VMware Horizon Client for Chrome のインストールとセットアップ ガイド

VMware Horizon Client for Chrome 2103

最新の技術ドキュメントは、 VMware の Web サイト （https://docs.vmware.com/jp/）

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

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

VMware Horizon Client for Chrome のインストールとセットアップ ガイド

このガイドでは、Chromebook に VMware Horizon® Client™ for Chrome をインストールして、構成および使用する方法について説明します。

この情報は、Chromebook を含む Horizon の導入設定を行う必要がある管理者向けです。本書に記載されている内容は、仮想マシン テクノロジーおよびデータセンターの運用に精通している経験豊富なシステム管理者向けに書かれています。

エンドユーザーの場合は、VMware Horizon Client for Chrome ユーザー ガイドまたは Horizon Client for Chrome オンライン ヘルプを参照してください。

セットアップとインストール

1

Horizon Client のセットアップでは、クライアント デバイスに Horizon Client for Chrome アプリケーションをインストールして、Connection Server を構成し、必要なポートを開きます。

この章には、次のトピックが含まれています。

システム要件

Horizon Client for Chrome を使用するデバイスは、特定のソフトウェア要件を満たす必要があります。

デバイス モデル

Chromebook

オペレーティング システム

Chrome OS 75 以降

CPU アーキテクチャ

ARM または x86

Connection Server と Horizon Agent

Horizon 7 バージョン 7.5 以降の最新メンテナンス リリース。

クライアント システムが企業のファイアウォールの外部から接続する場合は、クライアント システムで VPN 接続が不要となるように Unified Access Gateway アプライアンスを使用します。社内にワイヤレス ネットワークがあって、デバイスが使用できるリモート デスクトップへのアクセスがルーティング可能な場合、Unified Access Gateway または VPN 接続を設定する必要はありません。

スマート カード認証

スマート カード認証の要件を参照してください。

サードパーティ ファイアウォール

ファイアウォールで、特定の TCP ポートに対する受信トラフィックを許可する必要があります。クライアント Web ブラウザ アクセスのファイアウォール ルールを参照してください。

表示プロトコル

VMware Blast

スマート カード認証の要件

ユーザー認証にスマート カードを使用する Chromebook は、特定の要件を満たす必要があります。

クライアントのハードウェア要件とソフトウェア要件

スマート カードで認証を行うユーザーは物理スマート カードを所有している必要があり、各スマート カードにはユーザー証明書が含まれる必要があります。次のスマート カードに対応しています。

- 米国国防総省 Common Access Card (CAC)
- 米国連邦政府 Personal Identity Verification (PIV) カード（FIPS-201 スマート カードとも呼ばれる）

ユーザー認証にスマート カードを使用する各 Chromebook には、次のハードウェアおよびソフトウェアが必要です。

- Horizon Client for Chrome
- 互換性のあるスマート カード リーダー
- Google スマート カード コネクタ アプリケーション

  コネクタ アプリケーションは、Chrome OS にスマート カードのベーシック サポートを提供します。スマート カード コネクタ アプリケーションは、Chrome ウェブストアからダウンロードできます。VMware では、Google Smartcard Connector アプリケーション バージョン 1.2.16.1 以降の使用をおすすめします。

- Charismathics CSSI Smart Card Middleware アプリケーション

  ミドルウェアは、スマート カードと他のクライアント証明書と通信を行います。CSSI Smart Card Middleware アプリケーションは、Chrome ウェブストアからダウンロードできます。

Chromebook でルート証明書と中間証明書のインストールが必要になる場合があります。詳細については、Google Chrome OS のドキュメントを参照してください。

エージェント ソフトウェアの要件

Horizon 管理者は、エージェント マシンに Charismathics CSSI スマート カード ミドルウェア アプリケーションをインストールする必要があります。

エージェントでサポートされるオペレーティング システムについては、Chrome クライアントの機能サポートを参照してください。

スマート カード認証の追加要件

Horizon Client for Chrome のスマート カード要件以外に、他の Horizon コンポーネントは、スマート カードをサポートするための特定の設定要件を満たす必要があります。

Connection Server

スマート カードの使用をサポートするように Connection Server を構成する方法については、Horizon の管理を参照してください。

Unified Access Gateway アプライアンス

Unified Access Gateway 3.2 以降

スマート カードの使用をサポートするように Unified Access Gateway アプライアンスを設定する方法については、VMware Unified Access Gateway の導入および設定を参照してください。

Active Directory

スマート カード認証のために管理者が Active Directory で実行する必要があるタスクについては、Horizon の管理ドキュメントを参照してください。

スマート カード認証の制限

スマート カード認証では、Chromebook にスマート カード リーダーを接続してスマート カードを挿入し、Horizon Client でサーバを選択します。認証手順で、ユーザー名とパスワードの代わりに PIN を入力します。リモート デスクトップまたは公開アプリケーションを選択した後、スマート カードのコマンドと応答はすべてリモート デスクトップまたは公開アプリケーションにリダイレクトされます。

Horizon Client for Chrome で使用する場合、スマート カード認証には、いくつかの制限があります。

- 接続サーバと Unified Access Gateway スマート カードのユーザー名のヒント機能はサポートされません。
- 接続サーバのスマート カード取り外しポリシーはサポートされていません。
- シングル サインオンはサポートされていません。リモート デスクトップまたは公開アプリケーションに接続するときに、リモート セッション内でスマート カードの PIN をもう一度入力する必要があります。
- スマート カードを使用してサーバとの認証を行った後は、Active Directory 認証など、別の認証方法に切り替えることはできません。次にサーバに接続するときに別の認証方法を使用するには、Chrome OS からログアウトするか、Chromebook を再起動する必要があります。
- 証明書を選択して PIN を入力すると、選択した証明書が Chromebook のキャッシュに保存され、次にサーバに接続するときに使用されます。次にサーバに接続するときに別の証明書を選択するには、Chromebook を再起動する必要があります。

Connection Server の準備

エンド ユーザーがサーバに接続して、リモート デスクトップまたは公開アプリケーションにアクセスするには、Horizon 管理者が Connection Server をインストールして設定する必要があります。

Blast 外部 URL の構成

サーバがインストールされると、Horizon Console で該当する Connection Server インスタンスの [Blast Secure Gateway] 設定が有効になります。また、該当する Connection Server インスタンスの Blast Secure Gateway で使用するように、[Blast 外部 URL] 設定を構成します。

デフォルトでは、URL には安全なトンネル外部 URL の FQDN およびデフォルトのポート番号 8443 が含まれます。URL には、Connection Server ホストに到達するためにクライアント システムで使用できる FQDN とポート番号を含める必要があります。

詳細については、Horizon のインストールドキュメントの「Horizon Connection Server インスタンスの外部 URL を設定する」を参照してください。

ファイアウォール ルールの構成

サードパーティのファイアウォールを使用する場合は、複製されたグループのすべての Connection Server のホストで TCP ポート 8443 へのインバウンド トラフィックを許可するようにルールを構成し、データセンターのリモート デスクトップの仮想マシンと RDS ホストの TCP ポート 22443 に（サーバからの）インバウンド トラフィックを許可するためのルールを構成します。

