Führen Sie den Befehl `wfica32.exe /localgenericime:off` im Citrix Workspace-App-Installationsordner `C:\Program Files (x86)\Citrix\ICA Client` aus, um den generischen Client-IME zu deaktivieren. Dieser Befehl hat keine Auswirkungen auf die Einstellungen für die Tastaturlayoutsynchronisierung.



Wenn Sie den generischen Client-IME über die Befehlszeilenschnittstelle deaktiviert haben, können Sie das Feature durch Ausführen des Befehls `wfica32.exe /localgenericime:on` wieder aktivieren.



Ein-/Ausschalten:

Die Citrix Workspace-App unterstützt das Ein- und Ausschalten dieses Features. Sie können das Feature durch Ausführen des Befehls `wfica32.exe /localgenericime:on` ein- und ausschalten. Die Einstellungen für die Tastaturlayoutsynchronisierung haben jedoch Vorrang vor der

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ein-/Ausschaltfunktion. Wenn die Tastaturlayoutsynchronisierung auf **Aus** festgelegt ist, kann der generische Client-IME nicht durch Ein-/Ausschalten aktiviert werden.

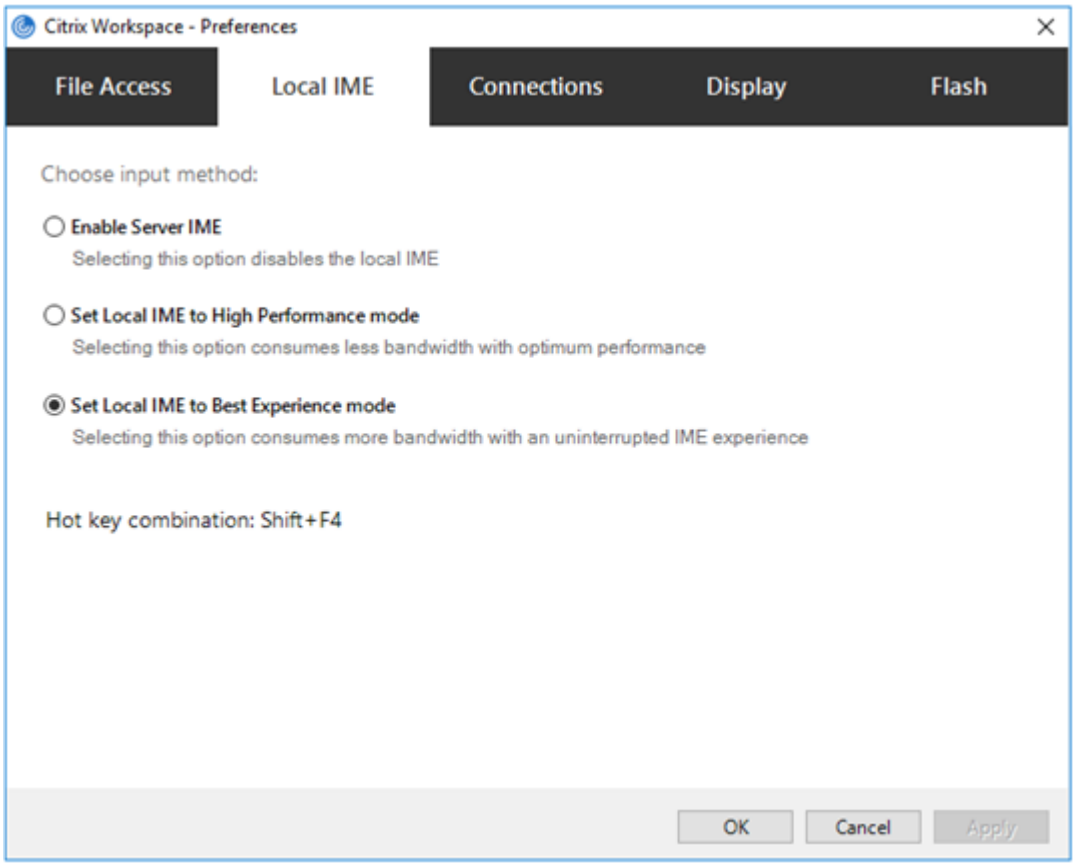
Konfigurieren eines generischen Client-IME über die grafische Benutzeroberfläche:

Der generische Client-IME erfordert VDA-Version 7.13 oder höher.

Das generische Client-IME-Feature kann durch Aktivieren der Tastaturlayoutsynchronisierung aktiviert werden. Weitere Informationen finden Sie unter Tastaturlayoutsynchronisierung.

Die Citrix Workspace-App ermöglicht das Konfigurieren verschiedener Optionen für den generischen Client-IME. Entsprechend Ihrer Anforderungen und der Nutzung können Sie eine der Optionen auswählen.

1. Klicken Sie in einer aktiven Anwendungssitzung mit der rechten Maustaste auf das Citrix Workspace-App-Symbol im Infobereich und wählen Sie **Connection Center**.
2. Wählen Sie **Einstellungen** und **Lokaler IME**.



Für die Unterstützung verschiedener IME-Modi sind die folgenden Optionen verfügbar:

1. **Server-IME aktivieren** –Deaktiviert den lokalen IME und nur die auf dem Server festgelegten Sprachen können verwendet werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. **Lokalen IME auf Hochleistungsmodus einstellen** –Verwendet den lokalen IME mit beschränkter Bandbreite. Diese Option schränkt die Funktionalität des Kandidatenfensters ein.
3. **Lokalen IME-Modus für beste Erfahrung einstellen** –Verwendet den lokalen IME mit optimaler Benutzerfreundlichkeit. Diese Option verbraucht hohe Bandbreite. Diese Option ist standardmäßig ausgewählt, wenn der generische Client-IME aktiviert ist.

Die Einstellungsänderung wird nur in der aktuellen Sitzung angewendet.

Tastenkombinationen mit einem Registrierungs-Editor konfigurieren:

Wenn der generische Client-IME aktiviert ist, können Sie mit der Tastenkombination **Umschalt+F4** verschiedene IME-Modi auswählen. Die verschiedenen Optionen für die IME-Modi werden oben rechts in der Sitzung angezeigt.

Standardmäßig ist die Tastenkombination für den generischen Client-IME deaktiviert.

Navigieren Sie im Registrierungs-Editor zu `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys`.

Wählen Sie **AllowHotKey** und ändern Sie den Standardwert in 1.

Einschränkungen:

- Der generische Client-IME unterstützt keine UWP-Apps (Universelle Windows-Plattform-Anwendungen) wie Suchbenutzeroberfläche und Edge-Browser des Windows 10-Betriebssystems. Verwenden Sie als Workaround den Server-IME.
- Der generische Client-IME wird für Internet Explorer Version 11 im **geschützten Modus** nicht unterstützt. Als Workaround können Sie den geschützten Modus unter **Internetoptionen** deaktivieren. Klicken Sie hierfür auf **Sicherheit** und deaktivieren Sie das Kontrollkästchen **Geschützten Modus aktivieren**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

H.265-Videocodierung

Die Citrix Workspace-App unterstützt die Verwendung des H.265-Videocodecs für die Hardwarebeschleunigung von Remote-Grafiken und -Videos. Um dieses Feature zu nutzen, muss es sowohl auf dem VDA als auch in der Citrix Workspace-App unterstützt und aktiviert sein. Wenn die GPU auf dem Endpunkt H.265-Decodierung über die DXVA-Schnittstelle nicht unterstützt, werden die Einstellungen der Richtlinie "H265-Decodierung für Grafiken"ignoriert und die Sitzung greift auf den H.264-Videocodec zurück.

Voraussetzungen:

1. VDA 7.16 oder höher.
2. Aktivieren Sie auf dem VDA die Richtlinie **Optimierung für 3D-Grafikworkload**.
3. Aktivieren Sie auf dem VDA die Richtlinie **Hardwarecodierung für Videocodec verwenden**.

> **Hinweis:**
>
> H.265-Codierung wird nur von der NVIDIA-GPU unterstützt.

Dieses Feature ist in der Citrix Workspace-App für Windows standardmäßig **deaktiviert**.

Citrix Workspace-App für die Verwendung von H.265-Videocodierung mit der administrativen Gruppenrichtlinienobjektvorlage von Citrix konfigurieren:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Benutzererfahrung**.
3. Wählen Sie die Richtlinie **H265-Decodierung für Grafiken**.
4. Wählen Sie **Aktiviert**.
5. Klicken Sie auf **Anwenden** und **OK**.

H.265-Videocodierung mit dem Registrierungs-Editor konfigurieren:

H.265-Videocodierung in einem nicht in eine Domäne eingebundenen Netzwerk auf einem 32-Bit-Betriebssystem aktivieren:

1. Starten Sie den Registrierungs-Editor, indem Sie den Befehl "regedit"ausführen.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Graphics Engine`.
3. Erstellen Sie einen DWORD-Schlüssel mit dem Namen **EnableH265** und legen Sie seinen Wert auf 1 fest.

H.265-Videocodierung in einem nicht in eine Domäne eingebundenen Netzwerk auf einem 64-Bit-Betriebssystem aktivieren:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Starten Sie den Registrierungs-Editor, indem Sie den Befehl "regedit"ausführen.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine`.
3. Erstellen Sie einen DWORD-Schlüssel mit dem Namen EnableH265 und legen Sie seinen Wert auf 1 fest.

Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

> **Hinweis:**
>
> - Wenn die Richtlinie **Hardwarebeschleunigung für Grafiken** in der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App für Windows deaktiviert ist, werden die Einstellungen der Richtlinie **H265-Decodierung für Grafiken** ignoriert und das Feature funktioniert nicht.
> - Führen Sie das Tool "HDX Monitor 3.x"aus, um festzustellen, ob der H.265-Videoencoder in den Sitzungen aktiviert ist. Weitere Informationen zu HDX Monitor 3.x finden Sie im Knowledge Center-Artikel CTX135817.

Tastaturlayout und Sprachenleiste

Tastaturlayout

> **Hinweis:**
>
> Sie können die über das Citrix Workspace-App-Symbol im Infobereich verfügbare Seite "Erweiterte Einstellungen"ganz oder teilweise ausblenden. Weitere Informationen finden Sie unter Erweiterte Einstellungen.

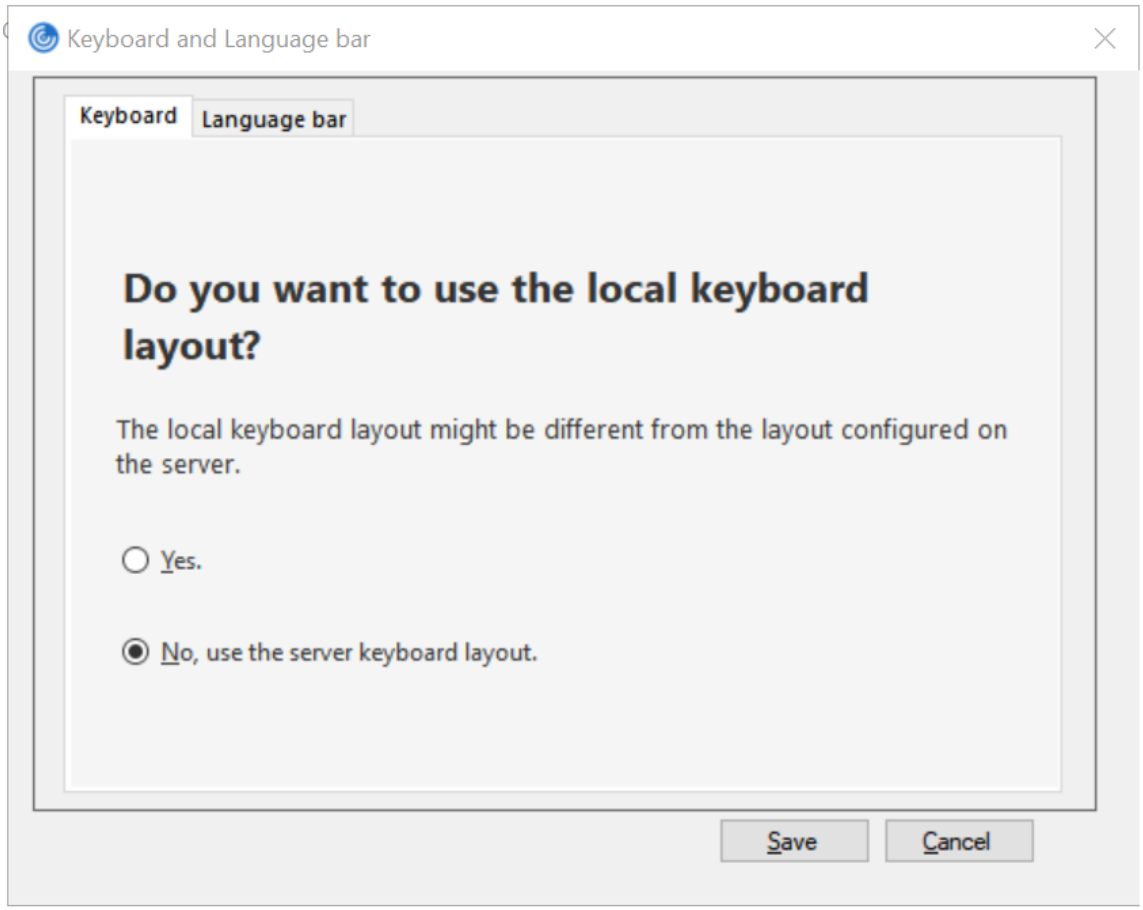
Die Tastaturlayoutsynchronisierung ermöglicht es Benutzern, zwischen bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Das Feature ist in der Standardeinstellung deaktiviert.

Aktivieren der Tastaturlayoutsynchronisierung:

1. Klicken Sie auf das Infobereichsymbol der Citrix Workspace-App und wählen Sie **Erweiterte Einstellungen** > **Tastatur und Sprachenleiste**.

   Das Dialogfeld Tastatur und Sprachenleiste wird angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Wählen Sie eine der folgenden Optionen:

   - Ja - Gibt an, dass das lokale Tastaturlayout in einer Sitzung verwendet wird.
   - Nein, Tastaturlayout des Servers verwenden - Gibt an, dass das Tastaturlayout auf dem VDA in einer Sitzung verwendet wird. Mit dieser Option wird das lokale Tastaturlayoutfeature deaktiviert.

3. Klicken Sie auf **Speichern**.

Sie können die Tastaturlayoutsynchronisierung auch über die Befehlszeile steuern, indem Sie den Befehl `wfica32:exe /localime:on` oder `wfica32:exe /localime:off` im Installationsordner `C:\Program files (x86)\Citrix\ICA Client` der Citrix Workspace-App für Windows ausführen.

Wenn Sie die lokale Tastaturlayoutoption verwenden, wird der Client-IME (Eingabemethoden-Editor) aktiviert. Wenn Benutzer, die Japanisch, Chinesisch oder Koreanisch verwenden, den Server-IME bevorzugen, müssen sie die Option für das lokale Tastaturlayout durch Auswählen von **Nein** deaktivieren oder den Befehl `wfica32:exe /localime:off` ausführen. Wenn sie eine Verbindung mit der nächsten Sitzung herstellen, wird das Tastaturlayout des Remoteservers wiederhergestellt.

Gelegentlich wird der Wechsel des Clienttastaturlayouts nicht in einer aktiven Sitzung wirksam.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sie beheben das Problem, indem Sie sich von der Citrix Workspace-App ab- und dann wieder anmelden.

Ausblenden der Benachrichtigung beim Tastaturlayoutwechsel:

Durch die Benachrichtigung beim Wechseln des Tastaturlayouts erfahren Sie, dass die VDA-Sitzung das Tastaturlayout ändert. Der Wechsel des Tastaturlayouts dauert ungefähr zwei Sekunden. Wenn Sie die Benachrichtigung ausblenden, warten Sie einige Zeit, bevor Sie mit der Eingabe beginnen, um die Eingabe falscher Zeichen zu vermeiden.

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Ausblenden der Benachrichtigung beim Tastaturlayoutwechsel mit dem Registrierungs-Editor:

1. Starten Sie den Registrierungs-Editor und navigieren Sie zu `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Erstellen Sie einen neuen Zeichenfolgenwertschlüssel mit dem Namen **HideNotificationWindow**.
3. Legen Sie den DWORD-Wert auf **1** fest.
4. Klicken Sie auf **OK**.
5. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Einschränkungen:

- Für Remoteanwendungen, die mit erhöhten Rechten ausgeführt werden (z. B. wenn Sie mit der rechten Maustaste auf ein Anwendungssymbol klicken und "Als Administrator ausführen" wählen), kann keine Tastaturlayoutsynchronisierung erfolgen. Als Workaround ändern Sie das Tastaturlayout manuell auf der Serverseite (VDA) oder deaktivieren Sie die Benutzerkontensteuerung (UAC).
- Wenn der Benutzer für das Tastaturlayout auf dem Client ein Layout wählt, das nicht auf dem Server unterstützt wird, dann wird das Feature für die Tastaturlayoutsynchronisierung aus Sicherheitsgründen deaktiviert, da ein unbekanntes Tastaturlayout als mögliches Sicherheitsrisiko behandelt wird. Um das Feature für die Tastaturlayoutsynchronisierung wiederherzustellen, muss der Benutzer sich von der Sitzung abmelden und wieder anmelden.
- In einer RDP-Sitzung können Sie das Tastaturlayout nicht mit der Tastenkombination Alt + Umschalt ändern. Als Workaround können Sie das Tastaturlayout mit der Sprachenleiste in der

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

RDP-Sitzung ändern.

- Dieses Feature ist in Windows Server 2016 aufgrund eines Drittanbieterproblems deaktiviert, was u. U. ein Risiko für die Leistung ist. Das Feature kann mit einer Registrierungseinstellung auf dem VDA aktiviert werden: in `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme`. Fügen Sie einen neuen Schlüssel namens **DisableKeyboardSync** hinzu und legen Sie den Wert auf 0 fest.

Sprachenleiste

Auf der Sprachenleiste wird die bevorzugte Eingabesprache von Sitzungen angezeigt. In früheren Releases konnten Sie diese Einstellung nur über Registrierungsschlüssel auf dem VDA ändern. Ab Citrix Receiver für Windows 4.11 können Sie die Einstellungen im Dialogfeld **Erweiterte Einstellungen** ändern. Die Sprachenleiste wird in Sitzungen standardmäßig angezeigt.

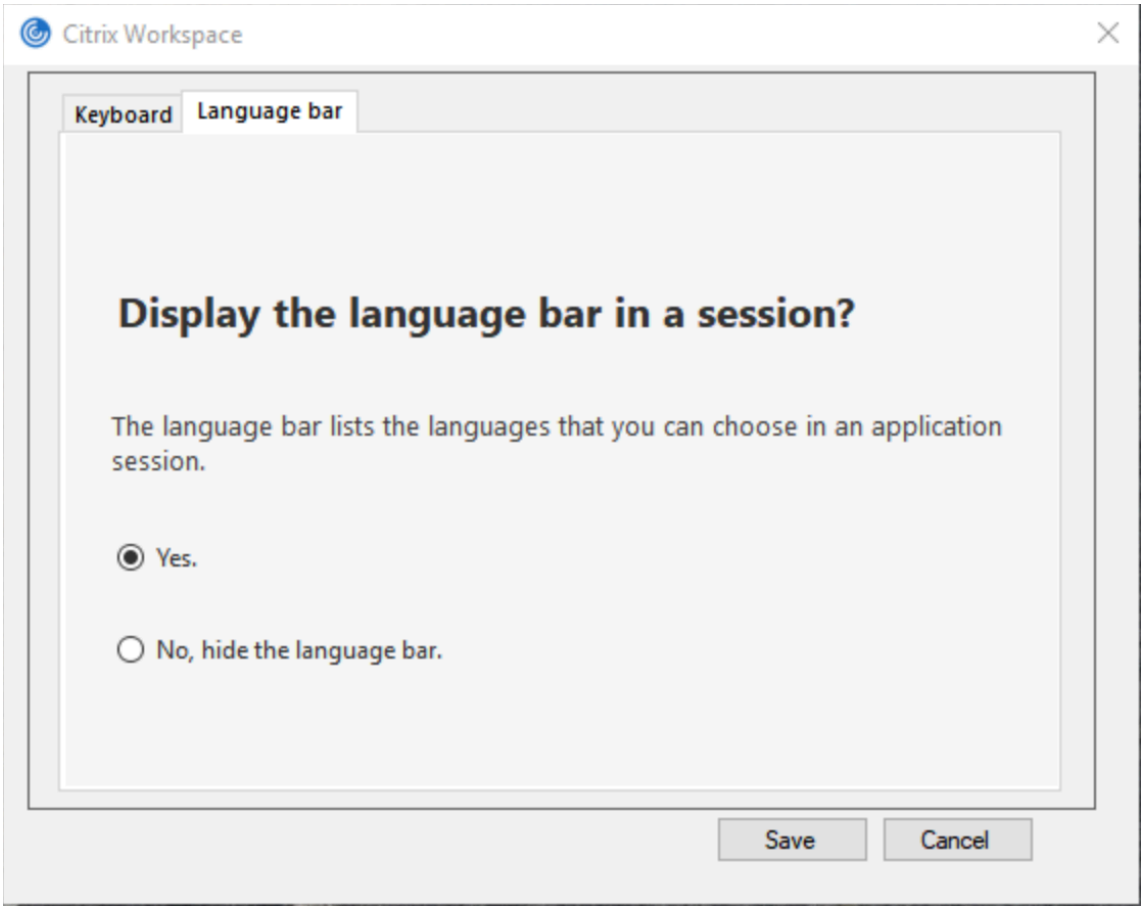
> **Hinweis:**
>
> Das Feature ist in Sitzungen verfügbar, die unter einem VDA der Version 7.17 und höher ausgeführt werden.

Anzeigen/Ausblenden der Remote-Sprachenleiste:

1. Klicken Sie im Infobereich mit der rechten Maustaste auf das Symbol der Citrix Workspace-App und wählen Sie **Erweiterte Einstellungen**.
2. Wählen Sie **Tastatur und Sprachenleiste**.
3. Wählen Sie die Registerkarte **Sprachenleiste**.
4. Wählen Sie eine der folgenden Optionen:
   a) Ja - Gibt an, dass die Sprachenleiste in einer Sitzung angezeigt wird.
   b) Nein, Sprachenleiste ausblenden − Zeigt an, dass die Sprachenleiste in einer Sitzung ausgeblendet ist.
5. Klicken Sie auf **Speichern**.

   Die Änderungen werden sofort wirksam.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Hinweis:**
>
> - Sie können die Einstellungen in einer aktiven Sitzung ändern.
> - Die Remotesprachenleiste wird in Sitzungen mit nur einer Eingabesprache nicht angezeigt.

Ausblenden der Registerkarte "Sprachenleiste"von der Seite "Erweiterte Einstellungen":

Sie können die Registerkarte "Sprachenleiste"von der Seite **Erweiterte Einstellungen** über die Registrierung ausblenden.

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LocalIME`.
3. Erstellen Sie den DWORD-Wertschlüssel **ToggleOffLanguageBarFeature** und legen Sie ihn auf **1** fest, um die Option für die Sprachenleiste auf der Seite "Erweiterte Einstellungen" auszublenden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

USB-Unterstützung

Mit der USB-Unterstützung können Sie mit zahlreichen USB-Geräten interagieren, wenn sie mit Citrix Virtual Apps and Desktops und Citrix DaaS verbunden sind. Sie können USB-Geräte an die Geräte anschließen und mit Remoting der Geräte stehen sie auf dem virtuellen Desktop zur Verfügung. Zu den USB-Geräten, die für Remoting verfügbar sind, gehören Flashlaufwerke, Smartphones, PDAs, Drucker, Scanner, MP3 Player, Sicherheitsgeräte und Tablets. Benutzer von Desktop Viewer können mit einer Einstellung auf der Symbolleiste steuern, ob USB-Geräte für Citrix Virtual Apps and Desktops und Citrix DaaS verfügbar sind.