詳細については、クライアント Web ブラウザ アクセスのファイアウォール ルールを参照してください。

ユーザー認証の設定

ユーザー認証を設定する場合は、次のチェック リストを使用します。

- それぞれの Connection Server インスタンスが、ユーザーが Web ブラウザで入力するホスト名を使用して完全に検証できる TLS 証明書を持つことを確認します。詳細については、Horizon のインストールを参照してください。
- RSA SecurID または RADIUS 認証などの 2 要素認証を使用するには、Connection Server でこの機能が有効であることを確認してください。RADIUS 認証のログイン ページでラベルをカスタマイズできます。リモート セッションのタイムアウト後に行われる 2 要素認証を設定できます。詳細については、Horizon の管理の 2 要素認証についてのトピックを参照してください。
- Horizon Client で [ドメイン] ドロップダウン メニューを非表示にするには、[クライアントのユーザー インターフェイスでドメイン リストを非表示] グローバル設定を有効にします。デフォルトでは、この設定は有効になっています。詳細については、Horizon の管理を参照してください。
- Horizon Client にドメイン リストを送信するには、[ドメイン リストを送信] グローバル設定を有効にします。デフォルトでは、この設定は無効になっています。詳細については、Horizon の管理を参照してください。
- 認証しなくても公開アプリケーションにアクセスできるようにするには、Connection Server でこの機能を有効にします。詳細については、Horizon の管理を参照してください。

次の表に、[ドメイン リストを送信] と [クライアントのユーザー インターフェイスでドメイン リストを非表示] グローバル設定によって、Horizon Client からサーバへのログイン方法がどのように決まるかを示します。

「ドメイン リストを送信」の設定	「クライアントのユーザー インターフェイスでドメイン リストを非表示」の設定	ユーザーのログイン方法
無効（デフォルト）	有効	[ドメイン] ドロップダウン メニューは表示されません。ユーザーは、[ユーザー名] テキスト ボックスに次のいずれかの値を入力する必要があります。 ■ ユーザー名（複数のドメインの場合は使用できません） ■ *domain\username* ■ *username@domain.com*
無効（デフォルト）	無効	クライアントでデフォルトのドメインが設定されている場合、デフォルトのドメインが [ドメイン] ドロップダウン メニューに表示されます。クライアントがデフォルトのドメインを認識していない場合は、[ドメイン] ドロップダウン メニューに *DefaultDomain** が表示されます。ユーザーは、[ユーザー名] テキスト ボックスに次のいずれかの値を入力する必要があります。 ■ ユーザー名（複数のドメインの場合は使用できません） ■ *domain\username* ■ *username@domain.com*
有効	有効	[ドメイン] ドロップダウン メニューは表示されません。ユーザーは、[ユーザー名] テキスト ボックスに次のいずれかの値を入力する必要があります。 ■ ユーザー名（複数のドメインの場合は使用できません） ■ *domain\username* ■ *username@domain.com*
有効	無効	ユーザーは、[ユーザー名] テキスト ボックスにユーザー名を入力して、[ドメイン] ドロップダウン メニューからドメインを選択できます。あるいは、[ユーザー名] テキスト ボックスに次のいずれかの値を入力できます。 ■ *domain\username* ■ *username@domain.com*

クライアント Web ブラウザ アクセスのファイアウォール ルール

Connection Server インスタンス、リモート デスクトップ、公開アプリケーションに接続することをクライアント Web ブラウザに許可するには、ファイアウォールで特定の TCP ポートの受信トラフィックを許可する必要があります。

Horizon Client Chrome との接続では HTTPS を使用する必要があります。HTTP 接続は許可されません。

デフォルトでは、Connection Server インスタンスをインストールする場合、ファイアウォールが TCP ポート 8443 へのインバウンド トラフィックを許可するように構成するため、Windows ファイアウォールで [VMware Horizon View Connection Server (Blast-In)] ルールが有効になります。

表 1-1. クライアント ブラウザ アクセスのファイアウォール ルール

送信元	デフォルトの送信元ポート	プロトコル	送信先	デフォルトの送信先ポート	注
クライアント Web ブラウザ	すべての TCP	HTTPS	Connection Server インスタンス	TCP 443	最初に接続するために、クライアント デバイスの Web ブラウザは、TCP ポート 443 で Connection Server インスタンスに接続します。
クライアント Web ブラウザ	すべての TCP	HTTPS	Blast Secure Gateway	TCP 8443	最初の接続が行われた後、クライアント デバイスの Web ブラウザは、TCP ポート 8443 で Blast Secure Gateway に接続します。この第 2 の接続を許可するためには、Blast Secure Gateway を Connection Server インスタンスで有効にする必要があります。
Blast Secure Gateway	すべての TCP	HTTPS	HTML Access Agent	TCP 22443	Blast Secure Gateway が有効になっている場合、ユーザーがリモート デスクトップまたは公開アプリケーションを選択すると、Blast Secure Gateway はリモート デスクトップ仮想マシンまたは RDS ホストの TCP ポート 22443 で HTML Access Agent に接続します。このエージェント コンポーネントは、Horizon Agent のインストールに含まれています。
クライアント Web ブラウザ	すべての TCP	HTTPS	HTML Access Agent	TCP 22443	Blast Secure Gateway が有効になっていない場合、ユーザーがリモート デスクトップまたは公開アプリケーションを選択すると、クライアント デバイスの Web ブラウザはデスクトップ仮想マシンまたは RDS ホストの TCP ポート 22443 で HTML Access Agent に直接接続します。このエージェント コンポーネントは、Horizon Agent のインストールに含まれています。

Horizon Client for Chrome のインストールまたはアップグレード

Horizon Client for Chrome は Chrome アプリケーションで、他の Chrome アプリケーションと同じ方法でインストールします。

前提条件

クライアント デバイスが Horizon Client for Chrome のシステム要件を満たしていることを確認します。システム要件を参照してください。

手順

1. Chromebook にログインします。
2. Chrome ウェブストアから VMware Horizon Client for Chrome をダウンロードして、インストールします。

Google 管理コンソールでの登録済みの Chromebook デバイスの設定

Google 管理コンソールを使用して、登録済みの Chromebook デバイスに Connection Sever の設定を行うことができます。

Connection Server インスタンス、デフォルトの Connection Server インスタンス、特定のサーバ機能とクライアント機能のリストを設定できます。

サーバのリストを設定すると、サーバが Horizon Client にショートカットとして表示されます。デフォルト サーバを設定すると、Horizon Client がそのサーバに自動的に接続します。

これらの設定は、JSON 設定ファイルに指定します。Chrome 管理者は、Google 管理コンソールを使用して、Horizon Client アプリケーションの JSON 設定ファイルをアップロードする必要があります。Google 管理コンソールの使用方法については、G Suite 管理者のヘルプを参照してください。

Connection Server インスタンスのリスト

server-list セクションのプロパティを使用して、サーバ リストの設定を行います。

プロパティ	説明
server	サーバの IP アドレスまたはホスト名。
username	（オプション）サーバの使用資格が付与されたユーザーの名前。
domain	（オプション）username プロパティで指定したユーザーのドメイン。
description	（オプション）サーバの説明。

次の JSON 構成ファイルの例では、サーバのリストを設定しています。

```
{
  "broker_list": {
    "Value": {
      "settings": {
        "server-list": [{
          "server": "viewserver0.mydomain.com",
          "default": false,
          "description": "View Server 0",
          "username": "User0",
          "desktopId": "RDS2012R2DC",
          "domain": "TestDomain0"
        },{
          "server": "viewserver1.mydomain.com",
          "description": "View Server 1",
          "username": "User1",
          "domain": "TestDomain1",
          "default": false
        }, {
          "server": "123.456.1.2",
          "description": "View Server 2",
          "username": "User2",
          "default": false,
          "domain": "TestDomain2"
        }, {
          "server": "123.456.1.3",
          "description": "View Server 3",
          "username": "User3",
          "default": false,
          "domain": "TestDomain3"
        }, {
          "server": "viewserver4.mydomain.com",
          "description": "View Server 4",
```

```
          "username": "User4",
          "default": false,
          "domain": "TestDomain4"
        }]}
    }
  }
}
```

デフォルトの Connection Server インスタンス

default プロパティを使用して、server-list セクションでデフォルトのサーバを指定できます。有効な値は、true および false です。

次の JSON 構成ファイルの例では、デフォルトのサーバを設定しています。

```
{
  "broker_list": {
    "Value": {
      "settings": {
        "server-list": [{
          "server": "viewserver0.mydomain.com",
          "default": true,
          "description": "View Server 0",
          "username": "User0",
          "desktopId": "RDS2012R2DC",
          "domain": "TestDomain0"
        }]}
    }
  }
}
```

クライアント機能

common-setting セクションの設定を使用して、特定のクライアント機能を構成できます。

設定	説明
allowDataSharing	Horizon Client データ共有機能を構成します。value プロパティには、機能を有効にするか無効にするかを指定します。editable プロパティには、ユーザーが Horizon Client で [データの共有を許可する] の設定を変更できるかどうかを指定します。両方のプロパティの有効値は true と false です。
enableAnonymousLogin	非認証アクセス機能を構成します。value プロパティには、機能を有効にするか無効にするかを指定します。editable プロパティには、ユーザーが Horizon Client で [認証されていないアクセスを使用して匿名ログイン] の設定を変更できるかどうかを指定します。両方のプロパティの有効値は true と false です。
powerSetting	リモート セッションでユーザーが非アクティブになった場合、デバイスがスリープ状態にならないようにします。 デフォルトでは、Chromebook は 10 分後にスリープ モードになります。powerSetting を構成すると、最後のリモート セッションが終了するまで、Chromebook はスリープ状態になりません。 keepAwakeLevel プロパティに電源ポリシー レベルを指定します。keepAwakeLevel には、次のいずれかの値を設定できます。 ■ system。ユーザーが非アクティブになったときに、システムがスリープ状態にならないようにします。これがデフォルトの値です。 ■ display。ユーザーが非アクティブになったときに、ディスプレイがオフになったり、淡色表示されたり、システムがスリープ状態にならないようにします。

次の JSON 構成ファイルの例では、共通設定を指定しています。

```
{
   "broker_list": {
      "settings": {
         "server-list": [{
            "server": "viewserver0.mydomain.com",
            "default": true,
            "description": "View Server 0",
            "username": "User0",
            "domain": "TestDomain0"
         }],
           "common-setting": {
                 "allowDataSharing": false,
                 "enableAnonymousLogin": true,
                 "editable":{
                    "allowDataSharing": true,
                    "enableAnonymousLogin: false
                  },
                  "powerSetting":{
                    "keepAwakeLevel":"display"
                  }
            }
        }
   }
}
```

サーバ機能

server_list セクションの設定を使用して、特定のサーバ機能を構成できます。

設定	説明
enableHighResolution	高解像度モード機能を構成します。value プロパティには、機能を有効にするか無効にするかを指定します。editable プロパティには、ユーザーが Horizon Client で [高解像度モード] の設定を変更できるかどうかを指定します。両方のプロパティの有効値は true と false です。
enableMultiMonitor	マルチモニタ機能を構成します。value プロパティには、機能を有効にするか無効にするかを指定します。有効な値は、true および false です。 value プロパティが有効になっている場合、Horizon Client の [ディスプレイ] は次のように設定されます。 ■ ユーザーがデバイスで特定のディスプレイを設定している場合、[ディスプレイ] は [選択したディスプレイを使用] に設定されます。 ■ ユーザーがデバイスで特定のディスプレイを設定していない場合、[ディスプレイ] は [すべてのディスプレイを使用] に設定されます。 value プロパティが無効になっている場合、[ディスプレイ] は [1 台のディスプレイを使用] に設定されます。
enableWindowsKey	リモート デスクトップの Windows キーを有効または無効にします。value プロパティには、機能を有効にするか無効にするかを指定します。editable プロパティには、ユーザーが Horizon Client で [デスクトップで Windows キーを有効にします] の設定を変更できるかどうかを指定します。両方のプロパティの有効値は true と false です。
timezoneSync	リモート デスクトップと公開アプリケーションのタイムゾーンを設定します。isSync プロパティには、タイム ゾーンを自動的に設定するかどうかを指定します。editable プロパティには、ユーザーが Horizon Client で [タイム ゾーンを自動的に設定する] の設定を変更できるかどうかを指定します。両方のプロパティの有効値は true と false です。isSync を false に設定した場合は、timezone プロパティを指定して、タイムゾーンを手動で設定することができます。 **注：** isSync プロパティを true に設定すると、timezone プロパティの値に関係なく、クライアントのタイムゾーンが常にホスト OS のタイムゾーンと同期されます。
resolution	画面解像度を構成します。width プロパティには画面の幅を指定します。height プロパティには画面の高さを指定します。両方の値は、Chromebook ウィンドウの幅と高さと同じか、それ以下にする必要があります。そうでない場合、Horizon Client はデフォルトの解像度（Chromebook ウィンドウの幅と高さ）を使用します。

設定	説明
usbAllowList	リダイレクトされる USB デバイスを指定します。デバイスがリストにない場合、デバイスはブロックされます。vid プロパティにベンダー ID を指定し、pid プロパティに各デバイスの製品 ID を指定します。 この設定を使用すると、同等のエージェント グループ ポリシー設定 ([Vid/Pid デバイスを含める]) は無視されます。
usbBlockList	リダイレクトしない USB デバイスを指定します。vid プロパティにベンダー ID を指定し、pid プロパティに各デバイスの製品 ID を指定します。 この設定を使用すると、同等のエージェント グループ ポリシー設定 ([Vid/Pid デバイスを除外する]) は無視されます。 usbBlockList 設定は、usbAllowList 設定よりも優先されます。両方のリストにあるデバイスはブロックされます。

次の JSON 構成ファイルの例では、サーバの設定を指定しています。

```
{
  "broker_list": {
    "Value": {
      "settings": {
         "server-list": [{
            "server": "viewserver0.mydomain.com",
            "default": true,
            "description": "View Server 0",
            "username": "User0",
            "domain": "TestDomain0",
            "settings": {
               "enableHighResolution": false,
               "enableMultiMonitor": false,
               "enableWindowsKey": true,
               "timezoneSync": {
                   "isSync": false,
                   "timezone": "-00:00"
               },
               "resolution": {
                 "width": 600,
                 "height": 800
               },
               "editable": {
                  "enableHighResolution": true,
                  "enableWindowsKey": true,
                  "timezoneSync": false
               },
               "usbAllowList":[{
                  "vid": 1111,
                  "pid": 2222
               },{
                  "vid": 1112,
                  "pid": 2223
               }],
               "usbBlockList":[{
                  "vid": 2222,
                  "pid": 3333
```

```
                },{
                  "vid": 2223,
                  "pid": 3334
                }],
           }
        }]
     }
   }
}
```

新しい TLS 証明書を使用するように HTML Access Agent を構成する

業界の規制やセキュリティ規制を遵守するため、証明書認証局 (CA) が署名した証明書と HTML Access Agent が生成するデフォルトの TLS 証明書を置き換えることができます。

リモート デスクトップに HTML Access Agent をインストールすると、HTML Access Agent サービスがデフォルトの自己署名の証明書を作成します。このサービスは、Horizon Client for Chrome を使用するブラウザにデフォルトの証明書を提示します。