Isochrone Features in USB-Geräten wie Webcams, Mikrofonen, Lautsprechern und Headsets werden in typischen LAN-Umgebungen mit geringer Latenz und hoher Geschwindigkeit unterstützt. Dadurch können diese Geräte mit Programmpaketen wie Microsoft Office Communicator und Skype verwendet werden.

Die folgenden Gerätetypen werden direkt in Sitzungen mit virtuellen Apps und Desktops unterstützt und verwenden daher keine USB-Unterstützung:

- Tastaturen
- Mäuse
- Smartcards

USB-Spezialgeräte (beispielsweise Bloomberg-Tastaturen und 3D-Maus) können für die USB-Unterstützung konfiguriert werden. Weitere Informationen zur Konfiguration von Bloomberg-Tastaturen finden Sie unter
Konfigurieren von Bloomberg-Tastaturen.

Weitere Informationen zur Konfiguration von Richtlinienregeln für andere USB-Spezialgeräte finden Sie im Knowledge Center-Artikel
CTX122615.

In der Standardeinstellung werden bestimmte Typen von USB-Geräten nicht für Remoting über Citrix Virtual Apps and Desktops und Citrix DaaS unterstützt. Beispielsweise könnte ein Benutzer eine Netzwerkkarte über internes USB mit der Systemplatine verbunden haben. Remoting wäre bei einem solchen Gerät nicht angebracht. Die folgenden USB-Gerätetypen werden standardmäßig nicht in Sitzungen mit virtuellen Apps und Desktops unterstützt:

- Bluetooth-Dongle
- Integrierte Netzwerkkarten
- USB-Hubs
- USB-Grafikadapter

Remoting ist möglich für USB-Geräte, die mit einem Hub verbunden sind, jedoch nicht für den Hub selbst.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Die folgenden USB-Gerätetypen werden standardmäßig nicht in einer Citrix Virtual Apps-Sitzung unterstützt:

- Bluetooth-Dongle
- Integrierte Netzwerkkarten
- USB-Hubs
- USB-Grafikadapter
- Audiogeräte
- Massenspeichergeräte

Funktionsweise der USB-Unterstützung:

Wenn ein Benutzer ein USB-Gerät anschließt, wird es mit der USB-Richtlinie überprüft, und wenn das Gerät zulässig ist, erfolgt ein Remoting zum virtuellen Desktop. Wenn das Gerät von der Standardrichtlinie abgelehnt wird, steht es nur auf dem lokalen Desktop zur Verfügung.

Wenn ein Benutzer ein USB-Gerät anschließt, wird eine Meldung über den Anschluss eines neuen Geräts angezeigt. Der Benutzer wählt die Geräte, für die ein Remoting zum virtuellen Desktop erfolgen soll, bei jeder Verbindung in der Liste aus. Der Benutzer kann die USB-Unterstützung auch so konfigurieren, dass für alle USB-Geräte, die vor oder während einer Sitzung angeschlossen werden, automatisch ein Remoting zu dem virtuellen Desktop erfolgt, der den Fokus hat.

Massenspeichergeräte

Ausschließlich für Massenspeichergeräte ist nicht nur die USB-Unterstützung sondern auch der Remotezugriff über die Clientlaufwerkzuordnung verfügbar, die Sie in der Richtlinie **Remoting von Clientgeräten** > **Clientlaufwerkzuordnung** der Citrix Workspace-App für Windows konfigurieren. Wenn diese Richtlinie angewendet wird, werden die Laufwerke auf dem Benutzergerät automatisch Laufwerkbuchstaben auf dem virtuellen Desktop zugeordnet, wenn sich Benutzer anmelden. Die Laufwerke werden als freigegebene Ordner mit zugeordneten Laufwerksbuchstaben angezeigt.

Die Hauptunterschiede zwischen den beiden Typen der Remotingrichtlinie sind:

Feature	Clientlaufwerkzuordnung	USB-Unterstützung
Diese Option ist in der Standardeinstellung aktiviert.	Ja	Nein
Konfigurierbare Leserechte	Ja	Nein
Sicheres Entfernen des Geräts in einer Sitzung	Nein	Ja, wenn der Benutzer im Infobereich auf Hardware sicher entfernen klickt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenn die Richtlinien für die generische USB-Umleitung und die Clientlaufwerkzuordnung aktiviert sind und ein Massenspeichergerät vor dem Sitzungsstart angeschlossen wird, wird es zuerst mit der Clientlaufwerkzuordnung umgeleitet, bevor eine Umleitung mit der USB-Unterstützung erwägt wird. Wenn das Gerät nach dem Sitzungsstart angeschlossen wird, wird die Umleitung mit der USB-Unterstützung vor der Clientlaufwerkzuordnung erwogen.

In der Standardeinstellung zulässige USB-Geräteklassen:

Verschiedene Klassen von USB-Geräten werden von den USB-Standardrichtlinienregeln in der Standardeinstellung zugelassen.

Auch wenn sie in dieser Liste sind, stehen manche Klassen nur nach zusätzlicher Konfiguration für das Remoting in Sitzungen mit virtuellen Apps und Desktops zur Verfügung. Es wird im Folgenden darauf hingewiesen.

- **Audio (Geräteklasse 01):** Umfasst Audioeingabegeräte (Mikrofone), Audioausgabegeräte und MIDI-Controller. Moderne Audiogeräte verwenden im Allgemeinen isochrone Transfers, die von XenDesktop 4 oder höher unterstützt werden. Audio (Geräteklasse 01) ist für Citrix Virtual Apps nicht relevant, da Geräte dieser Klasse für das Remoting in Citrix Virtual Apps mit USB-Unterstützung nicht verfügbar sind.

> **Hinweis:**
>
> Für manche Spezialgeräte (z. B. VOIP-Telefone) ist eine zusätzliche Konfiguration erforderlich. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX123015.

- **PID (Physical Interface Devices) (Geräteklasse 05):** Diese Geräte ähneln HIDs (Human Interface Devices), bieten jedoch im Allgemeinen Eingabe oder Feedback in Echtzeit, hierzu gehören u. a. Force-Feedback-Joysticks, Bewegungsplattformen und Force-Feedback-Endoskelette.
- **Bilder (Geräteklasse 06):** Hierzu gehören digitale Kameras und Scanner. Digitale Kameras unterstützen oft die Bilderklasse, in der Bilder mit den Protokollen PTP (Picture Transfer Protocol) oder MTP (Media Transfer Protocol) zu einem Computer oder zu einem anderen Peripheriegerät übertragen werden. Kameras können auch als Massenspeichergeräte angezeigt werden und eine Kamera kann möglicherweise über die Setupmenüs der Kamera für beide Klassen konfiguriert werden.

> **Hinweis:**
>
> Wird eine Kamera als Massenspeichergerät angezeigt, wird die Clientlaufwerkzuordnung verwendet und die USB-Unterstützung wird nicht benötigt.

- **Drucker (Geräteklasse 07):** Die meisten Drucker gehören zu dieser Klasse, obwohl einige herstellerspezifische Protokolle (Klasse ff) verwenden. Mehrfunktionsdrucker haben ggf. einen internen Hub oder sind Composite-Geräte. In beiden Fällen verwendet das Druckerelement meis-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tens die Druckerklasse und das Scanner- oder Faxelement verwendet eine andere Klasse, z. B. Bilder.

Drucker funktionieren normalerweise ohne USB-Unterstützung.

> **Hinweis**
>
> Für diese Klasse von Geräten (vor allem Drucker mit Scanfunktion) ist eine zusätzliche Konfiguration erforderlich. Anweisungen hierzu finden Sie im Knowledge Center-Artikel CTX123015.

- **Massenspeicher (Geräteklasse 08):** Die gängigsten Massenspeichergeräte sind USB-Flashlaufwerke sowie über USB angeschlossene Festplatten, CD- bzw. DVD-Laufwerke und SD/MMC-Kartenleser. Außerdem gibt es zahlreiche Geräte mit einem internen Speicher, der auch eine Massenspeicherschnittstelle darstellt, u. a. Media Player, digitale Kameras und Mobiltelefone. Massenspeicher (Geräteklasse 08) ist für Citrix Virtual Apps nicht relevant, da Geräte dieser Klasse für das Remoting in Citrix Virtual Apps mit USB-Unterstützung nicht verfügbar sind. Bekannte Unterklassen:
  - 01: Begrenzte Flashlaufwerke
  - 02: Normalerweise CD- bzw. DVD-Geräte (ATAPI/MMC-2)
  - 03: Normalerweise Bandgeräte (QIC-157)
  - 04: Normalerweise Diskettenlaufwerke (UFI)
  - 05: Normalerweise Diskettenlaufwerke (SFF-8070i)
  - 06: Die meisten Massenspeichergeräte verwenden diese SCSI-Variante

  Der Zugriff auf Massenspeichergeräte erfolgt oft über die Clientlaufwerkzuordnung und USB-Unterstützung wird daher nicht benötigt.
- **Content Security (Geräteklasse 0d):** Content-Security-Geräte erzwingen Inhaltsschutz normalerweise für die Lizenzierung oder das Management digitaler Rechte. Dongles gehören zu dieser Klasse.
- **Video (Geräteklasse 0e):** Die Videoklasse umfasst Geräte, mit denen Videos und mit Video zusammenhängendes Material manipuliert werden, u. a. Webcams, digitale Camcorder, analoge Videokonverter, einige Fernsehtuner und einige digitale Kameras, die Videostreaming unterstützen.

> **Wichtig**
>
> Die meisten Videostreaminggeräte verwenden isochrone Transfers, die von XenDesktop 4 oder höher unterstützt werden. Für manche Videogeräte (z. B. Webcams mit Bewegungserkennung) ist eine zusätzliche Konfiguration erforderlich. Anweisungen hierzu finden Sie im Knowledge Center-Artikel CTX123015.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Personal Healthcare (Geräteklasse 0f):** Hierzu gehören Geräte zur persönlichen Gesundheitspflege, u. a. Blutdruckmessgeräte, Herzfrequenzmessgeräte, Schrittzähler, Geräte zur Medikamenteneinnahmeüberwachung und Spirometer.
- **Anwendungs- und herstellerspezifisch (Geräteklasse fe und ff):** Bei vielen Geräten werden herstellerspezifische oder nicht USB-Konsortium-konforme Protokolle verwendet. Diese werden normalerweise als herstellerspezifisch (Klasse ff) ausgezeichnet.

In der Standardeinstellung nicht zugelassene USB-Geräteklassen

Die folgenden USB-Geräteklassen werden von den USB-Standardrichtlinienregeln nicht zugelassen:

- Kommunikation und CDC-Steuerung (Geräteklasse 02 und 0a): Die USB-Standardrichtlinie lässt diese Geräte nicht zu, da ein solches Gerät möglicherweise selbst die Verbindung zum virtuellen Desktop bereitstellt.
- HID (Human Interface Devices, Geräteklasse 03): Umfasst viele Eingabe- und Ausgabegeräte. Typische HIDs sind Tastaturen, Mäuse, Zeigegeräte, Grafiktabletts, Sensoren, Game Controller, Tasten und Steuerfunktionen.

  Die Unterklasse 01 wird "Boot Interface"-Klasse genannt und für Tastaturen und Maus verwendet.

  USB-Tastaturen (Klasse 03, Unterklasse 01, Protokoll 1) oder USB-Mäuse (Klasse 03, Unterklasse 01, Protokoll 2) werden von der USB-Standardrichtlinie nicht zugelassen. Begründung: Die meisten Tastaturen und Mäuse werden ohne USB-Unterstützung ausreichend gehandhabt und werden sowohl lokal als auch remote bei Verbindungen mit einem virtuellen Desktop verwendet.
- USB-Hubs (Geräteklasse 09): Mit USB-Hubs können zusätzliche Geräte am lokalen Computer angeschlossen werden. Auf diese Geräte muss nicht remote zugegriffen werden.
- Smartcard (Geräteklasse 0b): Zu Smartcardlesegeräten gehören berührungslose und Smartcard-Berührungslesegeräte sowie USB-Token mit einem eingebetteten smartcardäquivalenten Chip.

  Der Zugriff auf Smartcardlesegeräte erfolgt nicht mit Smartcard-Remoting und erfordert keine USB-Unterstützung.
- Kabellose Controller (Geräteklasse e0): Einige dieser Geräte sind u. U. unabdingbar für den Netzwerkzugang oder die Verbindung mit Peripheriegeräten wie Bluetooth-Tastaturen oder -Mäuse.

  Die USB-Standardrichtlinie lässt diese Geräte nicht zu. Es kann jedoch Geräte geben, denen Zugriff mit USB-Unterstützung gegeben werden sollte.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Verschiedene Netzwerkgeräte (Geräteklasse ef, Unterklasse 04):** Einige dieser Geräte sind u. U. unabdingbar für den Netzwerkzugang. Die USB-Standardrichtlinie lässt diese Geräte nicht zu. Es kann jedoch Geräte geben, denen Zugriff mit USB-Unterstützung gegeben werden sollte.

Für Remoting verfügbare USB-Geräteliste aktualisieren

Sie können die USB-Geräte aktualisieren, die für das Remoting zu Desktops verfügbar sind, indem Sie die Vorlagendatei für Citrix Workspace für Windows bearbeiten. Sie können so Citrix Workspace für Windows über eine Gruppenrichtlinie ändern. Die Datei ist in folgendem Installationsordner:

`\C:\Program Files\Citrix\ICA Client\Configuration\en`.