注： デスクトップ仮想マシンのゲスト OS で、このサービスは VMware Blast サービスと呼ばれます。

デフォルトの証明書を CA から取得する署名された証明書に置き換えるには、証明書を各リモート デスクトップの Windows ローカル コンピュータ証明書ストアにインポートする必要があります。また、HTML Access Agent が新しい証明書を使用できるように、レジストリ値を設定する必要があります。

デフォルトの HTML Access Agent 証明書を CA が署名した証明書に置き換える場合、各リモート デスクトップで一意の証明書を構成します。親仮想マシンまたはデスクトップ プールを作成するために使用するテンプレートに CA が署名した証明書を構成しないでください。この方法では、数百または数千台のリモート デスクトップが同じ証明書を持つことになります。

リモート デスクトップの MMC への証明書スナップインの追加

Windows ローカル コンピュータ証明書ストアに証明書を追加する前に、HTML Access Agent がインストールされるリモート デスクトップで Microsoft Management Console (MMC) に証明書のスナップインを追加する必要があります。

前提条件

MMC および証明書のスナップインが、HTML Access Agent がインストールされている Windows ゲスト OS で使用できることを確認します。

手順

1. リモート デスクトップで、[スタート] をクリックして **`mmc.exe`** を入力します。
2. [MMC] ウィンドウで、[ファイル] - [スナップインの追加と削除] に移動します。
3. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。

4 [証明書スナップイン] ウィンドウで、[コンピュータ アカウント] を選択し、[次へ] をクリックし、[ローカル コンピュータ] を選択し、[終了] をクリックします。

5 [スナップインの追加と削除] ウィンドウで、[OK] をクリックします。

次のステップ

SSL 証明書を Windows ローカル コンピュータ証明書ストアにインポートします。 HTML Access Agent 証明書の Windows 証明書ストアへのインポートを参照してください。

HTML Access Agent 証明書の Windows 証明書ストアへのインポート

デフォルトの HTML Access Agent 証明書を CA によって署名された証明書に置き換えるには、Windows ローカル コンピュータ証明書ストアに CA によって署名された証明書をインポートする必要があります。HTML Access Agent がインストールされている各リモート デスクトップでこの手順を実行します。

前提条件

- リモート デスクトップで HTML Access Agent がインストールされていることを確認します。
- CA によって署名された証明書がリモート デスクトップにコピーされたことを確認します。
- 証明書のスナップインが MMC に追加されたことを確認します。リモート デスクトップの MMC への証明書スナップインの追加を参照してください。

手順

1 リモート デスクトップの MMC ウィンドウで、[証明書 (ローカル コンピュータ)] ノードを拡張して [個人] フォルダを選択します。

2 [操作] ペインで、[追加の操作] - [すべてのタスク] - [インポート] の順に移動します。

3 [Certificate Import（証明書のインポート)] ウィザードで、[次へ] をクリックして証明書が格納されている場所を参照します。

4 証明書ファイルを選択して [開く] をクリックします。

   証明書ファイルのタイプを表示するには、[ファイル名] ドロップダウン メニューからそのファイル形式を選択できます。

5 証明書ファイルに含まれるプライベート キーのパスワードを入力します。

6 [この鍵をエクスポート可能にマークする] を選択します。

7 [すべての拡張可能なプロパティを含む] を選択します。

8 [次へ] をクリックして [終了] をクリックします。

   新しい証明書が [証明書（ローカル コンピュータ)] - [個人] - [証明書] フォルダに表示されます。

9 新しい証明書にプライベート キーが含まれていることを確認します。

   a [証明書（ローカル コンピュータ)] - [個人] - [証明書] フォルダで、新しい証明書をダブルクリックします。

   b [証明書情報] ダイアログ ボックスの [全般] タブで、「この証明書に対応するプライベート キーがあります。」というメッセージが表示されることを確認します。

次のステップ

必要に応じて、ルート証明書と中間証明書を Windows 証明書ストアにインポートします。 HTML Access Agent のルート証明書と中間証明書のインポートを参照してください。

適切なレジストリ キーを証明書のサムプリントで構成します。Windows レジストリへの証明書のサムプリントを設定するを参照してください。

HTML Access Agent のルート証明書と中間証明書のインポート

証明書チェーンのルート証明書と中間証明書が、HTML Access Agent にインポートした SSL 証明書と共にインポートされていない場合、Windows ローカル コンピュータ証明書ストアにこれらの証明書をインポートする必要があります。

手順

1 リモート デスクトップの MMC コンソールで、[証明書 (ローカル コンピュータ)] ノードを拡張して [信頼されたルート証明機関] - [証明書] フォルダに移動します。

   - ルート証明書がこのフォルダにあり、証明書チェーン内に中間証明書がない場合は、この手順をスキップします。
   - ルート証明書がこのフォルダになければ、手順 2 に進みます。

2 [信頼されたルート証明機関] - [証明書] フォルダを右クリックし、[すべてのタスク] - [インポート] をクリックします。

3 [証明書のインポート] ウィザードで、[次へ]をクリックしてルート CA 証明書が保存されている場所を参照します。

4 ルート CA 証明書ファイルを選択し、[開く] をクリックします。

5 [次へ] をクリックし、[次へ] をクリックし、そして [終了] をクリックします。

6 サーバ証明書に中間 CA が署名している場合は、証明書チェーンのすべての中間証明書を Windows ローカル コンピュータ証明書ストアにインポートします。

   a [証明書 (ローカル コンピュータ)] - [中間証明機関] - [証明書] フォルダに移動します。

   b インポートする必要がある各中間証明書で手順 3 から 6 を繰り返します。

次のステップ

適切なレジストリ キーを証明書のサムプリントで構成します。Windows レジストリへの証明書のサムプリントを設定するを参照してください。

Windows レジストリへの証明書のサムプリントを設定する

HTML Access Agent が、Windows 証明書ストアへインポートされた CA 署名の証明書を使用できるように、Windows レジストリ キーの証明書サムプリントを構成する必要があります。デフォルト証明書を CA 署名の証明書に交換する各リモート デスクトップでこの手順を実行する必要があります。

前提条件

CA 署名の証明書が、Windows 証明書ストアへインポートされていることを確認します。 HTML Access Agent 証明書の Windows 証明書ストアへのインポートを参照してください。

手順

1. HTML Access Agent がインストールされているリモート デスクトップの MMC ウィンドウで、[証明書（ローカル コンピュータ）] - [個人] - [証明書] フォルダの順に移動します。
2. Windows 証明書ストアへインポートした CA 署名の証明書をダブルクリックします。
3. [証明書] ダイアログ ボックスで、[詳細] タブをクリックし、スクロール ダウンして、[サムプリント]アイコンを選択します。
4. 選択したサムプリントをテキスト ファイルにコピーします。

   例： `31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e`

   注： サムプリントをコピーする場合は、先頭にあるスペースを含めないでください。サムプリントとともに先頭にあるスペースをレジストリ キー（手順 7 ）に誤って貼り付けると、証明書は正常に構成されない場合があります。先頭にあるスペースがレジストリの値テキスト ボックスに表示されなくても、この問題が発生する場合があります。
5. HTML Access Agent がインストールされたデスクトップで Windows レジストリ エディタを起動します。
6. `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` レジストリ キーに移動します。
7. `SslHash` 値を修正して、テキスト ボックスへ証明書サムプリントを貼り付けます。
8. Windows を再起動します。

結果

ユーザーが Horizon Client for Chrome を介してリモート デスクトップへ接続する場合、HTML Access Agent はユーザーのブラウザに CA 署名の証明書を提供します。

特定の暗号化スイートを使用するために HTML Access Agent を構成する

HTML Access Agent を構成して、デフォルトの暗号化セットではなく特定の暗号化スイートを使用できます。

デフォルトでは、HTML Access Agent は、ネットワークからのデータの盗み出しや偽装に対して、強力な保護を提供する特定の暗号化に基づいた暗号を使用するために、TLS 接続の受信を必要とします。HTML Access Agent が使用する暗号化の代替リストを構成できます。許可される暗号化のセットは、OpenSSL 形式で表記されます。暗号リストの形式を表示するには、Web ブラウザで **`openssl cipher string`** を検索します。

手順

1. HTML Access Agent がインストールされているデスクトップで、Windows レジストリ エディタを起動します。

2 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config レジストリ キーに移動します。

3 新しい文字列 (REG_SZ) の値 SslCiphers を追加して、OpenSSL 形式で暗号化リストをテキスト ボックスに貼り付けます。

4 変更を反映するには、VMware Blast サービスを再起動します。

Windows ゲスト OS では、HTML Access Agent のサービスは、VMware Blast と呼ばれます。

結果

デフォルトの暗号化リストを使用するように戻すには、SslCiphers 値を削除して、VMware Blast サービスを再起動します。値のデータ部分を単に削除しないでください。データ部分を削除すると、HTML AccessAgent は、OpenSSL 暗号化リスト形式の定義に従って、すべての暗号化を許可しなくなります。

HTML Access Agent が起動すると、VMware Blast サービスのログ ファイルに暗号化の定義を書き込みます。SslCiphers 値が Windows レジストリで構成されていない状態で VMware Blast サービスが起動するときに、ログを調査して現在のデフォルトの暗号化リストを把握できます。

HTML Access Agent のデフォルトの暗号定義は、セキュリティを向上するためにリリースごとに変更される場合があります。

Unified Access Gateway での CA 署名付き証明書の使用

Unified Access Gateway アプライアンスを使用する場合は、Subject Alternative Names (SAN) が設定された CA 署名付き証明書をインストールする必要があります。

SAN が設定されていない CA 署名付き証明書または自己署名証明書を使用すると、接続がプライベートではないエラーが発生し、Horizon Client for Chrome で接続できません。

注： Connection Server インスタンスを使用する場合は、「*ip-address* にアクセスする(安全ではありません)」リンクをクリックして接続できます。

証明書のインストールと設定の詳細については、Horizon のインストールを参照してください。Chrome に証明書をインストールする方法については、Google Chrome のドキュメントを参照してください。

Horizon Client データ共有の設定

Horizon 管理者が VMware カスタマー エクスペリエンス向上プログラム (CEIP) への参加を選択している場合、VMware は Connection Server 経由でクライアント システムから匿名データを収集して受信します。このクライアント データを Connection Server と共有するかどうかを設定できます。

CEIP に参加するように Horizon を設定する方法については、Horizon の管理を参照してください。

デフォルトでは、Horizon Client でデータ共有は有効に設定されています。データ共有の設定は、サーバに接続する前に行う必要があります。この設定は、すべてのサーバに適用されます。サーバに接続した後は、Horizon Client データ共有の設定を変更できません。

手順

1 サーバの選択ページで、[設定]（歯車のアイコン）をクリックします。

2 [データの共有を許可する] オプションをタップして、オンまたはオフにします。

VMware によって収集されるデータ

VMware カスタマー エクスペリエンス向上プログラム (CEIP) に参加し、クライアントでデータの共有が有効になっている場合、VMware はクライアント システムに関するデータを収集します。

VMware は、クライアント上で情報を収集し、ハードウェアとソフトウェアの互換性を優先度付けします。Horizon 管理者が CEIP への参加を決めた場合、VMware はお客様のご要望への対応を強化する目的で、現在ご使用の環境に関する匿名データを収集します。企業が特定できるような情報は収集されません。クライアントの情報はまず Connection Server に送信され、次いで、サーバ、デスクトップ プール、およびリモート デスクトップの情報とともに VMware に送信されます。

CEIP に参加するには、Connection Server をインストールする管理者が Connection Server インストール ウィザードを実行しているときに選択するか、インストール後に Horizon Console でオプションを設定します。

表 1-2. CEIP で収集されるクライアント データ

説明	フィールド名	このフィールドは匿名になりますか？	値の例
アプリケーションを開発する企業	<client_vendor>	いいえ	VMware
製品名	<client_product>	いいえ	VMware Horizon Client for Chrome
クライアント製品のバージョン	<client_version>	いいえ	2012-8.1.0-xxxxxxxx
クライアントのバイナリ アーキテクチャ	<client_arch>	いいえ	ブラウザ
ブラウザのネイティブ アーキテクチャ	<browser_arch>	いいえ	ChromeOS
ブラウザ ユーザー エージェント文字列	<browser_user_agent>	いいえ	Chrome/3.0.1750
ブラウザの内部バージョン文字列	<browser_version>	いいえ	3.0.1750（Chrome 用）
ブラウザのコア実装	<browser_core>	いいえ	Chrome
ブラウザがハンドヘルド デバイスで実行しているかどうか	<browser_is_handheld>	いいえ	true

リモート デスクトップ/公開アプリケーションとの接続の管理

2

エンドユーザーは、サーバに接続して、リモート デスクトップと公開アプリケーションを使用できます。トラブルシューティングを目的として、エンド ユーザーはリモート デスクトップや公開アプリケーションをリセットできます。

この章には、次のトピックが含まれています。

リモート デスクトップまたは公開アプリケーションへの接続

リモート デスクトップまたは公開アプリケーションに接続するには、サーバ名を指定し、ユーザー アカウントの認証情報を入力する必要があります。

エンド ユーザーがリモート デスクトップおよび公開アプリケーションにアクセスする前に、クライアント デバイスからリモート デスクトップまたは公開アプリケーションに接続できることをテストします。

前提条件

- ユーザー名とパスワード、RSA SecurID ユーザー名とパスコード、RADIUS 認証情報、スマート カード個人識別番号 (PIN) などのログイン認証情報を取得します。
- ログイン用の NETBIOS ドメイン名を取得します。たとえば、mycompany.com ではなく mycompany を使用してください。
- スマート カード認証を使用している場合は、すべてのスマート カード認証の要件を満たしていることと制限事項を確認します。詳細については、スマート カード認証の要件とスマート カード認証の制限を参照してください。
- 企業のネットワークの外部から VPN 接続でリモート デスクトップおよび公開アプリケーションにアクセスする必要がある場合には、クライアント デバイスが VPN 接続を使用するように設定され、その接続が有効になっていることを確認します。

- リモート デスクトップまたは公開アプリケーションへのアクセスを提供するサーバの完全修飾ドメイン名 (FQDN) があることを確認します。サーバ名ではアンダースコア (_) はサポートされません。ポートが 443 でない場合、ポート番号も必要です。

手順

1. Chromebook にログインします。
2. VPN 接続が必要な場合、VPN をオンにしてください。
3. VMware Horizon Client アプリケーションを開きます。
4. Smart Card Connector へのアクセスを許可するように求められたら、[許可] をクリックします。

   Chromebook でスマート カード認証が設定されている場合、Horizon Client を最初に起動したときに、このプロンプトが表示されます。
5. サーバに接続します。

オプション	アクション
新規サーバに接続	プラス記号 (+) をクリックし、サーバの名前を入力します。必要であれば、サーバの説明を入力します。[接続] をクリックします。
既存サーバに接続	サーバのショートカットをクリックします。