Sie können auch die Registrierung auf jedem Benutzergerät ändern und den folgenden Registrierungsschlüssel hinzufügen:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB
Type=String Name="DeviceRules"Value=
```

> **Wichtig**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Die Standardregeln für das Produkt sind an folgendem Speicherort gespeichert:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB Type=MultiSz Name="DeviceRules"Value=

Ändern Sie nicht die Produktstandardregeln.

Weitere Informationen zu den Richtlinieneinstellungen für USB-Geräte finden Sie unter Einstellungen der Richtlinie "USB-Geräte" in der Dokumentation zu Citrix Virtual Apps and Desktops.

USB-Audio konfigurieren

> **Hinweis:**
>
> - Wenn Sie die Citrix Workspace-App für Windows zum ersten Mal installieren oder aktualisieren, fügen Sie dem lokalen Gruppenrichtlinienobjekt die neuesten Vorlagendateien hinzu. Weitere Informationen über das Hinzufügen von Vorlagendateien zum lokalen Gruppenrichtlinienobjekt finden Sie unter Administrative Gruppenrichtlinienobjektvorlage. Bei

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> einem Upgrade bleiben die vorhandenen Einstellungen erhalten, während die neuesten Dateien importiert werden.
> - Dieses Feature ist nur für Citrix Virtual Apps-Server verfügbar.

USB-Audiogeräte konfigurieren:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Workspace > Benutzererfahrung** und wählen Sie **Audio über generische USB-Umleitung**.
3. Bearbeiten Sie die Einstellungen.
4. Klicken Sie auf **Anwenden** und **OK**.
5. Öffnen Sie eine Eingabeaufforderung im Administratormodus.
6. Führen Sie den Befehl `gpupdate /force` aus.

vPrefer-Start

In früheren Releases konnten Sie festlegen, dass die Instanz einer auf dem VDA installierten App (= "lokale Instanz"im vorliegenden Dokument) bevorzugt vor der veröffentlichten Anwendung gestartet werden muss, indem Sie in **Citrix Studio** das Attribut KEYWORDS:prefer="application"festlegten.

Ab Version 4.11 können Sie in einem Double-Hop-Szenario (wenn die Citrix Workspace-App auf dem VDA ausgeführt wird, der Ihre Sitzung hostet) steuern, ob die Citrix Workspace-App bevorzugt vor einer gehosteten App-Instanz die lokale Instanz einer auf dem VDA installierten Anwendung startet (sofern sie als lokale App verfügbar ist).

vPrefer ist in StoreFront 3.14 und in Citrix Virtual Desktops ab Version 7.17 verfügbar.

Wenn Sie die Anwendung starten, liest die Citrix Workspace-App die Ressourcendaten auf dem StoreFront-Server und wendet die Einstellungen auf der Grundlage des **vprefer**-Flags zum Zeitpunkt der Aufzählung an. Die Citrix Workspace-App sucht in der Windows-Registrierung auf dem VDA den Installationspfad der Anwendung und startet die lokale Instanz, sofern eine solche vorhanden ist. Andernfalls wird eine gehostete Instanz gestartet.
Wenn Sie eine Anwendung starten, die nicht auf dem VDA installiert ist, wird die gehostete Anwendung gestartet. Informationen zur Handhabung des lokalen Starts in StoreFront finden Sie unter Steuern des lokalen Starts von Anwendungen auf veröffentlichten Desktops in der Dokumentation zu Citrix Virtual Apps and Desktops.

Wenn Sie nicht möchten, dass die lokale Instanz einer Anwendung auf dem VDA gestartet wird, setzen Sie **LocalLaunchDisabled** auf dem Delivery Controller mithilfe von PowerShell auf **True**. Weitere Informationen finden Sie in der Dokumentation zu Citrix Virtual Apps and Desktops.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Das Feature beschleunigt den Anwendungsstart und bietet dadurch eine bessere Benutzererfahrung. Sie können es über die administrative GPO-Vorlage konfigurieren. Standardmäßig ist vPrefer nur in einem Double-Hop-Szenario aktiviert.

> **Hinweis:**
>
> Wenn Sie die Citrix Workspace-App zum ersten Mal installieren oder aktualisieren, fügen Sie dem lokalen Gruppenrichtlinienobjekt die neuesten Vorlagendateien hinzu. Weitere Informationen über das Hinzufügen von Vorlagendateien zum lokalen Gruppenrichtlinienobjekt finden Sie unter Administrative Gruppenrichtlinienobjektvorlage. Bei einem Upgrade bleiben die vorhandenen Einstellungen erhalten, während die neuesten Dateien importiert werden.

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Self-Service**.
3. Wählen Sie die Richtlinie **vPrefer**.
4. Wählen Sie **Aktiviert** und anschließend im Dropdownmenü neben **Apps zulassen** eine der folgenden Optionen:
    - **Alle Apps zulassen**: Mit dieser Option wird die lokale Instanz aller Apps auf dem VDA gestartet. Die Citrix Workspace-App sucht nach der installierten Anwendung (einschließlich nativer Windows-Anwendungen wie Editor, Rechner, WordPad, Eingabeaufforderung) und startet sie auf dem VDA (und nicht die gehostete App).
    - **Installierte Apps zulassen**: Mit dieser Option wird die lokale Instanz der installierten App auf dem VDA gestartet. Wenn die App nicht auf dem VDA installiert ist, wird die gehostete App gestartet. Standardmäßig ist die Option **Installierte Apps zulassen** ausgewählt, wenn die **vPrefer**-Richtlinie auf **Aktiviert** festgelegt ist. Diese Option gilt nicht für Windows-eigene Anwendungen wie Editor, Rechner usw.
    - **Netzwerk-Apps zulassen**: Durch diese Option wird die Instanz von Apps gestartet, die in einem freigegebenen Netzwerk veröffentlicht ist.
5. Klicken Sie auf **Anwenden** und **OK**.
6. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Einschränkung:

- Workspace für Web unterstützt dieses Feature nicht.

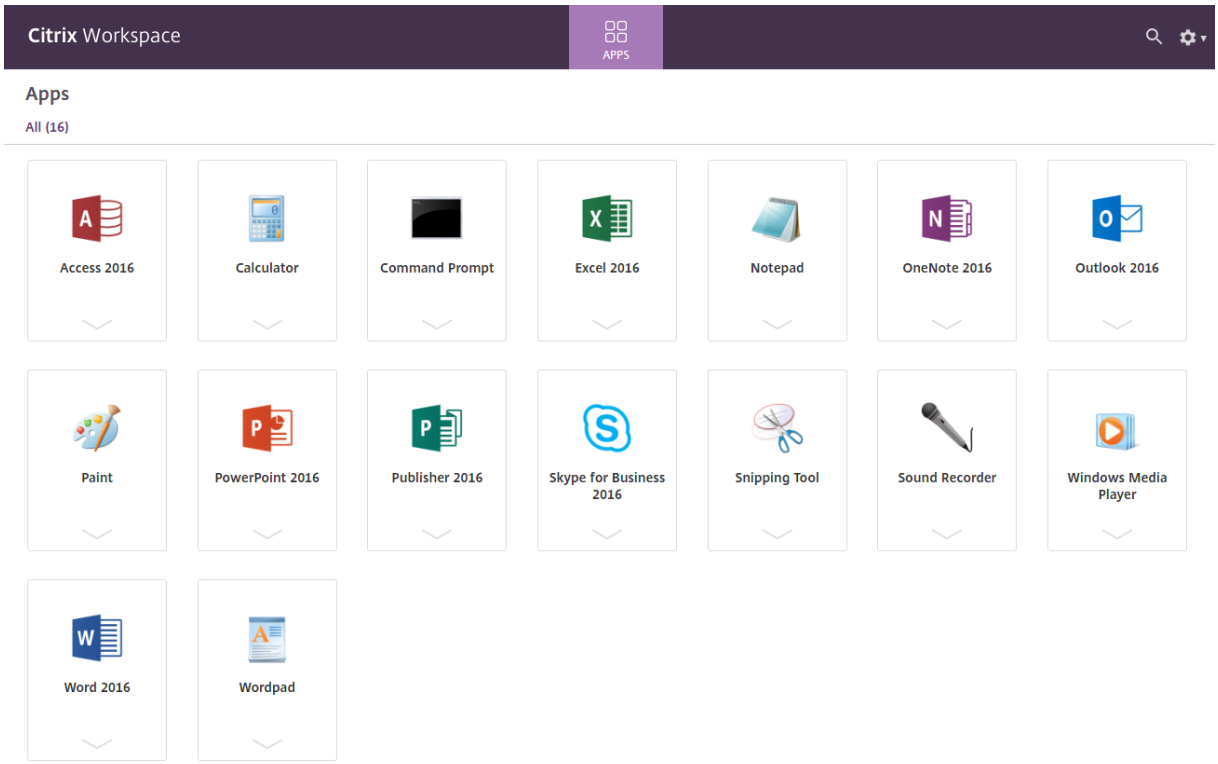
Workspacekonfiguration

Die Citrix Workspace-App für Windows unterstützt die Konfiguration von Workspaces für Abonnenten, die möglicherweise einen oder mehrere in Citrix Cloud verfügbare Dienste verwenden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Die Citrix Workspace-App zeigt nur die spezifischen Workspaceressourcen an, für die Benutzer berechtigt sind. Alle in der Citrix Workspace-App verfügbaren digitalen Workspace-Ressourcen werden vom Dienst für die Citrix Cloud Workspace-Benutzeroberfläche bereitgestellt.

Ein Workspace ist Teil einer digitalen Workspacelösung, mit der IT-Mitarbeiter von jedem Gerät aus den Zugriff auf Apps sicher bereitstellen können.
Der Screenshot ist ein Beispiel für die Workspace-Benutzeroberfläche Ihrer Abonnenten. Diese Benutzeroberfläche wird kontinuierlich weiterentwickelt und sieht möglicherweise anders aus als die, mit der Ihre Abonnenten heute arbeiten. Beispielsweise könnte oben auf der Seite "StoreFront" anstelle von "Workspace"angezeigt werden.



SaaS-Apps

Der sichere Zugriff auf SaaS-Anwendungen bietet eine einheitliche Benutzererfahrung bei der Bereitstellung veröffentlichter SaaS-Anwendungen. SaaS-Anwendungen sind mit Single Sign-On verfügbar. Administratoren können jetzt Netzwerk und Endbenutzergeräte vor Malware und Datenlecks schützen, indem sie den Zugriff auf bestimmte Websites und Websitekategorien filtern.

Die Citrix Workspace-App für Windows unterstützt die Verwendung von SaaS-Anwendungen unter Einsatz des Access Control Service. Über diesen Dienst können Administratoren eine geschlossene Erfahrung mit Single Sign-On und Inhaltsinspektion bereitstellen.

Die Bereitstellung von SaaS-Anwendungen über die Cloud hat folgende Vorteile:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Einfache Konfiguration: einfach zu bedienen, zu aktualisieren und zu nutzen.
- Single Sign-On: mühelose Anmeldung.
- Standardvorlage für verschiedene Anwendungen: vorlagenbasierte Konfiguration beliebter Anwendungen.

Voraussetzungen:

- Die SaaS-Anwendung muss für Single Sign-On die SAML 2.0-Authentifizierung unterstützen.
- Die Option **Höhere Sicherheit aktivieren** muss im Zugriffssteuerungsdienst aktiviert werden, damit für das Rendering von SaaS-Anwendungen Citrix Enterprise Browser (früher "Citrix Workspace Browser") verwendet wird. Ist die Option nicht aktiviert, werden SaaS-Anwendungen im Standardbrowser des Clients gestartet.

> **Hinweis:**
>
> Die Citrix Workspace-App aggregiert zur Erzielung einer einheitlichen Benutzererfahrung lokal und in Cloudumgebungen veröffentlichte Apps und Desktops.

Die Citrix Workspace-App enthält einen Citrix Secure Browser zum Starten der SaaS-Anwendungen. Das Chromium Embedded Framework, auf dem Citrix Secure Browser basiert, ist Version 70. Dies führt zu einer besseren Benutzererfahrung beim Zugriff auf sichere SaaS-Apps.

> **Hinweis:**
>
> - Bei Workspace für Web werden SaaS-Anwendungen immer im Standardbrowser des Clients und nicht im Citrix Secure Browser gestartet.
> - Die Benutzererfahrung bei einer ICA-Sitzungs-App kann sich von der einer sicheren SaaS-App unterscheiden.

Der Citrix Secure Browser unterstützt Funktionen wie eine Symbolleiste, Zwischenablage, Drucken, Herunterladen und Wasserzeichen. Diese werden in der Citrix Workspace-App gemäß der Richtlinienkonfiguration im Zugriffssteuerungsdienst angewendet.

Im Citrix Secure Browser mögliche Aktionen:

Symbolleiste: Wenn die Symbolleistenoption für eine App aktiviert ist, können Sie die Optionen "Zurück", "Weiter"und "Aktualisieren"in der gestarteten App anzeigen. Die Symbolleiste enthält außerdem drei Punkte mit Zwischenablageaktionen.

Zwischenablage: Wenn der Zugriff auf die Zwischenablage in einer App aktiviert ist, können Sie die Optionen "Ausschneiden", "Kopieren"und "Einfügen"auf der Symbolleiste der gestarteten App verwenden. Ist die Option deaktiviert, werden die Optionen abgeblendet angezeigt.

Drucken: Sie können einen Druckbefehl in der gestarteten Anwendung ausführen, wenn die Druckoption aktiviert ist. Ist die Option deaktiviert, wird die Druckoption nicht angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Navigation: Die Symbole für "Weiter"und "Zurück"erscheinen auf der Symbolleiste der gestarteten App, wenn die Navigationsoption aktiviert ist.

Download: Sie können Dateien über die gestartete App herunterladen, wenn die Downloadoption aktiviert ist. Klicken Sie mit der rechten Maustaste auf die gestartete App und wählen Sie **Speichern unter**. Navigieren Sie zum gewünschten Speicherort und klicken Sie auf **Herunterladen**.

> **Hinweis:**
>
> Beim Download von Dateien wird kein Fortschrittsbalken angezeigt. Der Download wird jedoch erfolgreich ausgeführt.

Wasserzeichen: Wenn die Wasserzeichenoption aktiviert ist, wird in der gestarteten App ein Wasserzeichen mit dem Benutzernamen und der IP-Adresse des Clients angezeigt. Das Wasserzeichen ist halbtransparent und kann nicht zur Anzeige anderer Informationen bearbeitet werden.

Konfigurieren des Cache mit dem Gruppenrichtlinienobjekt:

Wenn sich mehrere Benutzer mit demselben Gerät anmelden, um auf die sicheren SaaS-Apps zuzugreifen, wird der Cache an den nachfolgenden Benutzer übergeben, wodurch die Browserinformationen der Benutzer freigegeben werden.

Um dieses Problem zu beheben, führt die Citrix Workspace-App eine neue Verwaltungsrichtlinie für ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) ein. Diese Richtlinie verhindert das Speichern des Browsercache auf dem lokalen Gerät.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Citrix Secure Browser**.
3. Wählen Sie die Richtlinie **Cache** aus.
   Hinweis: Standardmäßig ist diese Richtlinie auf **Aktiviert**festgelegt.
4. Um sie zu deaktivieren, wählen Sie **Deaktiviert** aus und klicken Sie auf **Übernehmen** und **OK**.
5. Starten Sie die Citrix Workspace-App neu, um die Änderung zu übernehmen.

Einschränkungen:

1. Wenn Sie eine veröffentlichte App mit aktivierter Druckoption und deaktivierter Downloadoption starten und einen Druckbefehl übergeben, können Sie die betreffende PDF-Datei möglicherweise trotzdem speichern. Sollen Downloads auf jeden Fall unterbunden werden, deaktivieren Sie auch die Druckoption.
2. In einer App eingebettete Videos funktionieren möglicherweise nicht.

Weitere Informationen zur Konfiguration von Workspace finden Sie unter Workspacekonfiguration in der Dokumentation zu Citrix Cloud.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

PDF-Druck

Voraussetzungen:

- Citrix Workspace-App Version 1808 oder höher
- Citrix Virtual Apps and Desktops Version 7 1808 oder höher
- Auf Ihrem Computer muss mindestens ein PDF-Viewer installiert sein.

Aktivieren der PDF-Druckfunktion:

1. Verwenden Sie auf dem Delivery Controller das Citrix Studio, und wählen Sie im linken Bereich den Knoten **Richtlinie**. Sie können entweder eine Richtlinie erstellen oder eine vorhandene Richtlinie bearbeiten.
2. Legen Sie die Richtlinie **Universellen PDF-Drucker automatisch erstellen** auf **Aktiviert** fest.

Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

Einschränkung:

- Das Anzeigen und Drucken von PDF-Dateien wird im Microsoft Edge-Browser nicht unterstützt.

Erweiterter Tabletmodus in Windows 10 mit Windows Continuum

Windows Continuum ist ein Windows 10-Feature, das sich an die Art und Weise der Verwendung des Clientgeräts anpasst. Die Citrix Workspace-App für Windows Version 4.10 oder später unterstützt nun Windows Continuum, einschließlich der dynamischen Änderung von Modi.

Bei touchfähigen Geräten startet der Windows 10-VDA im Tabletmodus, wenn keine Tastatur oder Maus angeschlossen ist. Ist eine Tastatur und/oder Maus angeschlossen, startet er im Desktopmodus. Durch das Anschließen oder Trennen eines Eingabegeräts an beliebigen Clientgeräten oder am Bildschirm eines 2-in-1-Geräts (z. B. Surface Pro) wird zwischen Tablet- und Desktopmodus umgeschaltet. Weitere Informationen finden Sie unter Tabletmodus für Geräte mit Touchscreen in der Dokumentation von Citrix Virtual Apps and Desktops.

Der Windows 10-VDA erkennt das Vorhandensein einer Tastatur oder einer Maus auf einem touchfähigen Clientgerät, wenn Sie eine Verbindung herstellen oder eine Verbindung zu einer Sitzung herstellen. Er erkennt auch, wenn Sie während der Sitzung eine Tastatur oder eine Maus anschließen oder entfernen. Dieses Feature ist standardmäßig auf dem VDA aktiviert. Um das Feature zu deaktivieren, ändern Sie mit Citrix Studio die Richtlinie **Tabletmodus ein/aus**.

Der Tabletmodus bietet eine für Touchscreens besser geeignete Benutzeroberfläche:

- Die Schaltflächen sind etwas größer.
- Die **Startseite** und alle Apps werden im Vollbildmodus geöffnet.
- Die Taskleiste enthält eine Zurück-Schaltfläche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Die Taskleiste enthält keine Symbole.

Der Desktopmodus ist die klassische Benutzeroberfläche, bei der die Interaktion wie bei einem PC mit Tastatur und Maus erfolgt.

> **Hinweis:**
>
> Workspace für Web unterstützt Windows Continuum nicht.

Relative Maus

Durch die Unterstützung für relative Mausbewegungen wird die Mausposition auf relative statt auf absolute Weise interpretiert. Diese Funktion ist für Anwendungen erforderlich, die relative Mauseingabe statt absoluter Eingabe erfordern.

> **Hinweis**
>
> Dieses Feature kann nur in einer veröffentlichten Desktopsitzung angewendet werden.

Wenn Sie das Feature mit dem Registrierungs-Editor oder der Datei default.ica konfigurieren, kann die Einstellung auch nach dem Beendigung der Sitzung fortbestehen.

Sie können die Verfügbarkeit des Features pro Benutzer und pro Maschine mit der Registrierung wie folgt steuern:

Konfigurieren der relativen Mausfunktion mit dem Registrierungs-Editor

Um das Feature zu konfigurieren, aktivieren Sie die folgenden Registrierungsschlüssel und starten Sie dann die Sitzung neu, damit die Änderungen wirksam werden:

So stellen Sie das Feature pro Sitzung zur Verfügung:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse`

So stellen Sie das Feature pro Benutzer zur Verfügung:
`HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse`