   Horizon Client とサーバとの接続には常に TLS が使用されます。TLS 接続のデフォルト ポートは 443 です。サーバがデフォルト ポートを使用するように構成されていない場合、以下の例にある形式を使用します。`view.company.com:1443`。
6. スマート カードが必要となる場合またはオプションである場合、使用するスマート カード証明書を選択して PIN を入力します。
7. RSA SecurID または RADIUS の認証証明書の入力を求められた場合、認証情報を入力して [ログイン] をクリックします。

   パスコードには、PIN とトークンで生成された番号が含まれる場合があります。
8. 再度、RSA SecurID または RADIUS の認証情報を入力するダイアログが表示されたら、トークンで次に生成された番号を入力します。

   PIN は入力しないでください。過去に生成され、入力したものと同じ番号も入力しないでください。必要に応じて、新しい番号が生成されるのを待ちます。この手順は、最初のパスコードの入力をミスした、または RSA サーバの設定が変更された時にのみ、必要になります。
9. ユーザー名とパスワードの入力を要求されたら、Active Directory 認証情報を入力します。
   a. 少なくとも 1 台のデスクトップまたはアプリケーション プールを使用する資格が付与されているユーザーのユーザー名とパスワードを入力します。
   b. ドメインを選択します。

      ドメインを選択できない場合は、`username@domain` または `domain\username` の形式でユーザー名を入力する必要があります。
   c. [ログイン] をタップします。

10 （オプション） リモート デスクトップまたは公開アプリケーションをお気に入りとしてマークするには、リモート デスクトップまたは公開アプリケーションのアイコンの内側にある灰色の星をクリックします。

星のアイコンが灰色から黄色に変わります。次回ログインするときに、ブラウザ ウィンドウの右上部分にある星のアイコンをクリックすると、お気に入りのみを表示できます。

11 リモート デスクトップまたは公開アプリケーションに接続するには、デスクトップまたはアプリケーションの選択ウィンドウで、接続するデスクトップまたはアプリケーションのアイコンをクリックします。

12 スマート カード認証を使用している場合は、リモート セッション内でスマート カードの PIN を再度入力します。

結果

リモート デスクトップや公開アプリケーションに接続した後にすぐ切断され、リンクをクリックしてセキュリティ証明書を受け入れるよう求めるプロンプトが表示さる場合、ユーザーはその証明書を信頼するかどうかを選択できます。自己署名付ルート証明書の信頼を参照してください。

リモート デスクトップまたは公開アプリケーションのタイムゾーンが、クライアント デバイスで設定されたタイムゾーンを使用していない場合は、タイム ゾーンを手動で設定します。タイム ゾーンの設定を参照してください。

次のステップ

Horizon Client は、リモート デスクトップや公開アプリケーションの使用に役立つナビゲーション機能を提供します。詳細については、リモート デスクトップの使用と公開アプリケーションの使用を参照してください。

公開アプリケーションへの接続に非認証のアクセスを使用する

非認証アクセス ユーザーのアカウントを使用すると、サーバに匿名でログインし、公開アプリケーションに接続できます。

前提条件

- 管理タスクの実行については、Connection Server の準備で説明しています。
- Connection Server インスタンスで非認証アクセス ユーザーを設定します。詳細については、Horizon の管理の「公開アプリケーションでの非認証アクセスの提供」を参照してください。

手順

1 サーバ選択ページの右上隅にある [設定] ツールバー ボタンをクリックして、[認証されていないアクセスを使用して匿名ログイン] オプションをオンにします。

2 サーバに接続して非認証アクセス ユーザーのアカウント情報を入力し、[ログイン] をクリックします。

アプリケーション選択ウィンドウが表示されます。

3 アクセスする公開アプリケーションのアイコンをクリックします。

自己署名付ルート証明書の信頼

リモート デスクトップまたは公開アプリケーションに初めて接続したときに、リモート マシンで使用する自己署名証明書を受け入れるように指示するプロンプトが表示される場合があります。リモート デスクトップまたは公開アプリケーションに接続する前に、証明書を信頼する必要があります。

Chrome では、自己署名証明書を永続的に信頼するオプションを利用できます。証明書を永続的に信頼しない場合は、ブラウザを再起動するときに毎回証明書を確認する必要があります。

手順

1 信頼されていない証明書の警告や、接続がプライベートではないという警告がブラウザに表示される場合、証明書を調べて、ユーザーの企業によって使用されている証明書と一致しているか確認します。

システム管理者への連絡が必要になる場合があります。たとえば、Chrome では、次の手順を使用します。

a アドレス バーのロック アイコンをクリックします。

b [証明書情報] リンクをクリックします。

c 証明書がユーザーの企業で使用されている証明書と一致しているか確認します。

システム管理者への連絡が必要になる場合があります。

2 セキュリティ証明書を受け入れます。

Chrome でブラウザ ページの [詳細] リンクをクリックして、[*server-name* にアクセスする（安全ではありません）] をクリックすることができます。

結果

リモート デスクトップまたは公開アプリケーションが起動します。

タイム ゾーンの設定

リモート デスクトップまたは公開アプリケーションのタイムゾーンには、ローカル システムのタイムゾーンが自動的に設定されます。

ただし、Horizon Client で、特定の夏時間ポリシーのためタイムゾーンを正しく特定できない場合は、タイムゾーンを手動で設定する必要があります。

リモート デスクトップまたは公開アプリケーションに接続する前に、適切なタイムゾーンを手動で設定するには、デスクトップおよびアプリケーション選択ウィンドウの右上隅にある [設定] ツールバー ボタンをクリックします。[設定] ウィンドウで [タイム ゾーンを自動的に設定する] オプションをオフにして、ドロップダウン メニューからタイムゾーンを 1 つ選択します。選択した値は、リモート デスクトップまたは公開アプリケーションに接続するときに優先的に使用されるタイムゾーンとして保存されます。

リモート デスクトップまたは公開アプリケーションに接続した後に正しいタイムゾーンを手動で設定するには、デスクトップおよびアプリケーション選択ウィンドウに戻り、現在のタイムゾーン設定を変更します。

サーバ ショートカットを管理する

サーバに接続すると、Horizon Client でサーバ ショートカットが作成されます。サーバのショートカットは、編集したり、削除したりできます。

サーバ名や IP アドレスを誤入力した場合でも、Horizon Client はサーバ名や IP アドレスをショートカットとして保存します。サーバ名や IP アドレスを編集することによって、この情報を削除または変更できます。サーバの説明を入力しない場合、サーバ名または IP アドレスがサーバの説明となります。

手順

1 サーバのショートカットを右クリックします。

コンテキスト メニューが表示されます。

2 コンテキスト メニューを使用してサーバ ショートカットを削除するか、サーバ名またはサーバの説明を編集します。

3 サーバのショートカットを編集した場合は、[完了] をクリックして変更内容を保存します。

ログオフまたは切断

ログオフせずにリモート デスクトップから切断すると、リモート デスクトップ内のアプリケーションは開いたままになります。サーバから切断し、公開アプリケーションを実行したままにすることもできます。

手順

◆ リモート デスクトップから切断します。

オプション	説明
リモート デスクトップから	メニュー バーが表示されるまで、リモート デスクトップ ウィンドウの上部をマウスでポイントします。メニューが表示されたら [切断] ボタンをクリックします。あるいは、リモート デスクトップ ウィンドウの右上隅にある [X]（閉じる）ボタンをクリックします。
セッション管理センターから	デスクトップとアプリケーションの選択ウィンドウの右上隅にある [設定] ツールバー ボタンをクリックします。セッション管理センターを開いてリモート デスクトップ セッションを選択し、[切断] をクリックします。また、シェルフでリモート デスクトップのアイコンを右クリックして、[セッション管理センター] をクリックしても、セッション管理センターを開くことができます。

◆ リモート デスクトップからログアウトします。

オプション	説明
リモート デスクトップから	メニュー バーが表示されるまで、リモート デスクトップ ウィンドウの上部をマウスでポイントします。メニューが表示されたら [ログアウト] ボタンをクリックします。
セッション管理センターから	デスクトップとアプリケーションの選択ウィンドウの右上隅にある [設定] ツールバー ボタンをクリックします。セッション管理センターを開いてリモート デスクトップ セッションを選択し、[ログオフ] をクリックします。また、シェルフでリモート デスクトップのアイコンを右クリックして、[セッション管理センター] をクリックしても、セッション管理センターを開くことができます。

- 公開アプリケーションを閉じます。

オプション	説明
公開アプリケーションから	公開アプリケーション ウィンドウの隅にある [X]（閉じる）ボタンをクリックします。
シェルフから	シェルフで公開アプリケーション アイコンを右クリックして、[閉じる] をクリックします。

- サーバからログアウトするには、デスクトップとアプリケーションの選択ウィンドウの右上隅にある [ログアウト] ボタンをクリックします。

リモート デスクトップまたは公開アプリケーションの使用

3

Horizon Client は、使い慣れた個人用のデスクトップとアプリケーション環境を提供します。

この章には、次のトピックが含まれています。

Chrome クライアントの機能サポート

特定のゲスト OS とリモート デスクトップ機能には、特定の Horizon Agent バージョンが必要です。エンド ユーザーに提供する機能を計画する際に、この情報を使用してください。

サポート対象の Windows 仮想デスクトップ

Windows 仮想デスクトップは、単一セッションの仮想マシンです。

このバージョンの Horizon Client for Chrome は、Horizon Agent 7.5 以降がインストールされている Windows 仮想デスクトップでサポートされます。サポートされるゲスト OS は、Windows 7、Windows 8.x、Windows 10、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 ですが、次の制限があります。

- Windows Server 2019 仮想デスクトップでは、Horizon Agent 7.7 以降が必要です。
- Windows 7 および Windows 8.x の仮想デスクトップは、Horizon Agent 2006 以降でサポートされていません。
- VMware Integrated Printing 印刷機能は、Windows 10、Windows Server 2016、または Windows Server 2019 仮想デスクトップで Horizon Agent 7.12 以降と連携します。Windows 7、Windows 8.x、Windows Server 2012 R2 仮想デスクトップでは機能しません。

RDS ホストでサポートされる公開デスクトップ

RDS ホストは、Windows リモート デスクトップ サービスと Horizon Agent がインストールされたサーバ コンピュータです。RDS ホスト上のリモート デスクトップ セッションは複数のユーザーによる同時利用が可能です。RDS ホストには物理マシンまたは仮想マシンのいずれかを使用できます。

このバージョンの Horizon Client for Chrome は、Horizon Agent 7.5 以降がインストールされている RDS ホストでサポートされます。サポートされるゲスト OS は、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 ですが、次の制限があります。

- Windows Server 2019 RDS ホストでは、Horizon Agent 7.7 以降が必要です。
- Windows Server 2012 RDS ホストは Horizon Agent 2006 以降でサポートされていません。
- VMware Integrated Printing 機能は、Windows Server 2016 または Windows Server 2019 RDS ホストで Horizon Agent 7.12 以降と連携します。Windows Server 2012 および Windows Server 2012 R5 RDS ホストでは機能しません。

サポート対象の Linux デスクトップ

サポートされる Linux ゲスト オペレーティング システムと機能については、Horizon での Linux デスクトップのセットアップを参照してください。

動作

VMware は、Windows 以外のデバイス上で、従来の Windows ユーザー インターフェイス要素をナビゲートするためのユーザーとの対話補助を開発しました。

クリック

他のアプリと同様に、タッチパッドをタップして、ユーザー インターフェイスのエレメントをクリックできます。タッチ画面がある Chromebook の場合には、画面をタッチしてユーザー インターフェイスを操作できます。外部マウスも使用できます。

右クリック

次のオプションが右クリック用に利用可能です。

- タッチパッドを 2 本の指でタップします。
- キーボードの Alt キーを押しながら、1 本の指でタッチパッドをタップします。
- 外部マウスを使用して右クリックします。
- タッチ画面がある Chromebook の場合には、2 本の指でタップして右クリックします。

スクロールおよびスクロールバー

垂直方向のスクロールには次のオプションが利用可能です。

- 親指でタップしたままにしてから、タッチパッドで 1 本の指を使用してスクロール ダウンします。2 本の指でスクロールすることもできます。
- 外部マウスを使用してスクロールします。
- タッチ画面がある Chromebook の場合には、2 本の指でタップしてから、ドラッグしてスクロールします。指の下のテキストが指の動きを同じ方向に移動します。

ズームインおよびズームアウト

ズームインとズームアウトは使用できません。

画面のリサイズ

タッチパッドを使用してウィンドウのサイズを変更する場合は、ウィンドウの隅または左右の辺を 1 本の指でタッチして押したままドラッグします。

Chromebook で外付けマウスを使用する場合、カーソルをウィンドウの端に置き、ウィンドウ枠をドラッグして、ウィンドウを広くまたは狭くします。

タッチ画面のある Chromebook でウィンドウのサイズを変更する場合は、ウィンドウの隅を 1 本の指でタッチして押したままドラッグします。

音声、音楽、そしてビデオ

デバイスで音声がオンになっている場合、リモート デスクトップでオーディオを再生することができます。

複数のモニター機能の制限

複数のモニター機能を有効にすると、タッチ ジェスチャが無効になります。詳細については、リモート デスクトップの表示モードの変更を参照してください。

リモート デスクトップの表示モードの変更

リモート デスクトップの表示モードを変更できます。

複数のモニターを使用している場合は、すべてのモニターまたは特定のモニターにリモート デスクトップを表示できます。最大で 3 台のモニターを選択できます。

前提条件

- この機能を使用するには、Chrome OS 86 以降が必要です。
- この機能は、公開アプリケーションではサポートされません。
- クライアント デバイスで統合デスクトップ モードが有効になっている場合、この機能はサポートされません。

`enableMultiMonitor` JSON ファイルの設定がこの機能に与える影響については、サーバ機能を参照してください。

手順

1. サーバに接続します。
2. デスクトップとアプリケーションの選択ウィンドウの右上隅にある [設定] ツールバー ボタンをクリックします。[ディスプレイ] 設定までスクロールし、[設定] をクリックします。
3. ディスプレイ オプションを選択し、[OK] をクリックします。

オプション	アクション
すべてのディスプレイを使用	接続しているすべてのモニターにリモート デスクトップ ウィンドウが表示されます。
1 台のディスプレイを使用	プライマリ モニターにリモート デスクトップが表示されます。
選択したディスプレイを使用	選択したモニターにリモート デスクトップが表示されます。選択できるのは隣接するモニターだけです。 クライアント システムに現在接続されているモニターのサムネイルが、[ディスプレイの配置] に表示されます。表示トポロジは、クライアント システムの表示設定と一致します。 リモート デスクトップ ウィンドウを表示するモニターを選択または選択解除するには、サムネイルをクリックします。サムネイルをクリックすると、色が変わります。

次のステップ

マルチモニタ モードを終了するには、リモート デスクトップ ウィンドウの上部をポイントしてメニュー バーを表示し、[マルチモニター モードを終了] ボタンをクリックします。