```
1 - Name: Mouse
2 - Type: REG_SZ
3 - Value: True
```

> **Hinweis:**
>
> - Die im Registrierungs-Editor festgelegten Werte haben Vorrang vor den in der ICA-Datei festgelegten Einstellungen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Die in HKEY_LOCAL_MACHINE und HKEY_CURRENT_USER festgelegten Werte müssen identisch sein. Unterschiedliche Werte können Konflikte verursachen.

Konfigurieren der relativen Mausfunktion mit der Datei default.ica

1. Öffnen Sie die Datei default.ica, die normalerweise in `C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica` ist, wobei "sitename"der Name der Site ist, der bei ihrer Erstellung angegeben wurde. Bei StoreFront-Kunden ist die Datei default.ica normalerweise unter `C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica`, wobei "storename"der Name des Stores ist, der bei seiner Erstellung angegeben wurde.
2. Fügen Sie einen neuen Schlüssel namens "RelativeMouse"im Abschnitt WFClient hinzu, dessen Wert der Konfiguration im JSON-Objekt entspricht.
3. Legen Sie den Wert wie gewünscht fest:
   - true –Aktivieren der relativen Maus
   - false –Deaktivieren der relativen Maus
4. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Hinweis:

Die im Registrierungs-Editor festgelegten Werte haben Vorrang vor den in der ICA-Datei festgelegten Einstellungen.

Aktivieren der relativen Mausfunktion über den Desktop Viewer

1. Melden Sie sich bei der Citrix Workspace-App an.
2. Starten Sie eine veröffentlichte Desktopsitzung.
3. Klicken Sie auf der Desktop Viewer-Symbolleiste auf **Einstellungen**.

   Das Fenster "Citrix Workspace-Einstellungen"wird angezeigt.
4. Wählen Sie **Verbindungen**.
5. Aktivieren Sie unter **Relative Mauseinstellungen** die Option **Relative Maus verwenden**.
6. Klicken Sie auf **Anwenden** und auf **OK**.

Hinweis:

Beim Konfigurieren der relativen Maus mit dem Desktop Viewer wird das Feature nur pro Sitzung angewendet.

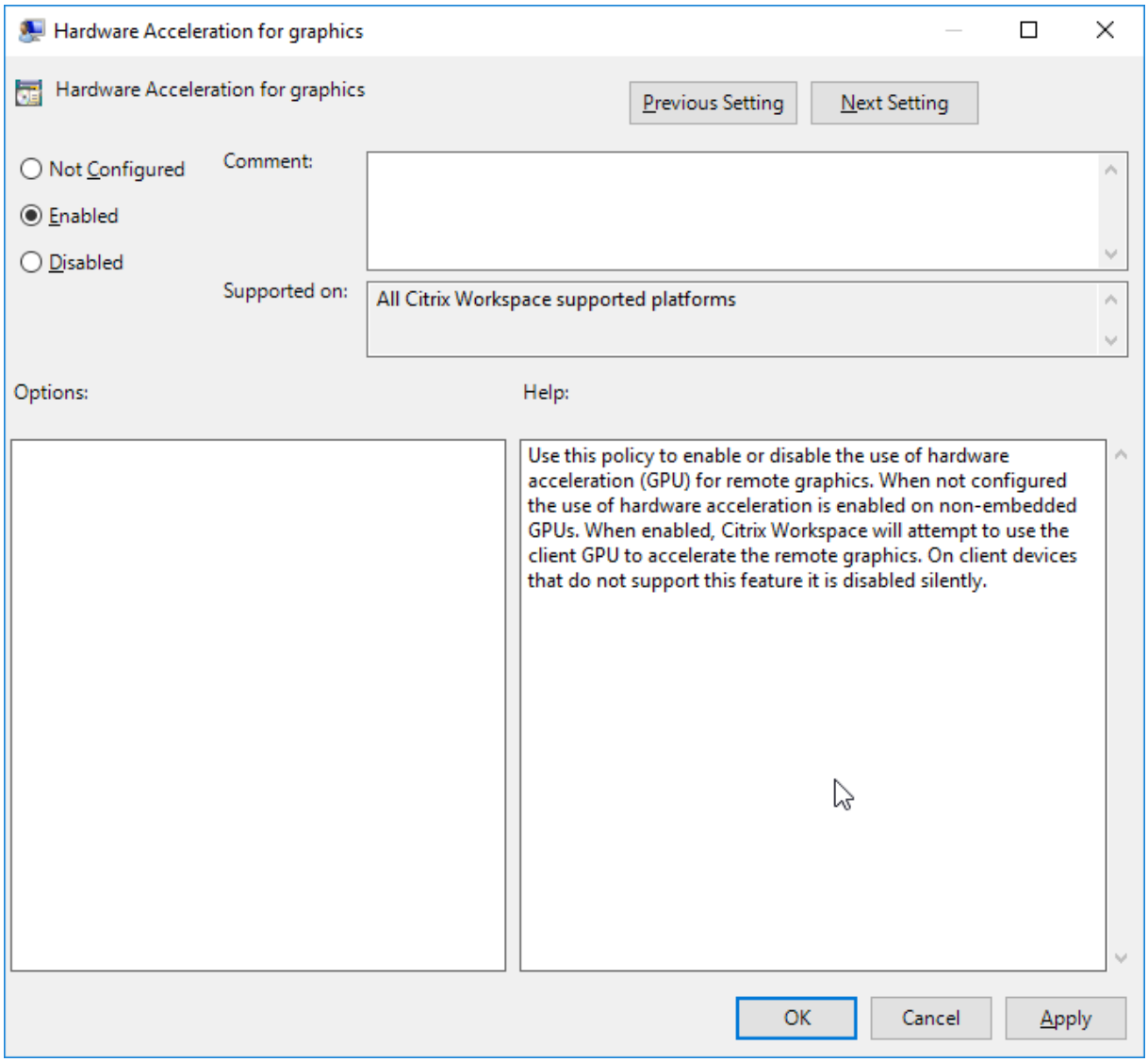
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hardwaredecodierung

Wenn Sie die Citrix Workspace-App (mit HDX Engine 14.4) verwenden, kann die GPU für H.264-Decodierung verwendet werden, wenn sie auf dem Client verfügbar ist. Die für GPU-Decodierung verwendete API-Ebene ist DirectX Video Acceleration.

Aktivieren der Hardwaredecodierung mit der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Benutzererfahrung**.
3. Wählen Sie **Hardwarebeschleunigung für Grafiken**.
4. Wählen Sie **Aktiviert** und klicken Sie auf **Übernehmen** und anschließend auf **OK**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Anhand der folgenden Registrierungseinträge sehen Sie, ob die Richtlinie angewendet wird und die Hardwarebeschleunigung in einer aktiven ICA-Sitzung verwendet wird:

Registrierungspfad: `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender`.

> **Tipp**
>
> Der Wert für **Graphics_GfxRender_Decoder** und **Graphics_GfxRender_Renderer** sollte 2 sein. Wenn der Wert 1 ist, wird auf der CPU basierende Decodierung verwendet.

Wenn Sie das Hardwaredecodierungsfeature verwenden, berücksichtigen Sie folgende Einschränkungen:

- Wenn der Client zwei GPUs hat und wenn einer der Bildschirme auf der zweiten GPU aktiv ist, wird CPU-Decodierung verwendet.
- Bei einer Verbindung mit einem Citrix Virtual Apps-Server, der unter Windows Server 2008 R2 ausgeführt wird, empfiehlt Citrix, auf dem Windows-Gerät des Benutzers keine Hardwaredecodierung zu verwenden. Ist die Hardwaredecodierung aktiviert, treten Probleme auf, wie geringe Leistung beim Markieren von Text und Flackern.

Mikrofoneingabe

Die Citrix Workspace-App unterstützt die mehrfache clientseitige Mikrofoneingabe. Lokal installierte Mikrofone können für Folgendes verwendet werden:

- Echtzeitaktivitäten, wie Softphone-Anrufe und Webkonferenzen
- Gehostete Aufzeichnungsanwendungen, z. B. Diktierprogramme
- Video- und Audio-Aufzeichnungen

Benutzer der Citrix Workspace-App können in Connection Center auswählen, ob am Gerät angeschlossene Mikrofone verwendet werden sollen. Benutzer von Citrix Virtual Apps and Desktops und Citrix DaaS können außerdem ihre Mikrofone und Webcams im Citrix Virtual Apps and Desktops-Viewer unter “Einstellungen”deaktivieren.

Multimonitorunterstützung

Sie können maximal acht Monitore mit der Citrix Workspace-App für Windows verwenden.

Jeder Monitor in einer Multimonitorumgebung hat eine eigene, vom Hersteller festgelegte Auflösung. Monitore können in Sitzungen verschiedene Auflösungen und Ausrichtungen haben.

Sitzungen können auf zwei Arten auf mehrere Monitore übergreifend ausgeführt werden:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Vollbildmodus: Mehrere Monitore werden in der Sitzung angezeigt; Anwendungen werden genauso wie beim lokalen Desktop an Monitore angedockt.

  Citrix Virtual Apps and Desktops und Citrix DaaS: Sie können das Desktop Viewer-Fenster über eine beliebige rechteckige Untergruppe von Monitoren ausdehnen, wenn Sie die Größe des Fensters über einen Monitorbereich hinweg ändern und auf **Maximieren** klicken.

- Im Fenstermodus mit einem Monitorbild für die Sitzung werden Anwendungen nicht an einzelne Monitore angedockt.

Citrix Virtual Apps and Desktops und Citrix DaaS: Wenn ein Desktop in derselben Zuordnung (früher Desktopgruppe) anschließend gestartet wird, wird die Fenstereinstellung gespeichert, und der Desktop wird auf denselben Monitoren angezeigt. Mehrere virtuelle Desktops können auf einem Gerät angezeigt werden, wenn die Monitoranordnung rechteckig ist. Wenn der primäre Monitor auf dem Gerät von der Sitzung mit virtuellen Apps und Desktops verwendet wird, wird er zum primären Monitor in der Sitzung. Sonst wird der zahlenmäßig niedrigste Monitor in der Sitzung zum primären Monitor.

Für die Multimonitorunterstützung müssen Sie Folgendes sicherstellen:

- Das Benutzergerät ist für die Unterstützung von mehreren Monitoren konfiguriert.
- Das Betriebssystem muss auch jeden Monitor erkennen können. Um auf Windows-Plattformen zu überprüfen, ob diese Erkennung erfolgt, gehen Sie zu **Einstellungen** > **System**, klicken Sie auf **Anzeige** und bestätigen Sie, dass jeder Monitor separat angezeigt wird.
- Nach dem Erkennen der Monitore:
  - **Citrix Virtual Desktops:** Konfigurieren Sie das Grafikspeicherlimit mit der Citrix Maschinenrichtlinieneinstellung **Anzeigespeicherlimit**.
  - **Citrix Virtual Apps:** Je nach installierter Citrix Virtual Apps-Serverversion:
    - Konfigurieren Sie das Limit für den Grafikspeicher mit der Citrix Computerrichtlinieneinstellung **Anzeigespeicherlimit**.
    - Wählen Sie im linken Bereich der Citrix Verwaltungskonsole für den Citrix Virtual Apps-Server die Farm aus. Wählen Sie im Aufgabenbereich **Servereigenschaften ändern > Alle Eigenschaften ändern > Serverstandard > HDX Broadcast > Anzeige (oder Servereigenschaften ändern > Alle Eigenschaften ändern > Serverstandard > ICA > Anzeige)** und stellen Sie "Maximaler Speicher für Grafiken pro Sitzung"ein.

Stellen Sie sicher, dass die Einstellung (in Kilobytes) hoch genug ist, damit ausreichend Grafikspeicher bereitgestellt wird. Wenn der Wert dieser Einstellung nicht hoch genug ist, wird die veröffentlichte Ressource auf einen Teilbereich der Monitore beschränkt, der in die angegebene Größe passt.

Verwenden von Citrix Virtual Desktops auf zwei Monitoren:

1. Wählen Sie den Desktop Viewer aus und klicken Sie auf den Pfeil nach unten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Wählen Sie **Fenster**.
3. Ziehen Sie den Bildschirm von Citrix Virtual Desktops zwischen die beiden Monitore. Stellen Sie sicher, dass etwa die Hälfte des Bildschirms in jedem Monitor angezeigt wird.
4. Wählen Sie auf der Symbolleiste des Citrix Virtual Desktops die Option **Vollbild** aus.

   Der Bildschirm ist nun auf beide Monitore erweitert.

Weitere Informationen zum Berechnen der Größe des Grafikspeichers in Sitzungen für Citrix Virtual Apps and Desktops und Citrix DaaS finden Sie im Knowledge Center-Artikel CTX115637.

Drucker

Überschreiben der Druckereinstellungen auf dem Benutzergerät

1. Klicken Sie im Menü **Drucken**, das in einer Anwendung auf dem Benutzergerät zur Verfügung steht, auf **Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Clienteinstellungen** auf **Erweiterte Optimierungen** und ändern Sie die Optionen "Bildkomprimierung"und "Bild- und Schriftartcaching".

Steuerung der Bildschirmtastatur

Damit über Windows-Tablets der Touchzugriff auf virtuelle Anwendungen und Desktops möglich ist, zeigt die Citrix Workspace-App automatisch eine Bildschirmtastatur an, wenn Sie ein Texteingabefeld aktivieren und das Gerät im Falt- oder Tabletmodus ist.

Auf einigen Geräten und unter bestimmten Umständen kann die Citrix Workspace-App den Modus des Geräts nicht genau bestimmen und die Bildschirmtastatur wird u. U. angezeigt, wenn sie nicht benötigt wird.

Um bei Verwendung eines konvertierbaren Geräts keine Bildschirmtastatur anzuzeigen, erstellen Sie einen REG_DWORD-Wert `DisableKeyboardPopup` in `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver` und legen den Wert auf 1 fest.

> **Hinweis:**
>
> Auf x64-Maschinen erstellen Sie den Wert in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver`.

Die Tasten können, wie nachfolgend erläutert, auf 3 verschiedene Modi festgelegt werden:

- **Automatisch**: AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Immer anzeigen** (Bildschirmtastatur): AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0
- **Nie anzeigen** (Bildschirmtastatur): AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1

Tastenkombinationen

Sie können Tastenkombinationen konfigurieren, die die Citrix Workspace-App als Sonderfunktionen interpretiert. Wenn die Richtlinie für Tastenkombinationen aktiviert ist, können Sie Zuordnungen von Citrix Tastenkombinationen, das Verhalten von Windows-Tastenkombinationen und das Tastaturlayout für Sitzungen festlegen.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzererfahrung**.
3. Wählen Sie die Richtlinie **Tastenkombinationen**.
4. Wählen Sie **Aktiviert** und die gewünschten Optionen.
5. Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

Unterstützung für Symbole in 32-Bit-Farben:

Die Citrix Workspace-App unterstützt Symbole in 32 Bit High Color und die Farbtiefe wird automatisch für Anwendungen ausgewählt, die im Dialogfeld **Citrix Connection Center**, im Startmenü und in der Taskleiste angezeigt werden, um Anwendungen im Seamlessmodus darzustellen.

> **Achtung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Um eine bevorzugte Farbtiefe zu definieren, können Sie unter `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences` einen Zeichenfolgenregistrierungsschlüssel `TWIDesiredIconColor` hinzufügen und auf den gewünschten Wert festlegen. Die möglichen Werte für die Farbtiefe von Symbolen sind 4, 8, 16, 24 und 32 Bits pro Pixel. Benutzer können eine geringere Farbtiefe für die Symbole wählen, wenn die Netzwerkverbindung langsam ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Desktop Viewer

Jedes Unternehmen hat andere Anforderungen. Die Wünsche und Anforderungen bezüglich des Benutzerzugriffs auf virtuelle Desktops können sich zudem im Laufe der Zeit ändern. Die Benutzererfahrung beim Verbinden mit virtuellen Desktops und der Umfang der Benutzereingriffe beim Konfigurieren der Verbindungen hängen davon ab, wie Sie die Citrix Workspace-App für Windows einrichten.

Verwenden Sie **Desktop Viewer**, wenn Benutzer mit dem virtuellen Desktop interagieren müssen. Bei einem virtuellen Desktop kann es sich um einen veröffentlichten virtuellen Desktop, einen freigegebenen Desktop oder einen dedizierten Desktop handeln. In diesem Zugriffsszenario kann der Benutzer über die Desktop Viewer-Symbolleiste einen virtuellen Desktop in einem Fenster öffnen und den Desktop im lokalen Desktop ziehen und skalieren. Benutzer können Einstellungen festlegen und mit mehreren Desktops über mehrere Citrix Virtual Apps and Desktops- und Citrix DaaS-Verbindungen auf demselben Benutzergerät arbeiten.

> **Hinweis:**
>
> Die Benutzer müssen die Citrix Workspace-App zum Ändern der Bildschirmauflösung auf ihren virtuellen Desktops verwenden. Die Bildschirmauflösung kann nicht in der Windows-Systemsteuerung geändert werden.

Tastatureingabe in Desktop Viewer

In Desktop Viewer-Sitzungen wird die **Windows-Logo-Taste+L** an den lokalen Computer gesendet.

Strg+Alt+Entf wird an den lokalen Computer gesendet.

Tastatureingaben, die die Einrastfunktion, die Anschlagverzögerung und Statusanzeige (Eingabehilfen von Microsoft) aktivieren, werden normalerweise an den lokalen Computer gesendet.

Als Eingabehilfe von Desktop Viewer werden die Schaltflächen der Desktop Viewer-Symbolleiste in einem Popupfenster angezeigt, wenn Sie Strg+Alt+Untbr drücken.

Strg+Esc wird an den virtuellen Remotedesktop gesendet.

> **Hinweis:**
>
> Wenn Desktop Viewer maximiert ist, können Sie mit Alt+Tab standardmäßig zwischen Fenstern in der Sitzung wechseln. Wenn Desktop Viewer in einem Fenster angezeigt wird, wechseln Sie mit Alt+Tab zwischen Fenstern außerhalb der Sitzung.

Citrix hat bestimmte Tastenkombinationen entwickelt. Beispiel: Mit Strg+F1 reproduzieren Sie Strg+Alt+Entf und mit Umschalt+F2 wechseln Sie Anwendungen vom Vollbild- in den Fenstermodus und umgekehrt. Sie können Tastenkombinationen nicht mit virtuellen Desktops verwenden, die in

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Desktop Viewer angezeigt werden (d. h. mit Sitzungen mit virtuellen Apps und Desktops). Sie können sie aber mit veröffentlichten Anwendungen verwenden (d. h. mit Citrix Virtual Apps-Sitzungen).

Virtuelle Desktops

In einer Desktopsitzung können Benutzer keine Verbindung zu demselben Desktop herstellen. Bei einem Versuch wird die bestehende Desktopsitzung getrennt. Aus diesem Grund empfiehlt Citrix Folgendes:

- Administratoren sollten die Clients auf dem Desktop nicht so konfigurieren, dass sie auf eine Site verweisen, die denselben Desktop veröffentlicht.
- Benutzer sollten keine Site besuchen, die denselben Desktop hostet, wenn die Site für die automatische Wiederverbindung der Benutzer mit vorhandenen Sitzungen konfiguriert ist.
- Benutzer sollten keine Site besuchen, die denselben Desktop hostet und versuchen, ihn zu starten.

Vergessen Sie nicht, dass ein Benutzer, der sich lokal an einem Computer anmeldet, der als virtueller Desktop fungiert, Verbindungen zu diesem Desktop blockiert.

Wenn Benutzer eine Verbindung mit virtuellen Anwendungen (die mit Citrix Virtual Apps veröffentlicht wurden) von einem virtuellen Desktop aus herstellen, und das Unternehmen einen separaten Citrix Virtual Apps-Administrator hat, sollten Sie mit ihm die Gerätezuordnung festlegen, sodass Desktopgeräte konsistent in Desktop- und Anwendungssitzungen zugeordnet werden. Da lokale Laufwerke in Desktopsitzungen als Netzwerklaufwerke angezeigt werden, muss der Citrix Virtual Apps-Administrator die Richtlinie für die Laufwerkzuordnung ändern und Netzwerklaufwerke einschließen.

Timeout der Statusanzeige

Sie können die Zeit ändern, die die Statusanzeige beim Start einer Sitzung durch einen Benutzer angezeigt wird. Zum Ändern des Timeoutzeitraums erstellen Sie einen REG_DWORD-Wert SI INACTIVE MS in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\. Sie können den REG_DWORD-Wert auf 4 festlegen, wenn die Statusanzeige eher ausgeblendet werden soll.

Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Erfasste Daten	Beschreibung	Verwendungszweck
Konfigurations- und Nutzungsdaten	Das Citrix-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) sammelt Konfigurations- und Nutzungsdaten in der Citrix Workspace-App für Windows und sendet die Daten automatisch an Citrix und Google Analytics.	Citrix nutzt diese Daten, um die Qualität, Zuverlässigkeit und Leistung der Citrix Workspace-App zu verbessern.

Weitere Informationen

Citrix verarbeitet Ihre Daten in Übereinstimmung mit den Bedingungen Ihres Vertrags mit Citrix und schützt sie gemäß dem im Citrix Trust Center festgelegten Citrix Services Security Exhibit.

Citrix verwendet Google Analytics, um bestimmte Daten aus der Citrix Workspace-App als Teil von CEIP zu sammeln. Sie können prüfen, wie Google die für Google Analytics gesammelten Daten verwendet.

Auf folgende Weise können Sie das Senden von CEIP-Daten an Citrix und Google Analytics deaktivieren (mit Ausnahme der beiden für Google Analytics erfassten Datenelemente, die durch ein * in der zweiten Tabelle unten gekennzeichnet sind):

1. Klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Citrix Workspace-App-Symbol.
2. Wählen Sie **Erweiterte Einstellungen**.
   Das Dialogfeld **Erweiterte Einstellungen** wird angezeigt.
3. Wählen Sie **Datensammlung**.
4. Wählen Sie **Nein, danke**, um CEIP zu deaktivieren und die Teilnahme abzulehnen.
5. Klicken Sie auf **Speichern**.

Alternativ navigieren Sie zum folgenden Registrierungseintrag und legen Sie den Wert wie vorgeschlagen fest:

Pfad: `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

Schlüssel: `Enable_CEIP`

Wert: `False`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Wenn Sie im Dialogfeld für die Datensammlung **Nein, danke** auswählen oder den Schlüssel `Enable_CEIP` auf `False` festlegen und dann das Senden der letzten beiden CEIP-Datenelemente an Google Analytics deaktivieren möchten (Betriebssystemversion & Version der Citrix Workspace-App), navigieren Sie zum folgenden Registrierungseintrag und legen Sie den Wert wie vorgeschlagen fest:

Pfad: `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

Schlüssel: `DisableHeartbeat`

Wert: `True`

Folgende CEIP-Datenelemente werden von Citrix gesammelt:

Betriebssystemversion	Citrix Workspace-App	Angeschlossene externe Geräte	Bildschirmauflösung
Flash-Version	Desktop Lock-Konfiguration	Toucheingabe aktiviert	Authentifizierungskonfiguration
Sitzungsstartmethode	Grafikkonfiguration	Desktop Viewer-Konfiguration	Drucken
Verbindungsfehler	Dauer des Starts	Sprache der Citrix Workspace-App	VDA-Informationen
SSON-Status	Status des Installers	Dauer der Installation	Verbindungsprotokoll
Internet Explorer-Version			

Folgende CEIP-Datenelemente werden von Google Analytics erfasst:

Betriebssystemversion*	Citrix Workspace-App-Version*	Authentifizierungskonfiguration	Sprache der Citrix Workspace-App
Sitzungsstartmethode	Verbindungsfehler	Verbindungsprotokoll	VDA-Informationen
Installerkonfiguration	Status des Installers	Clienttastaturlayout	Storekonfiguration
Einstellung für automatische Aktualisierung	Nutzung des Connection Centers	Konfiguration von App Protection	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Authentifizieren

October 26, 2023

Sichern Sie die Verbindungen zwischen der Citrix Workspace-App und den veröffentlichten Ressourcen, um eine maximale Sicherheit zu gewährleisten. Folgende Authentifizierungstypen können konfiguriert werden:

- Domänen-Passthrough
- Smartcard
- Kerberos mit Passthrough

Domänen-Passthrough-Authentifizierung

Mit Single Sign-On können Sie sich authentifizieren und virtuelle Apps and Desktops verwenden, ohne sich erneut authentifizieren zu müssen.

Wenn Sie sich bei der Citrix Workspace-App anmelden, können Ihre Anmeldeinformationen und aufgelisteten Ressourcen an StoreFront weitergeleitet werden.

In früheren Releases können Sie bei Verwendung von Google Chrome, Microsoft Edge oder Mozilla FireFox auch dann Single Sign-On-Sitzungen starten, wenn die Funktion nicht aktiviert ist.

Ab Version 1905 müssen Sie bei allen Webbrowsern Single Sign-On mit der administrativen Gruppenrichtlinienobjektvorlage konfigurieren. Weitere Informationen zum Konfigurieren von Single Sign-On mit der administrativen Gruppenrichtlinienobjektvorlage finden Sie unter Konfigurieren von Single Sign-On mit Citrix Gateway.

Sie können Single Sign-On sowohl bei der Neuinstallation als auch bei einem Upgrade konfigurieren, indem Sie eine der folgenden Optionen verwenden:

- Befehlszeilenoberfläche
- Grafische Benutzeroberfläche (GUI)

Single Sign-On während der Neuinstallation konfigurieren

Konfigurieren von Single Sign-On während der Neuinstallation:

1. Konfiguration in StoreFront oder im Webinterface.
2. Konfigurieren Sie XML-Vertrauensdienste auf dem Delivery Controller.
3. Ändern der Internet Explorer-Einstellungen.
4. Installieren der Citrix Workspace-App mit Single Sign-On.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfigurieren von Single Sign-On in StoreFront oder im Webinterface

Je nach Bereitstellung von Citrix Virtual Apps and Desktops kann Single Sign-On über die Verwaltungskonsole in StoreFront oder im Webinterface konfiguriert werden.

In der folgenden Tabelle finden Sie verschiedene Anwendungsfälle und die entsprechende Konfiguration:

Anwendungsfall	Konfigurationsdetails	Weitere Informationen
SSON ist in StoreFront oder im Webinterface konfiguriert	Starten Sie Citrix Studio, navigieren Sie zu **Store** > **Authentifizierungsmethoden verwalten** und aktivieren Sie **Domänen-Passthrough-Authentifizierung**.	Bei nicht konfiguriertem Single Sign-On ändert die Citrix Workspace-App die Authentifizierungsmethode automatisch von **Domänen-Passthrough-Authentifizierung** in **Benutzername und Kennwort**, sofern verfügbar.
Wenn Workspace für Web erforderlich ist	Starten Sie **Store** > **Workspace für Websites** > **Authentifizierungsmethoden verwalten** und aktivieren Sie **Domänen-Passthrough-Authentifizierung**.	Bei nicht konfiguriertem Single Sign-On ändert die Citrix Workspace-App die Authentifizierungsmethode automatisch von **Domänen-Passthrough-Authentifizierung** in **Benutzername und Kennwort**, sofern verfügbar.
Wenn StoreFront nicht konfiguriert ist	Wenn das Webinterface auf dem VDA konfiguriert ist, starten Sie XenApp Services-Sites > **Authentifizierungsmethoden** und aktivieren Sie **Passthrough**.	Bei nicht konfiguriertem Single Sign-On ändert die Citrix Workspace-App die Authentifizierungsmethode automatisch von **Passthrough** in **Explizit**, sofern verfügbar.

Single Sign-On mit Citrix Gateway konfigurieren

Sie aktivieren Single Sign-On mit Citrix Gateway über die administrative Gruppenrichtlinienobjektvorlage.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzerauthentifizierung**.
3. Wählen Sie die Richtlinie **Single Sign-On für Citrix Gateway** aus.
4. Wählen Sie **Aktiviert**.
5. Klicken Sie auf **Anwenden** und auf **OK**.
6. Starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.

XML-Vertrauensdienste auf dem Delivery Controller konfigurieren

Führen Sie auf Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) als Administrator den folgenden PowerShell-Befehl auf dem Delivery Controller aus:

```
asnp Citrix* Set-BrokerSite -TrustRequestsSentToTheXmlServicePort
$True
```

Ändern der Internet Explorer-Einstellungen

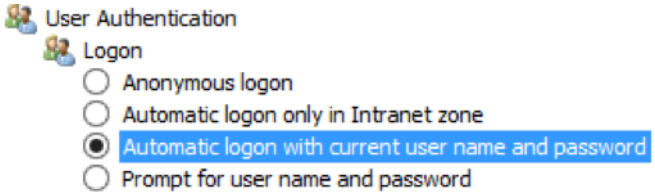
1. Fügen Sie den StoreFront-Server der Liste der vertrauenswürdigen Sites im Internet Explorer hinzu. Führen Sie folgende Schritte aus:

    a) Starten Sie **Internetoptionen** über die Systemsteuerung.
    b) Klicken Sie auf **Sicherheit** > **Lokales Internet** und dann auf **Sites**. Das Fenster **Lokales Intranet** wird angezeigt.
    c) Wählen Sie **Erweitert**.
    d) Fügen Sie die URL des StoreFront- oder Webinterface-FQDN mit den entsprechenden HTTP- oder HTTPS-Protokollen hinzu.
    e) Klicken Sie auf **Anwenden** und auf **OK**.

2. Ändern Sie im **Internet Explorer** die Einstellungen unter **Benutzerauthentifizierung**. Führen Sie folgende Schritte aus:

    a) Starten Sie **Internetoptionen** über die Systemsteuerung.
    b) Klicken Sie auf **Sicherheit** > **Vertrauenswürdige Sites**.
    c) Klicken Sie auf **Stufe anpassen**. Das Fenster **Sicherheitseinstellungen - Zone vertrauenswürdiger Sites** wird angezeigt.
    d) Wählen Sie im Bereich **Benutzerauthentifizierung** die Option **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



a) Klicken Sie auf **Anwenden** und auf **OK**.

Konfigurieren von Single Sign-On über die Befehlszeilenschnittstelle

Installieren Sie die Citrix Workspace-App für Windows mit dem Switch `/includeSSON` und starten Sie die Citrix Workspace-App neu, damit die Änderungen wirksam werden.

> **Hinweis:**
>
> Wenn die Citrix Workspace-App für Windows ohne die Single Sign-On-Komponente installiert wird, wird das Upgrade auf die neueste Version von Citrix Workspace-App mit dem Switch `/includeSSON` nicht unterstützt.

Konfigurieren von Single Sign-On über die grafische Benutzeroberfläche

1. Suchen Sie die Installationsdatei der Citrix Workspace-App (`CitrixWorkspaceApp.exe`).
2. Doppelklicken Sie auf `CitrixWorkspaceApp.exe`, um das Installationsprogramm zu starten.
3. Wählen Sie im **Installationsassistenten zum Aktivieren von Single Sign-On** die Option **Single Sign-On aktivieren**.
4. Klicken Sie auf **Weiter** und folgen Sie den Anweisungen, um die Installation abzuschließen.

Sie können sich jetzt mit der Citrix Workspace-App anmelden, ohne Benutzeranmeldeinformationen einzugeben.

Konfigurieren von Single Sign-On in Citrix Workspace für Web

Sie können Single Sign-On in Workspace für Web mit der administrativen Gruppenrichtlinienobjektvorlage konfigurieren.

1. Öffnen Sie die administrative GPO-Vorlage von Workspace, indem Sie gpedit.msc ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzerauthentifizierung**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Wählen Sie die Richtlinie **Lokaler Benutzername und Kennwort** aus und legen Sie sie auf **Aktiviert** fest.
4. Klicken Sie auf **Passthrough-Authentifizierung aktivieren**. Mit dieser Option kann Workspace für Web Ihre Anmeldeinformationen für die Authentifizierung auf dem Remoteserver verwenden.
5. Klicken Sie auf **Passthrough-Authentifizierung für alle ICA-Verbindungen zulassen**. Mit dieser Option werden alle Authentifizierungseinschränkungen umgangen und das Passthrough von Anmeldeinformationen für alle Verbindungen ermöglicht.
6. Klicken Sie auf **Anwenden** und auf **OK**.
7. Starten Sie Workspace für Web neu, um die Änderungen zu übernehmen.

Stellen Sie sicher, dass Single Sign-On aktiviert ist, indem Sie den **Task-Manager** starten und prüfen, ob der Prozess `ssonsvr.exe` ausgeführt wird.

Single Sign-On mit Active Directory konfigurieren

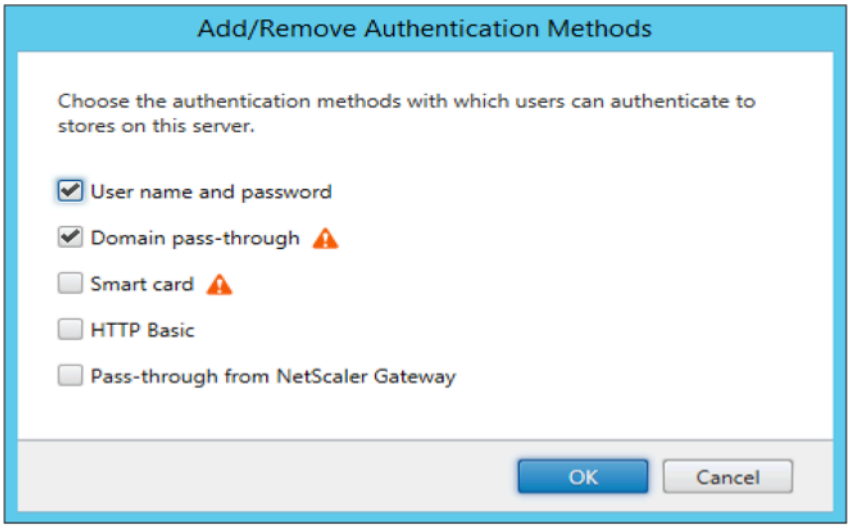
Sie können die Single Sign-On-Authentifizierung mit Active Directory konfigurieren. In diesem Fall benötigen Sie keine Bereitstellungstools wie Microsoft System Center Configuration Manager.

1. Laden Sie die Installationsdatei für die Citrix Workspace-App (CitrixWorkspaceApp.exe) auf eine geeignete Netzwerkfreigabe herunter. Die Maschinen, auf denen die Citrix Workspace-App installiert werden soll, müssen darauf Zugriff haben.
2. Laden Sie die Vorlage `CheckAndDeployWorkspacePerMachineStartupScript.bat` von der Downloadseite für die Citrix Workspace-App für Windows herunter.
3. Bearbeiten Sie den Speicherort und die Version von `CitrixWorkspaceApp.exe`.
4. Geben Sie in der **Active Directory-Gruppenrichtlinienverwaltungskonsole** als Startskript `CheckAndDeployWorkspacePerMachineStartupScript.bat` ein. Weitere Informationen zum Bereitstellen der Startskripts finden Sie im Abschnitt Active Directory.
5. Navigieren Sie im Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Vorlagen hinzufügen/entfernen**, um die Datei `icaclient.adm` hinzuzufügen.
6. Nachdem Sie die Vorlage `icaclient.adm` hinzugefügt haben, navigieren Sie zu **Computerkonfiguration** > **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzerauthentifizierung**.
7. Wählen Sie die Richtlinie **Lokaler Benutzername und Kennwort** aus und legen Sie sie auf **Aktiviert** fest.
8. Wählen Sie **Passthrough-Authentifizierung aktivieren** und klicken Sie auf **Übernehmen**.
9. Starten Sie die Maschine neu, damit die Änderungen wirksam werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfigurieren von Single Sign-On in StoreFront und im Webinterface

Konfigurieren in StoreFront Öffnen Sie **Citrix Studio** auf dem StoreFront-Server und wählen Sie **Authentifizierung > Authentifizierungsmethoden hinzufügen/entfernen**. Wählen Sie dann **Domänen-Passthrough**.

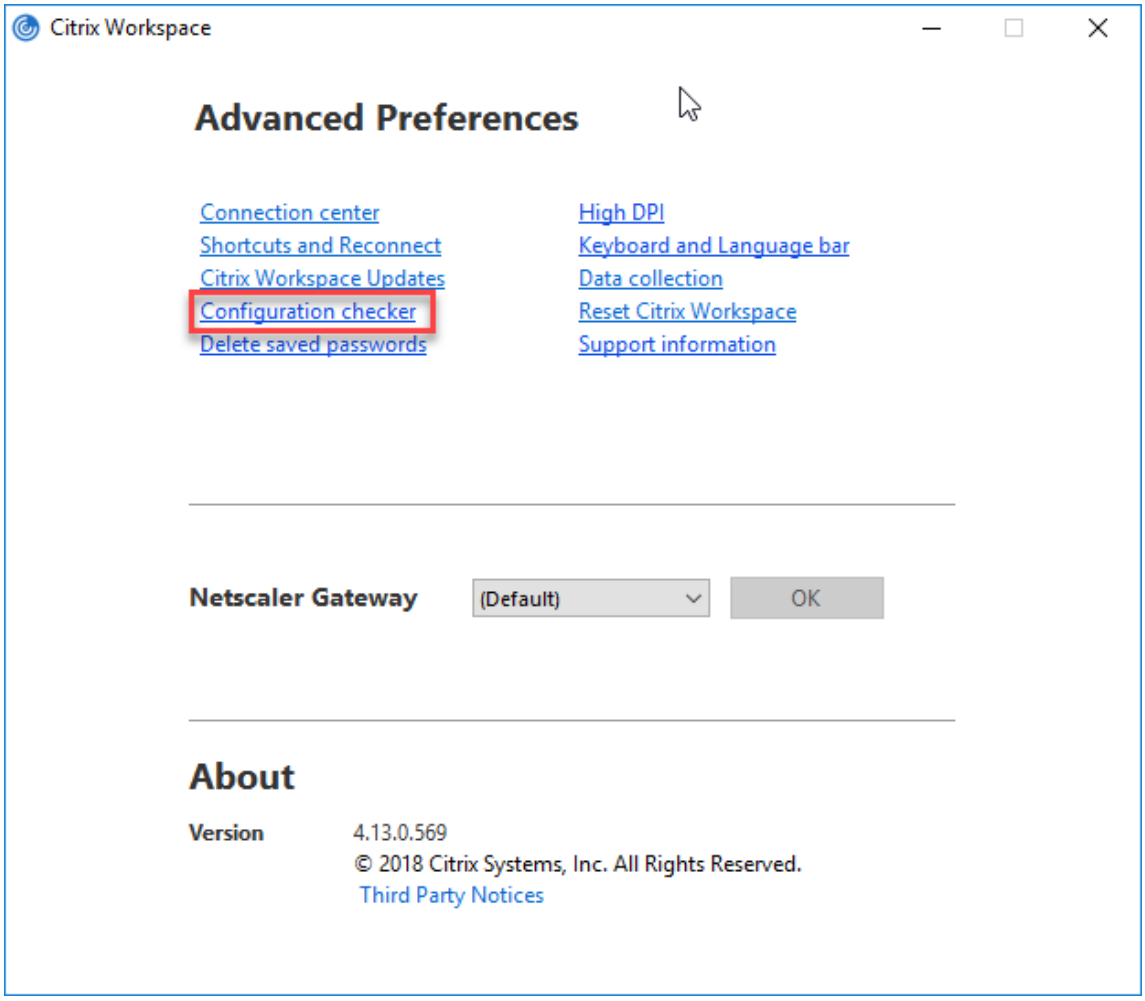


Konfigurationsprüfung

Mit der Konfigurationsprüfung können Sie einen Test ausführen, um sicherzustellen, dass Single Sign-On ordnungsgemäß konfiguriert ist. Der Test wird für verschiedene Prüfpunkte der Single Sign-On-Konfiguration ausgeführt und die Konfigurationsergebnisse werden angezeigt.

1. Klicken Sie mit der rechten Maustaste im Infobereich auf das Symbol der Citrix Workspace-App und dann auf **Erweiterte Einstellungen**.
   Das Dialogfeld **Erweiterte Einstellungen** wird angezeigt.
2. Klicken Sie auf **Konfigurationsprüfung**.
   Das Fenster der **Citrix Konfigurationsprüfung** wird angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Wählen Sie **SSONChecker** im Bereich **Auswählen** aus.
4. Klicken Sie auf **Ausführen**. Eine Fortschrittsanzeige mit dem Status des Tests wird angezeigt.

Das Fenster der **Konfigurationsprüfung** enthält die folgenden Spalten:

1. **Status:** zeigt das Ergebnis eines Tests auf einem bestimmten Prüfpunkt an.
    - Ein grünes Häkchen bedeutet, dass der Prüfpunkt ordnungsgemäß konfiguriert ist.
    - Ein blaues I bedeutet, dass zu dem Prüfpunkt Informationen vorhanden sind.
    - Ein rotes X bedeutet, dass der Prüfpunkt nicht ordnungsgemäß konfiguriert ist.
2. **Anbieter:** zeigt den Namen des Moduls an, auf dem der Test ausgeführt wird. In diesem Fall Single Sign-On.
3. **Suite:** die Kategorie des Tests. Beispiel: Installation.
4. **Test:** der Name des Tests, der ausgeführt wird.
5. **Details:** zusätzliche Informationen über den Test.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Der Benutzer erhält weitere Informationen zu den einzelnen Prüfpunkten und den entsprechenden Ergebnissen.

Die folgenden Tests werden ausgeführt:

1. Installation mit Single Sign-On.
2. Erfassen der Anmeldeinformationen.
3. Registrierung von Netzwerkanbieter: Das Testergebnis für "Registrierung von Netzwerkanbieter"hat nur ein grünes Häkchen, wenn "Citrix Single Sign-On"als erster Netzwerkanbieter festgelegt ist. Wenn "Citrix Single Sign-On"an einer weiteren Stelle in der Liste steht, werden neben dem Testergebnis für "Registrierung von Netzwerkanbieter"ein blaues I und zusätzliche Informationen angezeigt.
4. Single Sign-On-Prozess wird ausgeführt.
5. Gruppenrichtlinie: Diese Richtlinie ist standardmäßig auf dem Client konfiguriert.
6. Interneteinstellungen für Sicherheitszonen: Stellen Sie sicher, dass Sie die Store-/XenApp-Dienst-URL der Liste der Sicherheitszonen in den Internetoptionen hinzufügen.
   Wenn die Sicherheitszonen per Gruppenrichtlinie konfiguriert sind, erfordern Änderungen in der Richtlinie das erneute Öffnen des Fensters **Erweiterte Einstellungen**, damit die Änderungen wirksam werden und der richtige Teststatus angezeigt wird.
7. Authentifizierungsmethode für das Webinterface oder StoreFront.

> **Hinweis:**
>
> - Die Testergebnisse gelten nicht für Workspace für Web-Konfigurationen.
> - Bei mehreren konfigurierten Stores wird die Authentifizierungsmethode auf jedem Store getestet.
> - Sie können die Testergebnisse als Berichte speichern. Das Standardberichtformat ist TXT.

Ausblenden der Konfigurationsprüfung im Fenster "Erweiterte Einstellungen"

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie zu **Citrix Komponenten** > **Citrix Workspace** > **Self-Service** > **DisableConfigChecker**.
3. Klicken Sie auf **Aktiviert**, um die Option "Konfigurationsprüfung"im Fenster **Erweiterte Einstellungen** auszublenden.
4. Klicken Sie auf **Anwenden** und auf **OK**.
5. Führen Sie den Befehl `gpupdate /force` aus.

Beschränkung:

Die Konfigurationsprüfung enthält nicht den Prüfpunkt für die Konfiguration von "An XML-Dienst gesendeten Anfragen vertrauen"auf dem VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Beacontest Der Beacon Checker ist Teil der **Konfigurationsprüfung**. Mit diesem Test können Sie prüfen, ob der Beacon (ping.citrix.com) erreichbar ist. Dies hilft Ihnen, eine der vielen möglichen Ursachen für eine langsame Ressourcenenumeration (Beacon nicht verfügbar) zu eliminieren. Um den Test auszuführen, klicken Sie mit der rechten Maustaste auf die Citrix Workspace-App im Infobereich und wählen Sie **Erweiterte Einstellungen** > **Konfigurationsprüfung**. Wählen Sie aus der Liste der Tests **Beacon checker** und klicken Sie auf **Ausführen**.

Der Test kann folgende Ergebnisse haben:

- Erreichbar: Die Citrix Workspace-App kann den Beacon erfolgreich kontaktieren.
- Nicht erreichbar: Die Citrix Workspace-App kann den Beacon nicht kontaktieren.
- Teilweise erreichbar: Die Citrix Workspace-App kann den Beacon sporadisch kontaktieren.

Domänen-Passthrough-Authentifizierung mit Kerberos

Dieser Abschnitt gilt nur für Verbindungen zwischen der Citrix Workspace-App für Windows und StoreFront, Citrix Virtual Apps and Desktops und Citrix DaaS.

Die Citrix Workspace-App für Windows unterstützt Kerberos für Domänen-Passthrough-Authentifizierung in Bereitstellungen mit Smartcardverwendung. Kerberos ist eine der in der integrierten Windows-Authentifizierung (IWA) enthaltenen Authentifizierungsmethoden.

Kerberos handhabt die Authentifizierung ohne Kennwörter für die Citrix Workspace-App und verhindert so trojanerartige Angriffe auf Benutzergeräte, die den Zugriff auf Kennwörter zum Ziel haben. Die Benutzer können sich mit einer beliebigen Authentifizierungsmethode anmelden und auf veröffentlichte Ressourcen zugreifen. Beispiel wäre eine biometrische Authentifizierung, etwa ein Fingerabdruckleser.

Sind die Citrix Workspace-App, StoreFront sowie Citrix Virtual Apps and Desktops und Citrix DaaS für die Smartcard-Authentifizierung konfiguriert, geschieht bei der Anmeldung bei der Citrix Workspace-App mit einer Smartcard Folgendes:

1. Die App erfasst die Smartcard-PIN beim Single Sign-On.
2. Die App authentifiziert den Benutzer mit IWA (Kerberos) bei StoreFront. StoreFront stellt der Citrix Workspace-App dann Informationen zum verfügbaren Citrix Virtual Apps and Desktops und Citrix DaaS bereit.

> **Hinweis**
>
> Aktivieren Sie Kerberos, um eine zusätzliche PIN-Eingabeaufforderung zu vermeiden. Wird die Kerberos-Authentifizierung nicht verwendet, führt die Citrix Workspace-App mit den Smartcard-Anmeldeinformationen eine Authentifizierung bei StoreFront durch.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Die HDX Engine übergibt die Smartcard-PIN an den VDA, um den Benutzer an der Citrix Workspace-App-Sitzung anzumelden. Citrix Virtual Apps and Desktops und Citrix DaaS stellen dann die angeforderten Ressourcen bereit.

Stellen Sie zur Verwendung der Kerberos-Authentifizierung bei der Citrix Workspace-App sicher, dass die Kerberos-Konfiguration folgenden Punkten entspricht.

- Kerberos funktioniert nur zwischen Citrix Workspace-App und Servern, die zu denselben oder vertrauenswürdigen Windows Server-Domänen gehören. Den Servern muss außerdem für Delegierungszwecke vertraut werden, eine Option, die Sie über das Verwaltungstool Active Directory-Benutzer und -Computer konfigurieren können.
- Kerberos muss sowohl in der Domäne als auch in Citrix Virtual Apps and Desktops und Citrix DaaS aktiviert sein. Um hohe Sicherheit und die Verwendung von Kerberos zu gewährleisten, deaktivieren Sie in der Domäne alle IWA-Optionen außer Kerberos.
- Kerberos-Anmeldung ist nicht verfügbar für Remotedesktopdienste-Verbindungen, die eine Standardauthentifizierung oder immer vorgegebene Anmeldeinformationen verwenden oder die immer zur Eingabe des Kennworts auffordern.

> **Warnung**
>
> Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Domänen-Passthrough-Authentifizierung mit Kerberos für die Verwendung mit Smartcards

Lesen Sie die Smartcard-Informationen im Abschnitt Sichern der Bereitstellung in der Citrix Virtual Apps and Desktops-Dokumentation, bevor Sie fortfahren.

Wenn Sie die Citrix Workspace-App für Windows installieren, fügen Sie die folgende Befehlszeilenoption hinzu:

- `/includeSSON`

  Mit dieser Option wird die Single Sign-On-Komponente auf dem in die Domäne eingebundenen Computer installiert, sodass der Workspace mit IWA (Kerberos) die Authentifizierung bei StoreFront durchführen kann. Die Single Sign-On-Komponente speichert die Smartcard-PIN, mit der die HDX Engine eine Remoteverbindung zwischen Smartcard-Hardware und -Anmeldeinformationen und Citrix Virtual Apps and Desktops und Citrix DaaS herstellt. Citrix

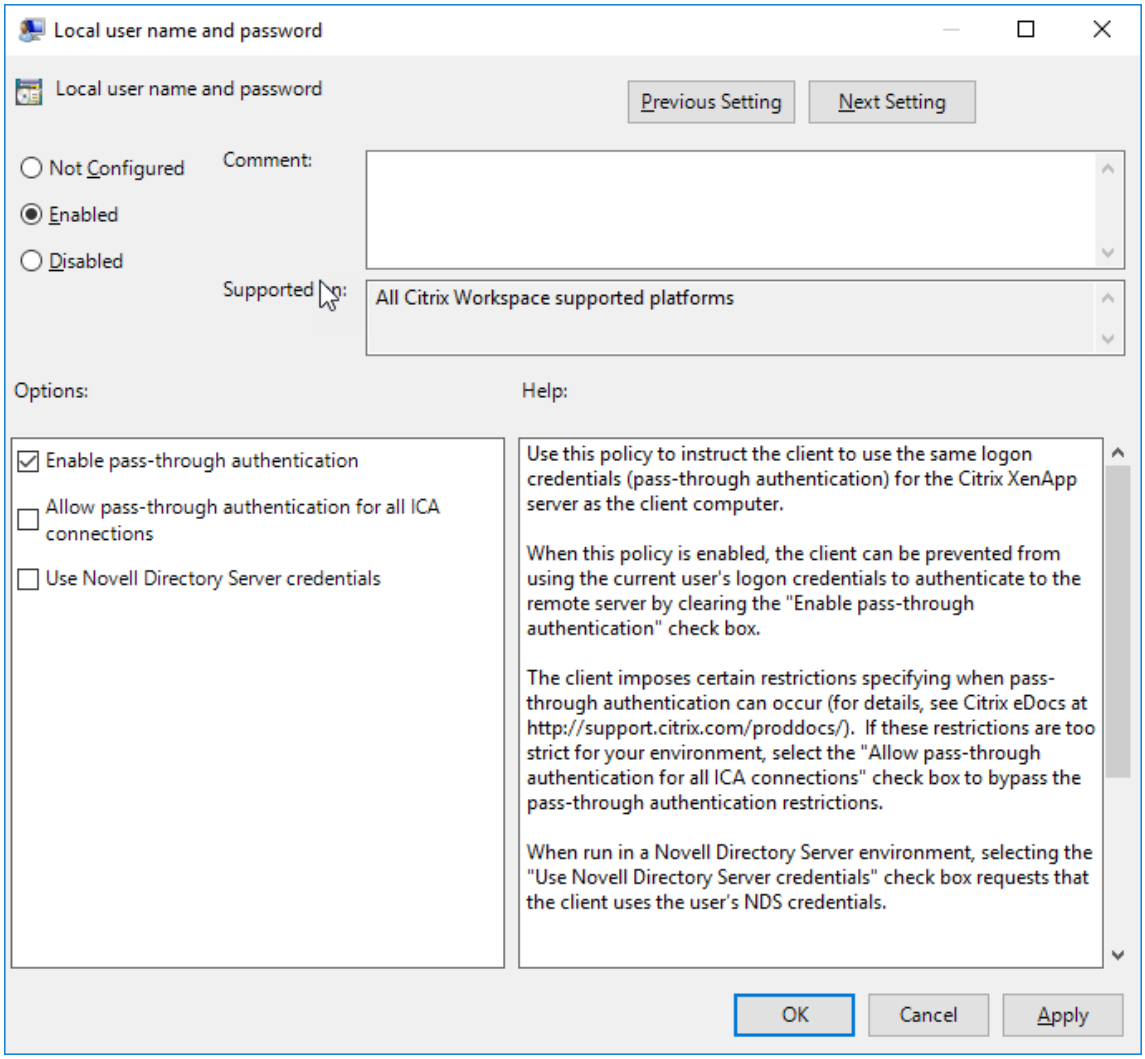
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Virtual Apps and Desktops und Citrix DaaS wählen automatisch ein Zertifikat von der Smartcard aus und rufen die PIN von der HDX Engine ab.

Die verwandte Option `ENABLE\\_SSON` ist standardmäßig aktiviert.

Wenn Sie Single Sign-On aufgrund einer Sicherheitsrichtlinie auf einem Gerät nicht aktivieren können, konfigurieren Sie die Citrix Workspace-App mit der administrativen Gruppenrichtlinienobjektsvorlage.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Wählen Sie **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzerauthentifizierung** > **Lokaler Benutzername und Kennwort**.
3. Wählen Sie **Passthrough-Authentifizierung aktivieren**.
4. Starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

StoreFront konfigurieren:

Wenn Sie den Authentifizierungsdienst auf dem StoreFront-Server konfigurieren, aktivieren Sie die Option Domänen-Passthrough. Mit dieser Einstellung wird die integrierte Windows-Authentifizierung aktiviert. Die Option "Smartcard"muss nur aktiviert werden, wenn Sie auch Clients haben, die nicht in Domänen eingebunden sind und mit Smartcards eine Verbindung mit StoreFront herstellen.

Weitere Informationen zur Verwendung von Smartcards mit StoreFront finden Sie unter Konfigurieren des Authentifizierungsdiensts in der StoreFront-Dokumentation.

Smartcard

Citrix Workspace-App für Windows unterstützt folgende Smartcardauthentifizierung.

- **Passthrough-Authentifizierung (Single Sign-On):** Die Passthrough-Authentifizierung erfasst Smartcard-Anmeldeinformationen, wenn sich Benutzer bei der Citrix Workspace-App anmelden. Die Citrix Workspace-App verwendet die erfassten Anmeldeinformationen wie folgt:

  - Benutzer von in Domänen eingebundenen Geräten, die sich mit Smartcard-Anmeldeinformationen bei der Citrix Workspace-App anmelden, starten virtuelle Desktops und Anwendungen ohne erneute Authentifizierung.
  - Bei Citrix Workspace-App auf Geräten, die nicht in Domänen eingebunden sind und Smartcardauthentifizierung verwenden, müssen Benutzer die Anmeldeinformationen erneut eingeben, um Desktops oder Apps zu starten.

  StoreFront und die Citrix Workspace-App müssen beide für die Passthrough-Authentifizierung konfiguriert werden.

- **Bimodale Authentifizierung:** Bei der bimodalen Authentifizierung können die Benutzer zwischen einer Smartcard und der Eingabe des Benutzernamens und des Kennworts wählen. Das Feature eignet sich für Fälle, wenn keine Smartcard verwendet werden kann. Beispielsweise wenn das Anmeldezertifikat abgelaufen ist. Für die bimodale Authentifizierung müssen dedizierte Stores pro Site eingerichtet werden, damit die Methode **DisableCtrlAltDel** zur Smartcardverwendung auf **False** festgelegt werden kann. Die bimodale Authentifizierung erfordert eine StoreFront-Konfiguration.

  Mit der bimodalen Authentifizierung kann der StoreFront-Administrator die Authentifizierung über Benutzernamen/Kennwort und per Smartcard bei dem gleichen Store durch Auswahl in der StoreFront-Konsole zulassen. Weitere Informationen finden Sie in der StoreFront-Dokumentation.

- **Mehrere Zertifikate:** Mehrere Zertifikate können für eine Smartcard verfügbar sein, wenn mehrere Smartcards verwendet werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Clientzertifikatauthentifizierung:** Citrix Gateway und StoreFront müssen für die Clientzertifikatauthentifizierung konfiguriert werden.
  - Für den Zugriff auf StoreFront über Citrix Gateway ist ggf. nach dem Entfernen der Smartcard eine erneute Authentifizierung erforderlich.
  - Wenn die SSL-Konfiguration von Citrix Gateway auf die verbindliche Clientzertifikatauthentifizierung eingestellt ist, ist der Betrieb sicherer. Die verbindliche Clientzertifikatauthentifizierung ist jedoch nicht mit der bimodalen Authentifizierung kompatibel.
- **Double-Hop-Sitzungen:** Wenn ein Double Hop benötigt wird, wird eine Verbindung zwischen Citrix Workspace-App und dem virtuellen Desktop des Benutzers hergestellt. Bereitstellungen, die Double Hop unterstützen, werden in der Citrix Virtual Apps and Desktops-Dokumentation beschrieben.
- **Smartcard-aktivierte Anwendungen:** In smartcard-aktivierten Anwendungen, wie Microsoft Outlook und Microsoft Office, können Benutzer Dokumente, die in Sitzungen mit virtuellen Apps und Desktops verfügbar sind, digital signieren oder verschlüsseln.

Einschränkungen:

- Zertifikate müssen auf einer Smartcard und nicht auf dem Benutzergerät gespeichert sein.
- Die Zertifikatauswahl wird in der Citrix Workspace-App nicht gespeichert, es wird jedoch bei entsprechender Konfiguration die PIN gespeichert. Die PIN wird nur im nicht ausgelagerten Speicher zwischengespeichert. Sie wird nicht auf der Festplatte gespeichert.
- Die Citrix Workspace-App stellt die Verbindung mit einer Sitzung nicht wieder her, wenn eine Smartcard eingesteckt wird.
- Wenn die Citrix Workspace-App für die Smartcardauthentifizierung konfiguriert ist, wird VPN-Single Sign-On oder Sitzungsvorabstart nicht unterstützt. Für die Verwendung von VPN mit der Smartcardauthentifizierung müssen die Benutzer das Citrix Gateway Plug-In installieren, sich über eine Webseite anmelden und sich mit den Smartcards und PINs bei jedem Schritt authentifizieren. Die Passthrough-Authentifizierung bei StoreFront mit dem Citrix Gateway Plug-In ist für Smartcardbenutzer nicht verfügbar.
- Die Kommunikation des Updater-Tools der Citrix Workspace-App mit citrix.com und Merchandising Server ist nicht mit der Smartcardauthentifizierung auf Citrix Gateway kompatibel.

> **Warnung**
>
> Einige Konfigurationen erfordern Registrierungsänderungen. Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Single Sign-On für die Smartcardauthentifizierung aktivieren:

Fügen Sie zum Konfigurieren der Citrix Workspace-App für Windows bei der Installation die folgende Befehlszeilenoption hinzu:

- `ENABLE\\_SSON=Yes`

  Single Sign-On ist ein anderer Begriff für Passthrough-Authentifizierung. Wenn diese Einstellung aktiviert ist, zeigt die Citrix Workspace-App keine zweite PIN-Eingabeaufforderung an.

- Wenn die Single Sign-On-Komponente nicht installiert ist, legen Sie **SSONCheckEnabled** auf "false"fest. Der Schlüssel verhindert, dass der Authentifizierungsmanager der Citrix Workspace-App nach der Single Sign-On-Komponente sucht, sodass die Citrix Workspace-App die Authentifizierung bei StoreFront durchführen kann.

  `HKEY\\_CURRENT\\_USER\Software\Citrix\AuthManager\protocols\integratedwindows\`

  `HKEY\\_LOCAL\\_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows\`

Zum Aktivieren der Smartcardauthentifizierung bei StoreFront anstelle von Kerberos installieren Sie die Citrix Workspace-App mit den aufgeführten Befehlszeilenoptionen:

- `/includeSSON` installiert die Single Sign-On-Authentifizierung (Passthrough-Authentifizierung). Aktiviert das Zwischenspeichern der Anmeldeinformationen und die Verwendung der domänenbasierten Passthrough-Authentifizierung.
- Wenn sich der Benutzer beim Endpunkt mit einer anderen Authentifizierungsmethode für Citrix Workspace-App als per Smartcard anmeldet (z. B. mit Benutzername und Kennwort), verwenden Sie folgende Befehlszeile:

  `/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No`

Hierdurch wird verhindert, dass die Anmeldeinformationen bei der Anmeldung erfasst werden, und ermöglicht, dass die PIN durch die Citrix Workspace-App bei der Anmeldung an der Citrix Workspace-App gespeichert wird.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Wählen Sie **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzerauthentifizierung** > **Lokaler Benutzername und Kennwort**.
3. Wählen Sie **Passthrough-Authentifizierung aktivieren**. Je nach Konfiguration und Sicherheitseinstellungen müssen Sie möglicherweise die Option **Passthrough-Authentifizierung für alle ICA-Verbindungen zulassen** aktivieren, damit die Passthrough-Authentifizierung funktioniert.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

StoreFront konfigurieren:

- Wenn Sie den Authentifizierungsdienst konfigurieren, aktivieren Sie das Kontrollkästchen **Smartcard**.

Weitere Informationen zur Verwendung von Smartcards mit StoreFront finden Sie unter Konfigurieren des Authentifizierungsdiensts in der StoreFront-Dokumentation.

Aktivieren der Benutzergeräte für die Smartcardverwendung:

1. Importieren Sie das Stammzertifikat der Zertifizierungsstelle in den Schlüsselspeicher des Geräts.
2. Installieren Sie die kryptografische Middleware.
3. Installieren und konfigurieren Sie die Citrix Workspace-App.

Ändern der Zertifikatauswahl:

Wenn mehrere Zertifikate gültig sind, fordert die Citrix Workspace-App den Benutzer standardmäßig auf, ein Zertifikat aus der Liste auszuwählen. Sie können die Citrix Workspace-App auch so konfigurieren, dass das Standardzertifikat (gemäß Smartcardanbieter) oder das Zertifikat mit dem spätesten Ablaufdatum verwendet wird. Wenn keine gültigen Anmeldezertifikate vorhanden sind, wird der Benutzer benachrichtigt und kann eine alternative Anmeldemethode (falls vorhanden) verwenden.

Ein gültiges Zertifikat muss die drei folgenden Merkmale haben:

- Die aktuelle Uhrzeit auf dem lokalen Computer liegt im Gültigkeitszeitraum des Zertifikats.
- Der **öffentliche Schlüssel des Subjekts** muss den RSA-Algorithmus verwenden und eine Schlüssellänge von 1024, 2048 oder 4096 Bit haben.
- Die Schlüsselverwendung muss digitale Signatur enthalten.
- Der alternative Name des Subjekts muss den UPN enthalten.
- Die erweiterte Schlüsselverwendung muss Smartcard-Anmeldung und Clientauthentifizierung oder alle Schlüsselverwendungen enthalten.
- Eine der Zertifizierungsstellen in der Ausstellerkette des Zertifikats muss mit einem der Distinguished Names übereinstimmen, den der Server im TLS-Handshake sendet.

Ändern Sie mit einer der folgenden Methoden, wie Zertifikate ausgewählt werden:

- Geben Sie in der Befehlszeile der Citrix Workspace-App die Option `AM\_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }` an.

  Prompt ist der Standard. Wenn mehrere Zertifikate die Anforderungen erfüllen, fordert Citrix Workspace für “SmartCardDefault”oder “LatestExpiry”den Benutzer zur Auswahl eines Zertifikats auf.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fügen Sie den folgenden Schlüsselwert dem Registrierungsschlüssel HKEY_CURRENT_USER oder HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\AuthManager hinzu: CertificateSelectionMode={ Prompt	SmartCardDefault	LatestExpiry }.

-

In HKEY_CURRENT_USER definierte Werte haben Priorität über Werte in HKEY_LOCAL_MACHINE, um dem Benutzer die Auswahl des Zertifikats zu erleichtern.

CSP-PIN-Aufforderungen verwenden:

Die PIN-Aufforderungen, die den Benutzern angezeigt werden, werden standardmäßig von der Citrix Workspace-App für Windows und nicht von dem Smartcard-Kryptografiedienstanbieter bereitgestellt. Die Citrix Workspace-App fordert die Benutzer bei Bedarf zur Eingabe einer PIN auf und übergibt die PIN an den Smartcard-Kryptografiedienstanbieter. Wenn die Site oder Smartcard strengere Sicherheitsanforderungen hat, z. B. kein Zwischenspeichern der PIN pro Prozess oder pro Sitzung, können Sie in der Citrix Workspace-App konfigurieren, dass die PIN-Eingabe, einschließlich der Aufforderung für eine PIN, von den CSP-Komponenten verwaltet wird.

Ändern Sie mit einer der folgenden Methoden, wie die PIN-Eingabe gehandhabt wird:

- Geben Sie in der Befehlszeile der Citrix Workspace-App die Option `AM\_SMARTCARDPINENTRY=CSP` an.
- Fügen Sie dem Registrierungsschlüssel HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\AuthMana den folgenden Schlüsselwert hinzu: SmartCardPINEntry=CSP.

Änderungen bei der Unterstützung und Entfernung von Smartcards

Berücksichtigen Sie Folgendes, wenn Sie eine Verbindung mit einer XenApp 6.5 PNAgent-Site herstellen:

- Die Smartcard-Anmeldung wird für PNAgent-Siteanmeldungen unterstützt.
- Für die Richtlinie zum Entfernen von Smartcards in der PNAgent-Site gilt folgende Änderung:

Eine Citrix Virtual Apps-Sitzung wird abgemeldet, wenn die Smartcard entfernt wird. Wenn Smartcard als Authentifizierungsmethode für die PNAgent-Site konfiguriert ist, muss die entsprechende Richtlinie in der Citrix Workspace-App für Windows konfiguriert sein, damit das Abmelden der Citrix

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Virtual Apps-Sitzung erzwungen werden kann. Aktivieren Sie das Roaming für die Smartcardauthentifizierung in der XenApp PNAgent-Site und aktivieren Sie die Richtlinie für das Entfernen von Smartcards, durch die Citrix Virtual Apps von der Citrix Workspace-App-Sitzung abgemeldet wird. Der Benutzer bleibt an der Citrix Workspace-App-Sitzung angemeldet.

Beschränkung:

Wenn Sie sich an der PNAgent-Site per Smartcardauthentifizierung anmelden, wird der Benutzername als **Angemeldet** angezeigt.

Sichere Kommunikation

April 22, 2024

Zum Sichern der Kommunikation zwischen dem Citrix Virtual Apps and Desktops-Server und der Citrix Workspace-App können Sie Citrix Workspace-App-Verbindungen mit sicheren Technologien wie den Folgenden integrieren:

- Citrix Gateway: Weitere Informationen finden Sie im vorliegenden Abschnitt und in der Dokumentation zu Citrix Gateway und StoreFront.

  > **Hinweis:**
  >
  > Citrix empfiehlt die Verwendung von Citrix Gateway zwischen StoreFront-Servern und Benutzergeräten.

- Eine Firewall: Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie die Citrix Workspace-App mit einer Firewall verwenden, die die interne Netzwerk-IP-Adresse des Servers einer externen Internetadresse zuweist (d. h. Netzwerkadressübersetzung oder NAT), konfigurieren Sie die externe Adresse.
- Vertrauenswürdige Server.
- Nur für Citrix Virtual Apps- oder Webinterface-Bereitstellungen (gilt nicht für XenDesktop 7): ein SOCKS-Proxyserver oder ein sicherer Proxyserver (auch Sicherheitsproxyserver bzw. HTTPS-Proxyserver). Mit Proxyservern schränken Sie den eingehenden und ausgehenden Zugriff auf das Netzwerk ein und handhaben Verbindungen zwischen der Citrix Workspace-App und Servern. Die Citrix Workspace-App unterstützt die Protokolle SOCKS und Secure Proxy.
- Nur für Citrix Virtual Apps- oder Webinterface-Bereitstellungen, gilt nicht für XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 und XenApp 7.5: SSL-Relay-Lösungen mit TLS-Protokollen (Transport Layer Security).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Für Citrix Virtual Apps and Desktops 7.6 können Sie eine SSL-Verbindung direkt zwischen Benutzern und VDAs aktivieren.

Unterstützung für den ausgehenden Proxy

Mit SmartControl können Administratoren detaillierte Richtlinien definieren, um mit Citrix Gateway Benutzerumgebungsattribute für Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktop Service) zu konfigurieren und durchzusetzen. Beispielsweise können Sie verhindern, dass Benutzer ihren Remotedesktops weitere Laufwerke zuordnen. Dies ermöglicht das SmartControl-Feature von Citrix Gateway.

Das Szenario ändert sich jedoch, wenn die Citrix Workspace-App und Citrix Gateway zu separaten Unternehmenskonten gehören. In diesem Fall kann die Clientdomäne das SmartControl-Feature nicht anwenden, da das Gateway in der Clientdomäne fehlt. Stattdessen können Sie den ausgehenden ICA-Proxy nutzen. Mit dem ausgehenden ICA-Proxy können Sie das SmartControl-Feature auch dann verwenden, wenn die Citrix Workspace-App und Citrix Gateway in verschiedenen Organisationen bereitgestellt sind.

Die Citrix Workspace-App unterstützt Sitzungsstarts mit dem NetScaler LAN-Proxy. Entweder wird ein einzelner statischer Proxy konfiguriert, oder der Proxyserver wird zur Laufzeit über das Plug-In für ausgehende Proxys ausgewählt.

Es gibt folgende Konfigurationsmethoden für ausgehende Proxys:

- Statischer Proxy: Der Proxyserver wird durch Angabe eines Proxy-Hostnamen und der Portnummer konfiguriert.
- Dynamischer Proxy: Ein einzelner Proxyserver wird mit der Proxy-Plug-In-DLL unter einem oder mehreren Proxyservern ausgewählt.

Sie können den ausgehenden Proxy mit der administrativen Gruppenrichtlinienobjektvorlage und dem Registrierungs-Editor konfigurieren.

Weitere Informationen zum ausgehenden Proxy finden Sie unter Unterstützung für den ausgehenden ICA-Proxy in der Citrix Gateway-Dokumentation.

Unterstützung für den ausgehenden Proxy - Konfiguration

> **Hinweis:**
>
> Wenn statische und dynamische Proxys konfiguriert sind, hat die Konfiguration des dynamischen Proxys Vorrang.

Konfigurieren des ausgehenden Proxys mit der administrativen GPO-Vorlage:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Netzwerkrouting**.
3. Wählen Sie eine der folgenden Optionen:

    - Statischer Proxy: Wählen Sie die Richtlinie **NetScaler LAN-Proxy manuell konfigurieren**. Wählen Sie **Aktiviert** und geben Sie den Hostnamen und die Portnummer ein.
    - Dynamischer Proxy: Wählen Sie die Richtlinie **NetScaler LAN-Proxy mit DLL konfigurieren**. Wählen Sie **Aktiviert** und geben Sie den vollständigen Pfad zur DLL-Datei ein. Beispiel: `C:\Workspace\Proxy\ProxyChooser.dll`.

4. Klicken Sie auf **Anwenden** und auf **OK**.

Konfigurieren des ausgehenden Proxys mit dem Registrierungs-Editor:

- **Statischer Proxy:**

    - Starten Sie den Registrierungs-Editor und navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler`.
    - Erstellen Sie folgende DWORD-Wertschlüssel:

      ```
      "StaticProxyEnabled"=dword:00000001
      "ProxyHost"="testproxy1.testdomain.com
      "ProxyPort"=dword:000001bb
      ```

- **Dynamischer Proxy:**

    - Starten Sie den Registrierungs-Editor und navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler LAN Proxy`.
    - Erstellen Sie folgende DWORD-Wertschlüssel:
      ```
      "DynamicProxyEnabled"=dword:00000001
      "ProxyChooserDLL"="c:\\Workspace\\Proxy\\ProxyChooser.dll"
      ```

TLS

Dieses Thema gilt für Citrix Virtual Apps and Desktops-Version 7.6 und höher.

Wenn Sie ausschließlich TLS-Verschlüsselung für die Kommunikation der Citrix Workspace-App verwenden möchten, konfigurieren Sie das Benutzergerät, die Citrix Workspace-App und, wenn Sie das Webinterface verwenden, den Webinterface-Server. Informationen zum Sichern der StoreFront-Kommunikation finden Sie unter Sichern in der StoreFront-Dokumentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Voraussetzungen:

Benutzergeräte müssen die in den Systemanforderungen angegebenen Anforderungen erfüllen.

Diese Richtlinie ermöglicht das Konfigurieren der TLS-Optionen, sodass die Citrix Workspace-App den Server für die Verbindung sicher identifizieren kann, und sie ermöglicht die Verschlüsselung der gesamten Kommunikation mit dem Server.

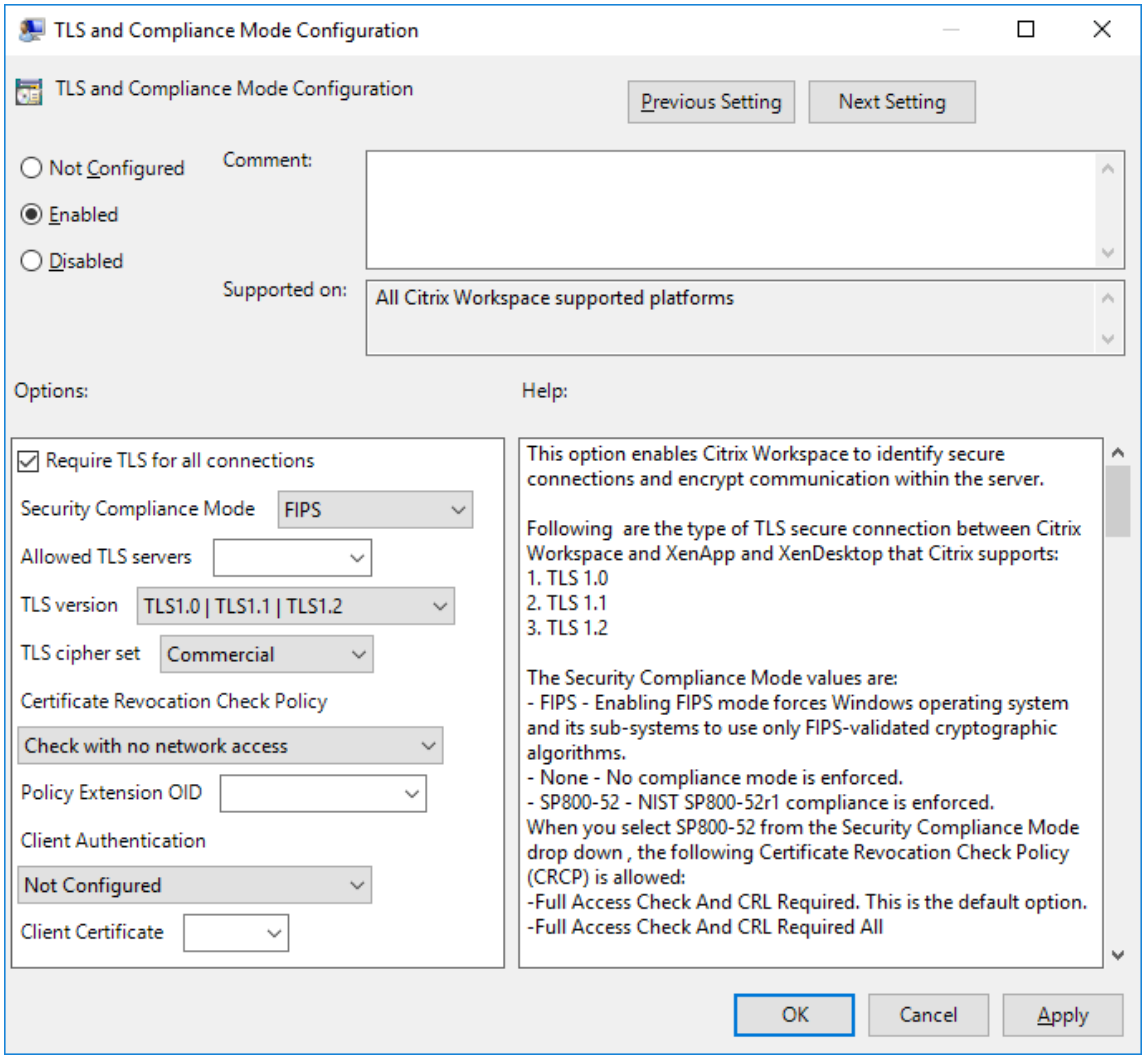
Diese Optionen ermöglichen Folgendes:

- Erzwingen der Verwendung von TLS: Citrix empfiehlt, für alle Verbindungen über nicht vertrauenswürdige Netzwerke, einschließlich für das Internet, TLS zu verwenden.
- Erzwingen der Verwendung der für FIPS (Federal Information Processing Standards): genehmigte Kryptografie und Einhalten der Empfehlungen im Dokument NIST SP 800-52. Diese Optionen sind standardmäßig deaktiviert.
- Erzwingen der Verwendung einer bestimmten Version von TLS und bestimmter TLS-Verschlüsselungssammlungen: Citrix unterstützt die Protokolle TLS 1.0, TLS 1.1 und TLS 1.2 zwischen der Citrix Workspace-App für Windows und Citrix Virtual Apps and Desktops und Citrix DaaS.
- Herstellen von Verbindungen mit bestimmten Servern.
- Überprüfen, ob das Serverzertifikat widerrufen wurde.
- Überprüfen auf eine bestimmte Serverzertifikatausstellungsrichtlinie.
- Auswählen eines bestimmten Clientzertifikats, wenn der Server für die Anforderung konfiguriert ist.

Unterstützung für TLS

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Netzwerkrouting**. Wählen Sie dann die Richtlinie **Konfiguration von TLS und Konformitätsmodus**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Wählen Sie **Aktiviert**, um sichere Verbindungen zu aktivieren und die Kommunikation auf dem Server zu verschlüsseln. Legen Sie folgende Optionen fest:

> **Hinweis:**
>
> Citrix empfiehlt TLS für sichere Verbindungen.

   a) Aktivieren Sie **TLS für alle Verbindungen verwenden**. Damit erzwingen Sie, dass die Citrix Workspace-App TLS für alle Verbindungen mit veröffentlichten Anwendungen und Desktops verwendet.

   b) Wählen Sie im Menü **Sicherheitskonformitätsmodus** die geeignete Option aus:

      i. **Ohne:** Es wird kein Konformitätsmodus erzwungen.
      ii. **SP800-52:** Wählen Sie **SP800-52** für Konformität mit NIST SP 800-52. Wählen Sie diese Option nur, wenn Server oder Gateway den Empfehlungen von NIST SP 800-52 entsprechen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Bei Auswahl von **SP800-52** wird automatisch FIPS-validierte Kryptografie verwendet, selbst wenn **FIPS aktivieren** nicht ausgewählt ist. Sie müssen auch die Windows-Sicherheitsoption **Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden aktivieren**. Andernfalls kann die Citrix Workspace-App u. U. keine Verbindung zu den veröffentlichten Anwendungen und Desktops herstellen.

Wenn Sie **SP800-52** auswählen, müssen Sie für die Richtlinie **Zertifikatsperrüberprüfung** die Einstellung **Volle Zugriffsprüfung** oder **Volle Zugriffsprüfung und CRL erforderlich** auswählen.

Wenn Sie **SP800-52** auswählen, überprüft die Citrix Workspace-App, ob das Serverzertifikat den Empfehlungen in NIST SP 800-52 entspricht. Wenn dies nicht der Fall ist, kann die Citrix Workspace-App möglicherweise keine Verbindung herstellen.

i. **FIPS aktivieren**: Wählen Sie diese Option, um die Verwendung von FIPS-validierter Kryptografie zu erzwingen. Sie müssen auch die Windows-Sicherheitsoption aus der Gruppenrichtlinie des Betriebssystems **Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden** aktivieren. Andernfalls kann die Citrix Workspace-App u. U. keine Verbindung zu veröffentlichten Anwendungen und Desktops herstellen.

c) Wählen Sie im Dropdownmenü neben **Zulässige TLS-Server** die Portnummer aus. Sie können festlegen, dass die Citrix Workspace-App für Windows nur eine Verbindung zu den Servern herstellt, die in einer durch Trennzeichen getrennten Liste aufgeführt sind. Sie können Platzhalter und Portnummern angeben. Beispielsweise ermöglicht *.citrix.com:4433 die Verbindung mit allen Servern auf Port 4433, deren allgemeiner Name mit .citrix.com endet. Die Genauigkeit der Informationen in einem Sicherheitszertifikat wird durch den Aussteller des Zertifikats bestätigt. Wenn Citrix Workspace den Aussteller nicht erkennt und ihm nicht traut, wird die Verbindung abgelehnt.

d) Wählen Sie im Menü **TLS-Version** eine der folgenden Optionen:

- **TLS 1.0, TLS 1.1 oder TLS 1.2**: Dies ist die Standardeinstellung. Diese Option wird nur empfohlen, wenn die Kompatibilität mit TLS 1.0 eine Geschäftsanforderung ist.
- **TLS 1.1, TLS 1.2**: Mit dieser Option stellen Sie sicher, dass TLS 1.1 oder TLS 1.2 für ICA-Verbindungen verwendet wird.
- **TLS 1.2**: Diese Option wird empfohlen, wenn TLS 1.2 eine Geschäftsanforderung ist.

a) **TLS-Verschlüsselungssatz**: Um die Verwendung von bestimmten TLS-Verschlüsselungssätzen zu erzwingen, wählen Sie “Behörden”(GOV), “Kommerziell”(COM) oder “Alle”(ALLE). Bei

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

bestimmten Citrix Gateway-Konfigurationen müssen Sie u. U. die Option **COM** wählen. Die Citrix Workspace-App unterstützt RSA-Schlüssellängen von 1024, 2048 und 3072 Bits. Darüber hinaus werden Stammzertifikate mit RSA-Schlüsseln von 4096 Bits Länge unterstützt.

> **Hinweis:**
>
> RSA-Schlüssel mit einer Länge von 1024 Bits werden von Citrix nicht empfohlen.

- **Beliebig**: Bei Verwendung der Einstellung "Beliebig"wird die Richtlinie nicht konfiguriert und jede der folgenden Verschlüsselungssammlungen ist zulässig:

  a) TLS_RSA_WITH_RC4_128_MD5
  b) TLS_RSA_WITH_RC4_128_SHA
  c) TLS_RSA_WITH_3DES_EDE_CBC_SHA
  d) TLS_RSA_WITH_AES_128_CBC_SHA
  e) TLS_RSA_WITH_AES_256_CBC_SHA
  f) TLS_RSA_WITH_AES_128_GCM_SHA256
  g) TLS_RSA_WITH_AES_256_GCM_SHA384

- **Kommerziell**: Bei Verwendung der Einstellung "Kommerziell"sind nur die folgenden Verschlüsselungssammlungen zulässig:

  a) TLS_RSA_WITH_RC4_128_MD5
  b) TLS_RSA_WITH_RC4_128_SHA
  c) TLS_RSA_WITH_AES_128_CBC_SHA
  d) TLS_RSA_WITH_AES_128_GCM_SHA256

- **Behörden**: Bei Verwendung der Einstellung "Behörden"sind nur die folgenden Verschlüsselungssammlungen zulässig:

  a) TLS_RSA_WITH_AES_256_CBC_SHA
  b) TLS_RSA_WITH_3DES_EDE_CBC_SHA
  c) TLS_RSA_WITH_AES_128_GCM_SHA256
  d) TLS_RSA_WITH_AES_256_GCM_SHA384

a) Wählen Sie im Menü **Richtlinie 'Zertifikatsperrüberprüfung'** eine der folgenden Optionen aus:

- **Prüfung ohne Netzwerkzugriff**: Es wird eine Überprüfung der Zertifikatsperrliste durchgeführt. Es werden nur lokale Zertifikatsperrlisten-Stores verwendet. Alle Verteilungspunkte werden ignoriert. Das Finden einer Zertifikatsperrliste ist für die Überprüfung des Serverzertifikats, das vom Ziel-SSL-Relay bzw. Citrix Secure Web Gateway-Server vorgelegt wird, nicht obligatorisch.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Volle Zugriffsprüfung**: Es wird eine Überprüfung der Zertifikatsperrliste durchgeführt. Lokale Zertifikatsperrlistenspeicher und alle Verteilungspunkte werden verwendet. Wenn Sperrinformationen für ein Zertifikat gefunden werden, wird die Verbindung abgelehnt. Das Finden einer Zertifikatsperrliste ist für die Überprüfung des Serverzertifikats, das vom Zielserver vorgelegt wird, nicht wichtig.
- **Volle Zugriffsprüfung und CRL erforderlich**: Die Zertifikatsperrliste wird ohne Stamm-Zertifizierungsstelle überprüft. Lokale Zertifikatsperrlistenspeicher und alle Verteilungspunkte werden verwendet. Wenn Sperrinformationen für ein Zertifikat gefunden werden, wird die Verbindung abgelehnt. Das Finden aller erforderlichen Zertifikatsperrlisten ist für die Überprüfung wichtig.
- **Volle Zugriffsprüfung und alle CRL erforderlich**: Die Zertifikatsperrliste und die Stamm-Zertifizierungsstelle werden überprüft. Lokale Zertifikatsperrlistenspeicher und alle Verteilungspunkte werden verwendet. Wenn Sperrinformationen für ein Zertifikat gefunden werden, wird die Verbindung abgelehnt. Das Finden aller erforderlichen Zertifikatsperrlisten ist für die Überprüfung wichtig.
- **Keine Prüfung**: Es wird keine Überprüfung der Zertifikatsperrliste durchgeführt.

a) Mit der **Richtlinienerweiterungs-OID** können Sie die Citrix Workspace-App auf Verbindungen mit Servern beschränken, auf denen eine bestimmte Zertifikatausstellungsrichtlinie festgelegt ist. Wenn Sie **Richtlinienerweiterungs-OID** auswählen, akzeptiert die Citrix Workspace-App nur Serverzertifikate mit dieser Richtlinienerweiterungs-OID.

b) Wählen Sie im Menü zur **Clientauthentifizierung** eine der folgenden Optionen aus:

- **Deaktiviert**: Die Clientauthentifizierung ist deaktiviert.
- **Zertifikatauswähler anzeigen**: Der Benutzer wird immer aufgefordert, ein Zertifikat auszuwählen.
- **Wenn möglich automatisch auswählen**: Die Aufforderung wird nur angezeigt, wenn mehrere Zertifikate zur Identifizierung ausgewählt werden können.
- **Nicht konfiguriert**: Gibt an, dass die Clientauthentifizierung nicht konfiguriert ist.
- **Angegebenes Zertifikat verwenden**: Verwenden Sie das unter "Clientzertifikat" festgelegte Clientzertifikat.

a) Geben Sie mit der Einstellung **Clientzertifikat** den Fingerabdruck des identifizierenden Zertifikats an, damit Benutzer nicht unnötig aufgefordert werden.

b) Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.

Die folgende Tabelle enthält die Verschlüsselungssammlungen in jeder Gruppe:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ciphersuite	Native Cyrpto Kit mode and cipher set								
	Open			FIPS			SP800-52		
	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y		Y	Y		Y	Y	
TLS_RSA_WITH_AES_256_GCM_SHA384 (1) (2)	X								
TLS_RSA_WITH_AES_128_GCM_SHA256 (1) (2)	X	X							
TLS_RSA_WITH_AES_256_CBC_SHA256 (1) (2)	X								
TLS_RSA_WITH_AES_256_CBC_SHA (2)	X								
TLS_RSA_WITH_AES_128_CBC_SHA (2)	X	X							
TLS_RSA_WITH_RC4_128_SHA (2) (3)	X	X							
TLS_RSA_WITH_RC4_128_MD5 (2) (3)	X	X							
TLS_RSA_WITH_3DES_EDE_CBC_SHA (2)	X								
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	Y	Y	Y	Y	Y	Y	Y	Y	Y
Notes									
(1) Ciphersuites that require TLS1.2/DTLS 1.2									
(2) Ciphersuites disabled by default									
(3) Ciphersuites not available for DTLS protocol									
Y - Supported ciphersuites									
X-Deprecated ciphersuites									

Firewall

Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie eine Firewall in der Bereitstellung verwenden, muss die Citrix Workspace-App für Windows über die Firewall mit dem Webserver und dem Citrix Server kommunizieren können.

Allgemeine Citrix Kommunikationsports

Quelle	Typ	Port	Details
Citrix Workspace-App	TCP	80/443	Kommunikation mit StoreFront
ICA/HDX	TCP	1494	Zugriff auf Anwendungen und virtuelle Desktops
ICA/HDX mit Sitzungszuverlässigkeit	TCP	2598	Zugriff auf Anwendungen und virtuelle Desktops
ICA/HDX über SSL	TCP	443	Zugriff auf Anwendungen und virtuelle Desktops

Weitere Informationen zu Ports finden Sie im Knowledge Center-Artikel CTX101810.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenn die Firewall für die Netzwerkadressenübersetzung konfiguriert ist, definieren Sie im Webinterface Zuordnungen von internen Adressen zu externen Adressen und Ports. Beispiel: Wenn der Citrix Virtual Apps and Desktops-Server nicht mit einer alternativen Adresse konfiguriert ist, kann das Webinterface der Citrix Workspace-App eine alternative Adresse bereitstellen. Die Citrix Workspace-App stellt dann mit der externen Adresse und der Portnummer eine Verbindung mit dem Server her.

Proxyserver

Mit Proxyservern wird der eingehende und ausgehende Netzwerkzugriff beschränkt und die Verbindung zwischen der Citrix Workspace-App für Windows und Servern gehandhabt. Die Citrix Workspace-App unterstützt die Protokolle SOCKS und Secure Proxy.

Für die Kommunikation mit dem Server verwendet die Citrix Workspace-App die Proxyservereinstellungen, die remote auf dem Server konfiguriert sind, auf dem Workspace für Web oder das Webinterface ausgeführt wird. Informationen zur Proxyserverkonfiguration finden Sie in der StoreFront- oder Webinterface-Dokumentation.

Für die Kommunikation mit dem Webserver verwendet die Citrix Workspace-App die Einstellungen für den Proxyserver, die über die **Internetoptionen** des Standardwebbrowsers auf dem Benutzergerät konfiguriert wurden. Sie müssen die **Internetoptionen** des Standardwebbrowsers auf dem Benutzergerät entsprechend konfigurieren.

Konfigurieren Sie die Proxyeinstellungen mit dem Registrierungs-Editor, um zu erzwingen, dass die Citrix Workspace-App den Proxyserver für Verbindungen verwendet oder ihn ignoriert.

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können.

1. Navigieren Sie zu `\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\AuthManager`
2. Definieren Sie **ProxyEnabled** (REG_SZ).
    - True - gibt an, dass die Citrix Workspace-App den Proxyserver bei Verbindungen berücksichtigt.
    - False - gibt an, dass die Citrix Workspace-App den Proxyserver bei Verbindungen ignoriert.
3. Starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Vertrauenswürdige Server

Die Konfiguration von vertrauenswürdigen Servern dient dazu, Vertrauensstellungen bei Verbindungen der Citrix Workspace-App zu identifizieren und durchzusetzen.

Wenn Sie die Option für vertrauenswürdige Server aktivieren, legt die Citrix Workspace-App die Anforderungen für vertrauenswürdige Server fest und entscheidet, ob die Verbindung zum Server als vertrauenswürdig angesehen werden kann. Beispiel: Wenn die Citrix Workspace-App eine Verbindung mit einer bestimmten Adresse herstellt (wie `https://\*.citrix.com`) und dabei einen bestimmten Verbindungstyp verwendet (wie TLS), wird sie an eine vertrauenswürdige Zone auf dem Server weitergeleitet.

Wenn Sie dieses Feature aktivieren, befindet sich der verbundene Server in der **Zone vertrauenswürdiger Sites** von Windows. Eine Anleitung, wie Sie Server der **Zone vertrauenswürdiger Sites** von Windows hinzufügen, finden Sie in der Onlinehilfe von Internet Explorer.

Aktivieren der vertrauenswürdigen Serverkonfiguration über die administrative Gruppenrichtlinienobjektvorlage

Voraussetzung:

Beenden Sie alle Citrix Workspace-App-Komponenten, einschließlich Connection Center.

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Erweitern Sie den Knoten **Computerkonfiguration** und navigieren Sie zu **Administrative Vorlagen** > **Klassische administrative Vorlagen (ADM)** > **Citrix Komponenten** > **Citrix Workspace** > **Netzwerkrouting** > **Vertrauenswürdige Serverkonfiguration konfigurieren**.
3. Wählen Sie **Aktiviert**, um die Regionsidentifizierung in der Citrix Workspace-App durchzusetzen.
4. Wählen Sie **Vertrauenswürdige Serverkonfiguration erzwingen**. Der Client muss dann die Identifizierung mit einem vertrauenswürdigen Server durchführen.
5. Wählen Sie im Dropdownmenü zu **Windows-Internetzone** die Client-Serveradresse aus. Diese Einstellung gilt nur für die Zone vertrauenswürdiger Sites von Windows.
6. Legen Sie im Feld **Adresse** die Client-Serveradresse für die Zone vertrauenswürdiger Sites außer Windows fest. Sie können eine durch Trennzeichen getrennte Liste verwenden.
7. Klicken Sie auf **OK** und **Übernehmen**.

ICA-Dateisignierung

Die ICA-Dateisignierung schützt vor unautorisierten Anwendungs- oder Desktopstarts. Die Citrix Workspace-App prüft, ob eine vertrauenswürdige Quelle die Anwendung oder den Desktop gestartet hat und verhindert basierend auf administrativen Richtlinien das Starten von Ressourcen auf nicht

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

vertrauenswürdigen Servern. Sie können die ICA-Dateisignierung über die administrative Vorlage für Gruppenrichtlinienobjekte oder StoreFront konfigurieren. Die ICA-Dateisignierung ist in der Standardeinstellung nicht aktiviert.

Informationen zum Aktivieren der ICA-Dateisignierung für StoreFront finden Sie unter Aktivieren der ICA-Dateisignierung in der StoreFront-Dokumentation.

In Webinterface-Bereitstellungen konfiguriert das Webinterface mit dem Citrix ICA-Dateisignierungsdienst, dass beim Start von Anwendungen und Desktops eine Signatur eingeschlossen wird. Der Dienst kann die ICA-Datei mit einem Zertifikat des lokalen Zertifikatspeichers signieren.

Konfigurieren der ICA-Dateisignatur

> **Hinweis:**
>
> Wenn CitrixBase.admx\adml nicht dem lokalen Gruppenrichtlinienobjekt hinzugefügt wird, ist die **Richtlinie zum Aktivieren der ICA-Dateisignierung** evtl. nicht vorhanden.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten**.
3. Wählen Sie die Richtlinie **ICA-Dateisignierung aktivieren** und dann nach Bedarf eine der folgenden Optionen:
    a) Aktiviert: gibt an, dass Sie den Fingerabdruck des Signaturzertifikats der Positivliste der vertrauenswürdigen Zertifikatfingerabdrücke hinzufügen können.
    b) Vertrauenswürdige Zertifikate: Klicken Sie auf **Anzeigen**, um den Fingerabdruck des Signaturzertifikats aus der Positivliste zu entfernen. Sie können die Fingerabdrücke von Signaturzertifikaten von den Eigenschaften des Signaturzertifikats kopieren und einfügen.
    c) Sicherheitsrichtlinie: Folgende Optionen sind im Menü verfügbar.
        i. Nur signierte Starts zulassen (sicherer): lässt nur richtig signierte Anwendungs- oder Desktopstarts von einem vertrauenswürdigen Server zu. Im Falle einer ungültigen Signatur wird eine Sicherheitswarnung angezeigt. Die Sitzung kann dann nicht gestartet werden.
        ii. Benutzer bei nicht signierten Starts auffordern (weniger sicher): Eine Nachricht wird angezeigt, wenn eine nicht signierte oder ungültig signierte Sitzung gestartet wird. Sie können den Start fortsetzen oder abbrechen (Standard).
4. Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.
5. Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

Auswählen und Verteilen eines digitalen Signaturzertifikats:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bei der Auswahl eines digitalen Signaturzertifikats empfiehlt Citrix eine Auswahl aus der folgenden Prioritätsliste:

1. Erwerben Sie ein codesigniertes Zertifikat oder ein SSL-Signaturzertifikat einer öffentlichen Zertifizierungsstelle.
2. Wenn Ihr Unternehmen eine private Zertifizierungsstelle hat, erstellen Sie ein codesigniertes oder SSL-Signaturzertifikat mit der privaten Zertifizierungsstelle.
3. Verwenden Sie ein vorhandenes SSL-Zertifikat, z. B. das Webinterface-Serverzertifikat.
4. Erstellen Sie ein Stammzertifikat der Zertifizierungsstelle und verteilen es mit einem Gruppenrichtlinienobjekt oder einer manuellen Installation auf die Benutzergeräte.

Storebrowse

April 22, 2024

Storebrowse ist ein einfaches Befehlszeilenhilfsprogramm zur Interaktion zwischen Client und Server. Es wird zur Authentifizierung aller Operationen innerhalb von StoreFront und mit Citrix Gateway verwendet.

Informationen zur älteren Version des Storebrowse-Hilfsprogramms für Citrix Receiver für Windows finden Sie in der Dokumentation für Storebrowse für Citrix Receiver für Windows.

Mit Storebrowse können Administratoren folgende Routinevorgänge automatisieren:

- Hinzufügen von Stores
- Enumerieren des veröffentlichten Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) von einem konfigurierten Store.
- Manuelles Erstellen einer ICA-Datei unter Auswahl von beliebigem Citrix Virtual Apps and Desktops und Citrix DaaS.
- Generieren einer ICA-Datei mit der Storebrowse-Befehlszeile
- Starten der veröffentlichten Anwendung

Das Storebrowse-Hilfsprogramm ist jetzt Teil der Authmanager-Komponente. Nach der Installation der Citrix Workspace-App ist das Storebrowse-Hilfsprogramm im `AuthManager`-Installationsordner.

Um sicherzustellen, dass Storebrowse gemeinsam mit der `Authmanager`-Komponente installiert wurde, können Sie den Registrierungspfad wie folgt überprüfen:

Bei Installation der Citrix Workspace-App durch Administratoren:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Auf 32-Bit-Maschinen	[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\Inst
Auf 64-Bit-Maschinen	[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\A

Bei Installation der Citrix Workspace-App durch Benutzer (Nicht-Administratoren):

Auf 32-Bit-Maschinen	[HKEY_CURRENT_USER\SOFTWARE\Citrix\AuthManager\Insta
Auf 64-Bit-Maschinen	[HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\Au

Anforderungen

Installieren Sie die Citrix Workspace-App Version 1808 für Windows oder höher, damit das Storebrowse-Hilfsprogramm optimal mit StoreFront und Citrix Gateway verwendet werden kann. Die Citrix Workspace-App Version 1809 benötigt zur Installation mindestens 530 MB freien Speicherplatz und 2 GB RAM.

Compatibility Matrix

Das Storebrowse-Hilfsprogramm ist mit folgenden Betriebssystemen kompatibel:

Betriebssystem
Windows 10 (32-Bit- und 64-Bit-Edition)
Windows 8.1 (32- und 64-Bit-Edition)
Windows 7 SP1 (32- und 64-Bit-Edition)
Windows Thin PC
Windows Server 2016
Windows Server 2012 R2, Standard und Datacenter Edition
Windows Server 2012, Standard und Datacenter Edition
Windows Server 2008 R2, 64-Bit-Edition
Windows Server 2008 R2, 64-Bit-Edition

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verbindungen

Das Storebrowse-Hilfsprogramm unterstützt folgende Verbindungsarten:

- HTTP-Store
- HTTPS-Store
- Citrix Gateway 11.0 und höher

> **Hinweis:**
>
> Das Storebrowse-Hilfsprogramm akzeptiert keine Anmeldeinformationen mit Eingabe über die Befehlszeile in einem HTTP-Store.

Authentifizierungsmethoden

StoreFront-Server StoreFront unterstützt verschiedene Authentifizierungsmethoden für den Zugriff auf Stores, es werden jedoch nicht alle empfohlen. Aus Sicherheitsgründen sind einige Authentifizierungsmethoden standardmäßig deaktiviert, wenn Sie einen Store erstellen.

- **Benutzername und Kennwort:** Die Benutzer können zur Authentifizierung bei ihren Stores ihre Anmeldeinformationen eingeben. Die explizite Authentifizierung ist standardmäßig aktiviert, wenn Sie den ersten Store erstellen. Alle Benutzerzugriffsmethoden unterstützen die explizite Authentifizierung.
- **Domänen-Passthrough**: Benutzer authentifizieren sich bei den Windows-Computern, die der Domäne angehören, und werden beim Zugriff auf ihre Stores automatisch angemeldet. Um diese Option zu verwenden, muss die Passthrough-Authentifizierung aktiviert sein, wenn die Citrix Workspace-App auf den Benutzergeräten installiert wird. Weitere Informationen zum Konfigurieren des Domänen-Passthroughs finden Sie unter Konfigurieren von Domänen-Passthrough-Authentifizierung.
- **HTTP-Basic**: Für das Storebrowse-Hilfsprogramm muss die HTTP Basic-Authentifizierung zur Kommunikation mit StoreFront-Servern aktiviert sein. Diese Option ist standardmäßig auf dem StoreFront-Server deaktiviert. Sie müssen die HTTP Basic-Authentifizierungsmethode aktivieren.

Das Storebrowse-Hilfsprogramm unterstützt folgende Authentifizierungsmethoden:

- Verwendung des `AuthManager`, der in das Storebrowse-Hilfsprogramm integriert ist. Hinweis: Sie müssen die HTTP Basic-Authentifizierungsmethode in StoreFront aktivieren, während Sie mit Storebrowse arbeiten. Dies gilt, wenn der Benutzer die Anmeldeinformationen über die Storebrowse-Befehle bereitstellt.
- Externer `Authmanager`, der in die Citrix Workspace-App für Windows integriert werden kann.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Unterstützung für Citrix Gateway

Im aktuellen Release des Storebrowse-Hilfsprogramms können Sie nun eine Citrix Gateway-URL hinzufügen. Die Kommunikation mit Citrix Gateway muss nicht zusätzlich im Storebrowse-Hilfsprogramm konfiguriert werden.

Single Sign-On mit Citrix Gateway

Zusätzlich zur neuen Unterstützung für Citrix Gateway können Sie jetzt auch Single Sign-On verwenden. Sie können einen neuen Store hinzufügen und die veröffentlichten Ressourcen enumerieren, ohne Ihre Benutzeranmeldeinformationen angeben zu müssen.

Weitere Informationen zur Unterstützung von Single Sign-On mit Citrix Gateway finden Sie unter Unterstützung von Single Sign-On mit Citrix Gateway.

> **Hinweis:**
>
> Dieses Feature wird nur auf in Domänen eingebundenen Maschinen unterstützt, auf denen Citrix Gateway mit Authentifizierung per Single Sign-On konfiguriert ist.

Starten eines veröffentlichten Desktops oder einer veröffentlichten Anwendung

Sie können Ressourcen jetzt direkt aus dem Store starten, ohne eine ICA-Datei verwenden zu müssen.

Verwendung von Befehlen

Der folgende Abschnitt enthält detaillierte Informationen zu den Befehlen, die Sie im Storebrowse-Hilfsprogramm verwenden können.

-a, –addstore

Beschreibung:

Fügt einen neuen Store hinzu. Gibt die vollständige URL des Stores zurück. Wenn dies fehlschlägt, wird ein Fehler gemeldet.

> **Hinweis:**
>
> Sie können mit dem Storebrowse-Hilfsprogramm mehrere Stores hinzufügen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Befehlsbeispiel in StoreFront:

Befehl:

```
storebrowse.exe –U *username* -P *password* -D *domain* -a *URL of Storefront*
```

Beispiel:

‘.\storebrowse.exe –U {Username} –P {Password} –D {Domain} –a https://my.firstexamplestore.net‘

Befehlsbeispiel in Citrix Gateway:

Befehl:

```
storebrowse.exe –U *username* -P *password* -D *domain* -a *URL of CitrixGateway*
```

Beispiel:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –a <https://mysecondexample.com>
```

/?

Beschreibung:

Bietet Details zur Verwendung des Storebrowse-Hilfsprogramms.

(-l), –liststore

Beschreibung:

Listet die Stores auf, die vom Benutzer hinzugefügt wurden.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe –l
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe –l
```

(-M 0x2000 -E)

Beschreibung:

Enumeriert die verfügbaren Ressourcen.

Befehlsbeispiel in StoreFront:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –M 0
x2000 –E <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –M 0
x2000 –E <https://my.secondexample.net>
```

-q, –quicklaunch

Beschreibung:

Erstellt die erforderliche ICA-Datei für veröffentlichte Apps und Desktops mit dem Storebrowse-Hilfsprogramm. Die Schnellstartoption erfordert die Eingabe einer Start-URL und der Store-URL: Dies kann entweder der StoreFront-Server oder die Citrix Gateway-URL sein. Die ICA-Datei wird im Verzeichnis `%LocalAppData%\Citrix\Storebrowse\cache` erstellt.

Sie können die Start-URL für alle veröffentlichten Apps und Desktops mit folgendem Befehl abrufen:

```
.\storebrowse –M 0X2000 –E https://myfirstexamplestore.net/Citrix/
Second/discovery
```

Eine typische Start-URL sieht folgendermaßen aus:

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix
/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –q {
Launch_URL_of_published_ apps and desktops } <https://my.firstexamplestore
.net/Citrix/Store/resources/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https
://my.firstexamplestore.net/Citrix/Store/discovery>
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –q {
Launch_URL_of_published_ apps and desktops } <https://my.secondexmaplestore
.com>
```

-L, –launch

Beschreibung:

Erstellt die erforderliche ICA-Datei für veröffentlichte Apps und Desktops mit dem Storebrowse-Hilfsprogramm. Die Startoption erfordert die Eingabe des Ressourcennamens und der Store-URL:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dies kann entweder der StoreFront-Server oder die Citrix Gateway-URL sein. Die ICA-Datei wird im Verzeichnis `%LocalAppData%\Citrix\Storebrowse\cache` erstellt.

Sie können den Anzeigenamen der veröffentlichten Apps und Desktops mit folgendem Befehl abrufen:

```
.\storebrowse –M 0X2000 –E https://myfirstexamplestore.net/Citrix/
Second/discovery
```

Dieser Befehl führt zu folgender Ausgabe:

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix
/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

Der in der obigen Ausgabe fett gedruckte Name wird als Eingabeparameter für die Startoption verwendet.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -U { Username } –P { Password } –D { Domain } –L
“{ Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/
discovery>
```

Befehlsbeispiel in Citrix Gateway:

```
<.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –L {
Resource_Name } https://my.secondexamplestore.com>
```

-S, –sessionlaunch

Beschreibung:

Sie können mit einem einzigen Befehl den Store hinzufügen, die veröffentlichten Ressourcen (Apps und Desktops) enumerieren und die Ressource starten. Diese Option verwendet die folgenden Parameter: Benutzername, Kennwort, Domäne, Anzeigename der zu startenden Ressource und Store-URL. Wenn Benutzer keine Anmeldeinformationen angeben, werden sie von `AuthManager` zur Eingabe der Anmeldeinformationen aufgefordert. Anschließend erfolgt der Start der Ressource.

Sie können den Namen der Ressource von veröffentlichten Apps und Desktops mit folgendem Befehl abrufen:

```
.\storebrowse –M 0X2000 –E https://myfirstexamplestore.net/Citrix/
Second/discovery
```

Dieser Befehl führt zu folgender Ausgabe:

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix
/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Der in der obigen Ausgabe fett gedruckte Name wird als Eingabeparameter für die Option –S verwendet.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -U { Username } –P { Password } –D { Domain } –S “
{ Friendly_Resource_Name } <https://my.firstexamplestore.net/Citrix/
Store/discovery >
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –S {
Friendly_Resource_Name } <https://my.secondexamplestore.com>
```

-f, –filefolder

Beschreibung:

Erstellt für alle veröffentlichten Apps und Desktops mit dem Storebrowse-Hilfsprogramm die erforderliche ICA-Datei im benutzerdefinierten Verzeichnis, das in der Option –f definiert wurde.

Die Startoption erfordert einen Ordnernamen und den Namen der Ressource sowie die Eingabe der Store-URL: Dies kann entweder der StoreFront-Server oder die Citrix Gateway-URL sein.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe –f “C:\Temp\Launch.ica” –L “Resource_Name” { Store }
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe –f “C:\Temp\Launch.ica” –L “Resource_Name” { NSG_URL
 }
```

-t, –traceauthentication

Beschreibung:

Protokollerstellung für die integrierte `AuthManager`-Komponente des Storebrowse-Hilfsprogramms. Protokolle werden nur erstellt, wenn Storebrowse einen integrierten `AuthManager` verwendet. Protokolle werden im Verzeichnis `localappdata%\Citrix\Storebrowse\logs` erstellt.

Hinweis: Diese Option darf nicht der letzte Parameter in der Befehlszeile des Benutzers sein.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe –t –U { UserName } –P { Password } –D { Domain } –a
{ StoreURL }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe –t –U { UserName } –P { Password } –D { Domain } –a
{ NSG_URL }
```

-d, –deletestore

Beschreibung:

Löscht den vorhandenen StoreFront- oder Citrix Gateway-Store.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe –d https://my.firstexamplestore.net/Citrix/Store/
discovery
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe –d https://my.secondexmaplestore.com
```

Unterstützung von Single Sign-On mit Citrix Gateway

Mit Single Sign-On können Sie sich bei einer Domäne authentifizieren und von dieser Domäne bereitgestelltes Citrix Virtual Apps and Desktops und Citrix DaaS verwenden, ohne sich für jede App oder jeden Desktop neu authentifizieren zu müssen. Wenn Sie mit dem Storebrowse-Hilfsprogramm einen Store hinzufügen, werden Ihre Anmeldeinformationen zusammen mit den für Sie enumerierten virtuellen Apps und Desktops (einschließlich Startmenüeinstellungen) an den Citrix Gateway-Server übergeben. Nach der Single Sign-On-Konfiguration können Sie den Store hinzufügen, die virtuellen Apps und Desktops enumerieren und erforderliche Ressourcen starten, ohne Ihre Anmeldeinformationen mehrmals eingeben zu müssen.

Dieses Feature wird ab Citrix Gateway Version 11 unterstützt.

Voraussetzungen:

Informationen zu den Voraussetzungen für die Konfiguration des Single Sign-On für Citrix Gateway finden Sie unter Konfigurieren von Domänen-Passthrough-Authentifizierung.

Das Single Sign-On-Feature mit Citrix Gateway kann über die administrative Gruppenrichtlinienobjektvorlage aktiviert werden.

> **Hinweis:**
>
> Wenn Sie die Citrix Workspace-App zum ersten Mal installieren oder ein Upgrade von Citrix Receiver durchführen, müssen Sie dem lokalen Gruppenrichtlinienobjekt die neuesten Vorlagendateien hinzufügen. Weitere Informationen über das Hinzufügen von Vorlagendateien

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> zum lokalen Gruppenrichtlinienobjekt finden Sie unter Konfigurieren der administrativen Gruppenrichtlinienobjektvorlage. Bei einem Upgrade bleiben die vorhandenen Einstellungen erhalten, während die neuesten Dateien importiert werden.

1. Öffnen Sie die administrative GPO-Vorlage von Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzerauthentifizierung** > **Single Sign-On für Citrix Gateway**.
3. Verwenden Sie die Umschaltoptionen, um Single Sign-On ein- oder auszuschalten.
4. Klicken Sie auf **Anwenden** und auf **OK**.
5. Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

Einschränkungen:

- Zur Eingabe von Anmeldedaten mit dem Storebrowse-Hilfsprogramm muss auf dem StoreFront-Server die HTTP Basic-Authentifizierung aktiviert sein.
- Wenn Sie mit dem Hilfsprogramm die veröffentlichten virtuellen Apps und Desktops enumerieren oder starten, um eine Verbindung zu einem HTTP-Store herzustellen, wird die Eingabe der Anmeldeinformationen über die Befehlszeilenoption nicht unterstützt. Verwenden Sie als Workaround das externe `AuthManager`-Modul, das aktiviert wird, wenn Sie keine Anmeldeinformationen über die Befehlszeile bereitstellen.
- Das Storebrowse-Hilfsprogramm unterstützt derzeit nur ein einzelnes, Store-konfiguriertes Citrix Gateway auf dem StoreFront-Server.
- Die Funktion "Credential Injection"im Storebrowse-Hilfsprogramm funktioniert nur, wenn das Citrix Gateway mit einstufiger Authentifizierung konfiguriert ist.
- Für die Befehlszeilenoptionen `Username (-U)`, `Password (-P)` und `Domain (-D)` des Storebrowse-Dienstprogramms wird die Groß- und Kleinschreibung beachtet und es dürfen nur Großbuchstaben verwendet werden.

Citrix Workspace-App Desktop Lock

January 18, 2024

Sie können Citrix Workspace-App Desktop Lock verwenden, wenn Sie nicht mit dem lokalen Desktop arbeiten müssen. Sie können den Desktop Viewer verwenden (wenn aktiviert), jedoch sind auf der Symbolleiste nur die folgenden Optionen verfügbar:

- Strg+Alt+Entf
- Einstellungen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Geräte
- Trennen:

Die Citrix Workspace-App für Windows mit Desktop Lock funktioniert auf in Domänen eingebundenen Maschinen, für die Single Sign-On und ein Store konfiguriert sind. PNA-Sites werden nicht unterstützt. Vorherige Versionen von Desktop Lock werden beim Upgrade auf Citrix Receiver für Windows 4.2 oder höher nicht unterstützt.

Installieren von Desktop Lock über die Befehlszeilenschnittstelle

Voraussetzungen:

- Sie müssen Administrator einer Maschine sein, die in die Domäne eingebunden ist.
- Single Sign-On muss aktiviert sein.
- Store muss konfiguriert sein.

1. Installieren Sie die Citrix Workspace-App mit folgendem Befehl:

```
`CitrixWorkspaceApp.exe /includeSSON /Silent STORE0= " AppStore;
   https://testserver.net/Citrix/MyStore/discover;on;Desktop App
   Store" `
```

2. Laden Sie das `CitrixWorkspaceDesktopLock.msi` von der Citrix Downloadseite herunter.
3. Installieren Sie Desktop Lock mit folgendem Befehl:

```
installationSilent : msiexec /i CitrixWorkspaceDesktopLock.msi /
qn
```

Der veröffentlichte Desktop wird nach dem Anmelden des Benutzers automatisch gestartet.

Systemanforderungen

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. Weitere Informationen finden Sie auf der Microsoft-Downloadseite.
- Unterstützung für Windows 7 (einschließlich Embedded Edition), Windows 7 Thin PC, Windows 8, Windows 8.1 und Windows 10 (einschließlich Anniversary Update).
- Verbindung mit StoreFront nur über native Protokolle.
- Benutzergeräte müssen mit einem LAN oder WAN verbunden sein.

Lokaler App-Zugriff

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Wichtig!**
>
> Aktivieren des lokalen App-Zugriffs kann den lokalen Desktopzugriff ermöglichen, es sei denn, es wurde eine vollständige Sperrung über die Gruppenrichtlinienobjektvorlage oder eine ähnliche Richtlinie angewendet. Weitere Informationen finden Sie unter Konfigurieren von lokalem App-Zugriff und URL-Umleitung in der Dokumentation zu Citrix Virtual Apps and Desktops.

Arbeiten mit Citrix Workspace-App Desktop Lock

- Citrix Workspace-App Desktop Lock kann mit den folgenden Features der Citrix Workspace-App verwendet werden:
  - 3Dpro, Flash, USB, HDX Insight, Microsoft Lync 2013-Plug-In und lokaler App-Zugriff.
  - Nur Domänen-, Smartcard- oder zweistufige Authentifizierung.
- Trennen der Citrix Workspace-App Desktop Lock-Sitzung führt zur Abmeldung des Endgeräts.
- Flash-Umleitung ist unter Windows 8 und höher deaktiviert. Flash-Umleitung ist unter Windows 7 aktiviert.
- Desktop Viewer ist für Citrix Workspace-App Desktop Lock ohne die Eigenschaften "Home", "Restore", "Maximize"und "Display"optimiert.
- Strg+Alt+Entf ist auf der Desktop Viewer-Symbolleiste verfügbar.
- Die meisten Windows-Tastenkombinationen werden an die Remotesitzung weitergegeben, Ausnahme bildet Windows+L.
- Strg+F1 löst Strg+Alt+Entf aus, wenn Sie die Verbindung oder Desktop Viewer für Desktopverbindungen deaktivieren.

> **Hinweis:**
>
> Wenn Desktop Lock installiert ist und `LiveInDesktopDisconnectOnLock` am Registrierungspfad `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` oder `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle` auf **False** festgelegt ist, wird die aktive Sitzung getrennt, wenn der Endpunkt aus dem Ruhezustand oder Standbymodus reaktiviert wird.

Installieren von Citrix Workspace-App Desktop Lock

Mit diesen Schritten installieren Sie die Citrix Workspace-App für Windows so, dass virtuelle Desktops mit Citrix Workspace-App Desktop Lock angezeigt werden. Informationen zu Bereitstellungen, die Smartcards verwenden, finden Sie unter Smartcard.

1. Melden Sie sich mit einem lokalen Administratorkonto an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Führen Sie an einer Eingabeaufforderung den folgenden Befehl aus (befindet sich im Ordner "Citrix Workspace-App and Plug-Ins > Windows > Citrix Workspace-App"auf dem Installationsmedium).

   Beispiel:

```
CitrixWorkspaceApp.exe /includeSSON STORE0="DesktopStore;https://my.
storefront.server/Citrix/MyStore/discovery;on;Desktop Store"
```

Informationen zum Befehl finden Sie unter Installation.

1. Doppelklicken Sie im selben Ordner auf dem Installationsmedium auf `CitrixWorkspaceDesktopLock.msi`. Der Assistent "Desktop Lock"wird angezeigt. Folgen Sie den Anweisungen.
2. Wenn die Installation abgeschlossen ist, starten Sie das Benutzergerät neu. Wenn Sie Zugriffsrechte für einen Desktop haben und sich als Domänenbenutzer anmelden, wird das neu gestartete Gerät mit Citrix Workspace-App Desktop Lock angezeigt.

Um die Verwaltung des Benutzergeräts nach der Installation zu ermöglichen, wird das Konto, das für die Installation von `CitrixWorkspaceDesktopLock.msi` verwendet wurde, bei der Ersatz-Shell ausgeschlossen. Wenn das Konto später gelöscht wird, können Sie sich nicht bei dem Gerät anmelden und es verwalten.

Verwenden Sie zum Installieren von Citrix Workspace Desktop Lock **ohne Benutzereingriff** folgenden Befehl:

```
msiexec /i CitrixWorkspaceDesktopLock.msi /qn
```

Konfigurieren von Citrix Workspace-App Desktop Lock

Gewähren Sie jedem Benutzer nur Zugriff auf einen virtuellen Desktop mit Citrix Workspace-App Desktop Lock.

Verhindern Sie mit Active Directory-Richtlinien, dass Benutzer virtuelle Desktops in den Ruhezustand versetzen.

Verwenden Sie das Administratorkonto zum Konfigurieren von Citrix Workspace-App Desktop Lock, das Sie für die Installation verwendet haben.

- Stellen Sie sicher, dass die Dateien receiver.admx (oder receiver.adml) und receiver_usb.admx (.adml) in die Gruppenrichtlinie geladen wurden (wo die Richtlinien unter "Computerkonfiguration"bzw. "Benutzerkonfiguration"> "Administrative Vorlagen"> "Klassische administrative Vorlagen (ADMX)"> "Citrix Komponenten"angezeigt werden). Die ADMX-Dateien sind in %Programme%\Citrix\ICA Client\Configuration\.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- USB-Einstellungen: Wenn ein Benutzer ein USB-Gerät anschließt, erfolgt ein automatisches Remoting des Geräts zum virtuellen Desktop. Es ist kein Benutzereingriff erforderlich. Der virtuelle Desktop steuert das USB-Gerät und zeigt es auf der Benutzeroberfläche an.
  - Aktivieren Sie die USB-Richtlinienregel.
  - Aktivieren und konfigurieren Sie unter "Citrix Workspace-App > Remoting von Clientgeräten > Generisches USB-Remoting"die Richtlinien "Vorhandene USB-Geräte"und "Neue USB-Geräte".
- Laufwerkszuordnung: Aktivieren und konfigurieren Sie unter "Citrix Workspace-App > Remoting von Clientgeräten"die Richtlinie "Clientlaufwerkzuordnung".
- Mikrofon: Aktivieren und konfigurieren Sie unter "Citrix Workspace-App > Remoting von Clientgeräten"die Richtlinie "Clientmikrofon".

Konfigurieren von Smartcards für die Verwendung mit Windows Desktop Lock

1. Konfigurieren Sie StoreFront.
   a) Konfigurieren Sie den XML-Dienst zur Verwendung der DNS-Adressauflösung für Kerberos-Unterstützung.
   b) Konfigurieren Sie StoreFront-Sites für HTTPS-Zugriff, erstellen Sie ein Serverzertifikat, das von Ihrer Domänenzertifizierungsstelle signiert wurde und fügen Sie HTTPS-Bindung zur Standardwebsite hinzu.
   c) Stellen Sie sicher, dass Passthrough-Authentifizierung mit Smartcard aktiviert ist (standardmäßig aktiviert).
   d) Aktivieren Sie Kerberos.
   e) Aktivieren Sie Kerberos und Passthrough-Authentifizierung mit Smartcard.
   f) Aktivieren Sie den anonymen Zugriff auf die IIS-Standardwebsite und verwenden Sie die integrierte Windows-Authentifizierung.
   g) Stellen Sie sicher, dass für die IIS-Standardwebsite kein SSL erforderlich ist, und dass Clientzertifikate ignoriert werden.
2. Verwenden Sie die Gruppenrichtlinien-Verwaltungskonsole zum Konfigurieren lokaler Computerrichtlinien auf dem Benutzergerät.
   a) Importieren Sie die Vorlage Receiver.admx aus %Programme%\Citrix\ICA Client\Configuration\.
   b) Erweitern Sie "Administrative Vorlagen > Klassische administrative Vorlagen (ADMX) > Citrix Komponenten > Citrix Workspace > Benutzerauthentifizierung".
   c) Aktivieren Sie "Smartcardauthentifizierung".
   d) Aktivieren Sie "Lokaler Benutzername und Kennwort".
3. Konfigurieren Sie das Benutzergerät vor der Installation von Citrix Workspace-App Desktop Lock.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a) Fügen Sie die URL für den Delivery Controller in der Windows Internet Explorer-Liste "Vertrauenswürdige Sites"hinzu.
b) Fügen Sie die URL für die erste Bereitstellungsgruppe in der Windows Internet Explorer-Liste "Vertrauenswürdige Sites"im Format "desktop:// delivery-group-name"hinzu.
c) Aktivieren Sie Internet Explorer für die automatische Anmeldung für vertrauenswürdige Sites.

Wenn Citrix Workspace-App Desktop Lock auf dem Benutzergerät installiert ist, wird eine konsistente Richtlinie für das Entfernen der Smartcard zwingend angewendet. Wird die Richtlinie für das Entfernen der Smartcard beispielsweise für den Desktop auf Abmelden erzwingen festgelegt, muss der Benutzer sich auch vom Benutzergerät abmelden, unabhängig davon, wie die Richtlinie dort eingestellt ist. Dadurch wird sichergestellt, dass das Benutzergerät sich nicht in einem inkonsistenten Zustand befindet. Dies gilt nur für Benutzergeräte mit Citrix Workspace-App Desktop Lock.

Entfernen von Desktop Lock

Stellen Sie sicher, dass beide der unten aufgeführten Komponenten entfernt werden.

1. Melden Sie sich mit demselben lokalen Administratorkonto an, das bei der Installation und Konfiguration von Citrix Workspace-App Desktop Lock verwendet wurde.
2. Gehen Sie mit der Windows-Funktion zum Entfernen oder Ändern von Programmen wie folgt vor:

    - Entfernen Sie Citrix Workspace-App Desktop Lock.
    - Entfernen Sie die Citrix Workspace-App für Windows.

Weitergeben von Windows-Tastenkombinationen an die Remotesitzung

Die meisten Windows-Tastenkombinationen werden an die Remotesitzung weitergegeben. In diesem Abschnitt finden Sie einige der gebräuchlichsten Tastenkombinationen.

Windows

- Win+D - Minimieren aller Fenster auf dem Desktop.
- Alt+Tab - Wechseln des aktiven Fensters.
- Strg+Alt+Entf - über Strg+F1 und die Desktop Viewer-Symbolleiste.
- Alt+Umschalt+Tab
- Windows+Tab
- Windows+Umschalt+Tab
- Windows+Alle Zeichentasten

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Windows 8

- Win+C - Charms öffnen.
- Win+Q - Charm "Suche".
- Win+H - Charm "Teilen".
- Win+K - Charm "Geräte".
- Win+I - Charm "Einstellungen".
- Win+Q - Apps durchsuchen.
- Win+W - Einstellungen durchsuchen.
- Win+F - Dateien durchsuchen.

Windows 8 Apps

- Win+Z - App-Optionen anzeigen.
- Win+. - App links andocken.
- Win+Umschalt+. - App rechts andocken.
- Strg+Tab - Zum App-Verlauf wechseln.
- Alt+F4 - App schließen.

Desktop

- Win+D - Desktop öffnen.
- Win+, - Desktop kurz anzeigen.
- Win+B - Zurück zum Desktop.

Sonstiges

- Win+U - Center für erleichterte Bedienung öffnen.
- Strg+Esc - Startbildschirm.
- Win+Eingabetaste - Windows Sprachausgabe öffnen.
- Win+X - Menü für Systemprogrammeinstellungen öffnen.
- Win+Druck - Bildschirmfoto erstellen und unter "Bilder"speichern.
- Win+Tab - Liste zum Wechseln öffnen.
- Win+T - Vorschau offener Fenster in Taskleiste anzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SDK und API

June 14, 2023

Certificate Identity Declaration SDK

Mit dem Certificate Identity Declaration (CID) SDK können Entwickler ein Plug-In erstellen, mit dem die Citrix Workspace-App mithilfe des auf dem Clientcomputer installierten Zertifikats beim StoreFront-Server authentifiziert werden kann. CID deklariert die Smartcard-Identität des Benutzers an einem StoreFront-Server, ohne anhand der Smartcard eine Authentifizierung durchzuführen.

Weitere Informationen finden Sie unter Certificate Identity Declaration SDK for Citrix Workspace app for Windows.

Citrix Common Connection Manager SDK

Das Common Connection Manager (CCM) SDK stellt eine Reihe nativer APIs bereit, mit denen Sie programmgesteuert interagieren und grundlegende Vorgänge ausführen können. Das SDK erfordert keinen separaten Download, da es Teil des Installationspakets der Citrix Workspace-App für Windows ist.

> **Hinweis:**
>
> Bei einigen APIs, die mit dem Start in Zusammenhang stehen, muss die ICA-Datei den Startvorgang für Sitzungen mit virtuellen Apps und Desktops initiieren.

Die CCM SDK-Funktionen umfassen Folgende:

- Sitzungsstart
  - Ermöglicht das Starten von Anwendungen und Desktops mit der generierten ICA-Datei.
- Session disconnect
  - Ähnlich wie das Trennen der Verbindung über Connection Center. Die Trennung kann für alle Sitzungen oder für einen bestimmten Benutzer erfolgen.
- Session logoff
  - Ähnlich wie die Abmeldung über Connection Center. Die Abmeldung kann für alle Sitzungen oder für einen bestimmten Benutzer erfolgen.
- Sitzungsinformationen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Bietet verschiedene Methoden zum Abrufen von Verbindungsinformationen zu den gestarteten Sitzungen. Dazu gehören Desktopsitzung, Anwendungssitzung und invertierte Seamless-Anwendungssitzung.

Weitere Informationen über die Dokumentation zum SDK finden Sie unter Programmers guide to Citrix CCM SDK.

Citrix Virtual Channel SDK

Das Citrix Virtual Channel Software Development Kit (SDK) bietet Unterstützung für das Schreiben von serverseitigen Anwendungen und clientseitigen Treibern für zusätzliche virtuelle Kanäle, die das ICA-Protokoll verwenden. Die serverseitigen virtuellen Kanalanwendungen sind auf Citrix Virtual Apps and Desktops-Servern. Wenn Sie virtuelle Treiber für andere Clientplattformen schreiben möchten, wenden Sie sich an den technischen Support von Citrix.

Das Virtual Channel SDK bietet Folgendes:

- Die Citrix Virtual Driver Application Programming Interface (VDAPI) wird mit dem virtuellen Kanal im Citrix Server API SDK (WFAPI SDK) verwendet, um neue virtuelle Kanäle zu erstellen. Die von der VDAPI bereitgestellte Unterstützung für virtuelle Kanäle macht das Schreiben der eigenen virtuellen Kanäle einfacher.
- Die Windows Monitoring API, die die visuelle Darstellung verbessert und Unterstützung für Anwendungen von Drittanbietern bietet, die in ICA integriert sind.
- Funktionierender Quellcode für Beispielprogramme für virtuelle Kanäle, die Programmiermethoden demonstrieren.
- Das Virtual Channel SDK erfordert, dass das WFAPI SDK die serverseitige Komponente des virtuellen Kanals schreibt.

Weitere Informationen finden Sie unter Citrix Virtual Channel SDK for Citrix Workspace app for Windows.

Fast Connect 3 Credential Insertion API

Die Fast Connect 3 Credential Insertion API bietet eine Schnittstelle zum Bereitstellen von Benutzeranmeldeinformationen für Single Sign-On (SSON). Dieses Feature ist für die Citrix Workspace-App für Windows 4.2 und höher verfügbar. Mit dieser API können Citrix Partner Authentifizierungs- und SSO-Produkte bereitstellen, die StoreFront oder das Webinterface verwenden, um Benutzer an virtuellen Anwendungen oder Desktops anzumelden und die Verbindungen zu diesen Sitzungen auch wieder zu trennen.

Weitere Informationen finden Sie unter Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Referenz für ICA-Einstellungen

June 14, 2023

Die Referenzdatei für ICA-Einstellungen enthält Registrierungseinstellungen und Listen der ICA-Dateieinstellungen, mit denen Administratoren das Verhalten der Citrix Workspace-App anpassen können. Sie können die Referenz für ICA-Einstellungen auch zur Problembehandlung bei unerwartetem Verhalten der App verwenden.

Referenz für ICA-Einstellungen (PDF-Download)

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).