画面解像度の設定

Horizon Client では、ブラウザ ウィンドウのサイズに合わせてリモート デスクトップのサイズを変更できます。この機能を使用するには、適切な量のビデオ RAM (VRAM) を使用するように、Horizon 管理者がリモート デスクトップを構成する必要があります。デフォルトの VRAM 構成は 36 MB です。3D アプリケーションを使用しない場合、VRAM の最小要件は 16 MB です。

Google Chromebook Pixel など、ピクセル密度解像度が高い Chromebook デバイスを使用している場合は、その解像度を使用するようにリモート デスクトップや公開アプリケーションを設定できます。[設定] ウィンドウで [高解像度モード] オプションをオンにします。このオプションが [設定] ウィンドウに表示されるのは、高解像度ディスプレイを使用している場合か、通常の画面を 100% を超えるスケールで使用し、管理者がこの機能を無効にしている場合だけです。

高解像度モード機能を無効にする方法については、Google 管理コンソールでの登録済みの Chromebook デバイスの設定を参照してください。

高解像度モード機能では、アクティブなリモート セッションの解像度を変更できません。機能を有効にするには、ログアウトしてからもう一度ログインする必要があります。

3D レンダリング機能を使用するには、それぞれのリモート デスクトップに十分な VRAM を割り当てる必要があります。

- ソフトウェア アクセラレータによるグラフィック機能を使用すると、Windows Aero テーマや Google Earth などの 3D アプリケーションを使用できます。この機能には、64 MB ～ 128 MB の VRAM が必要です。
- vSphere 5.1 以降で利用できるハードウェア アクセラレータによるグラフィック機能 (vSGA) により、デザイン、モデリング、およびマルチメディア用の 3D アプリケーションを使用できます。この機能には、64 MB ～ 512 MB の VRAM が必要です。デフォルトは 96MB です。
- vSphere 5.5 以降で使用できる専用のハードウェア高速グラフィックス機能 (vDGA) は、ESXi ホスト上の単一の物理的な GPU（グラフィック処理ユニット）を単一の仮想マシン専用にするための機能です。この機能は、ハイエンドのハードウェア高速ワークステーション グラフィックスが必要な場合に使用します。この機能には、64 MB ～ 512 MB の VRAM が必要です。デフォルトは 96MB です。

3D レンダリングが有効である場合、モニターの最大数は 1 で、最大解像度は 3840 x 2160 です。

同様に、Google Chromebook Pixel など、ピクセル密度解像度が高い Chromebook を使用している場合は、各リモート デスクトップに十分な VRAM を割り当てる必要があります。

重要： VMware Blast 表示プロトコルに必要な VRAM 容量の計算は、PCoIP 表示プロトコルに必要な VRAM の計算に類似しています。

全画面表示モードの使用

リモート デスクトップを全画面表示モードで表示できます。

前提条件

リモート デスクトップに接続します。

手順

- リモート デスクトップを全画面表示モードで表示するには、リモート デスクトップ ウィンドウの上部をポイントしてメニュー バーを表示し、[全画面表示] ボタンをクリックします。
- 全画面表示モードを終了するには、リモート デスクトップ ウィンドウの上部をポイントしてメニュー バーを表示し、[全画面表示モードを終了] ボタンをクリックします。

DPI 同期の使用

DPI 同期機能により、リモート デスクトップまたは公開アプリケーションの DPI 設定とクライアント システムの DPI 設定が確実に一致します。

ディスプレイのスケーリング機能と同様に、DPI 同期機能を使用すると、高 DPI ディスプレイでテキストやアイコンが見やすくなります。ディスプレイのスケーリング機能の場合、フォントや画像のサイズを大きくすると、ぼやけてしまうことがありますが、DPI 同期機能の場合は、シャープさを維持した状態でフォントや画像のサイズを大きくすることができます。このため、最適なユーザー エクスペリエンスを提供するために、DPI 同期機能の使用が推奨されています。

DPI 同期を無効にすると、ディスプレイ スケーリングが使用されます。ディスプレイ スケーリング機能は、リモート デスクトップまたは公開アプリケーションを適切にスケーリングします。

DPI 同期機能は、[DPI 同期] エージェント グループ ポリシー設定で有効または無効にします。この機能は、デフォルトで有効になっています。

DPI 同期の動作

デフォルトの DPI 同期動作は、エージェント マシンにインストールされている Horizon Agent のバージョンによって異なります。

Horizon Agent 2012 以降のデフォルトでは、クライアントのモニターごとの DPI 設定がエージェントと同期され、リモート セッションの実行中に変更が有効になります。この機能は、「モニターごとの DPI 同期」エージェント グループ ポリシー設定によって制御されます。仮想デスクトップおよび物理デスクトップで、モニターごとの DPI 同期機能がデフォルトでサポートされます。この機能は、公開デスクトップでサポートされません。

以前のバージョンの Horizon Agent の場合、クライアントはシステムの DPI 設定に対してのみ同期をサポートします。DPI 同期は最初の接続時に実行されます。再接続の場合は、必要に応じてディスプレイのスケーリングが実行されます。DPI 同期が有効で、クライアント システムの DPI 設定がリモート デスクトップの DPI 設定と一致する場合、ユーザー インターフェイスで [ディスプレイのスケーリングを許可する] オプションを選択していても、ディスプレイのスケーリングを有効にすることはできません。Windows では、ユーザーが現在のユーザー セッションでシステム レベルの DPI 設定を変更することはできません。DPI の同期は、ユーザーがログインしてリモート セッションを開始した場合にのみ行われます。リモート セッションの実行中に DPI 設定を変更する場合は、リモート デスクトップの DPI 設定とクライアント システムの新しい DPI 設定を一致させるため、ログアウトしてから再度ログインする必要があります。

エージェントの DPI 設定は、Windows レジストリの `Computer\HKEY_CURRENT_USER\Control Panel\Desktop: logPixels` に保存されています。

注： システムの DPI 設定がメイン モニターの DPI 設定と異なる場合があります。たとえば、メイン モニターを閉じて、メイン モニターと異なる DPI 設定の外部ディスプレイに切り替えると、システムの DPI 設定は、終了したメイン モニターの DPI 設定と同じままになります。

このバージョンのクライアントでは、Horizon Agent バージョン 7.8 から 2006 までで提供されている「接続ごとの DPI の同期」エージェント グループ ポリシー設定はサポートされません。

DPI 同期グループ ポリシー設定の詳細については、ご使用の Horizon Agent バージョンの Horizon でのリモート デスクトップ機能の構成を参照してください。

仮想デスクトップでサポートされるゲスト OS

仮想デスクトップの場合、DPI 同期機能は次のゲスト OS に対応します。

- 32 ビットまたは 64 ビットの Windows 7
- 32 ビットまたは 64 ビットの Windows 8.x
- 32 ビットまたは 64 ビットの Windows 10
- デスクトップとして構成されている Windows Server 2012 R2
- デスクトップとして構成されている Windows Server 2016
- デスクトップとして構成されている Windows Server 2019

注： デスクトップとして構成されている Windows サーバ マシンの場合、モニターごとの DPI 同期機能はサポートされません。

公開デスクトップと公開アプリケーションでサポートされている RDS ホスト

公開デスクトップおよび公開アプリケーションでは、DPI 同期機能は次の RDS ホストでサポートされます。

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

注： RDS ホストの場合、モニターごとの DPI 同期機能はサポートされていません。この制限は、仮想マシンがホストするアプリケーション機能を使用してデスクトップ プールで実行される公開アプリケーションには適用されません

Web カメラとマイクでリアルタイム オーディオ ビデオ機能を使用

リアルタイム オーディオビデオ機能を使用すれば、リモート デスクトップまたは公開アプリケーションでクライアント マシンの Web カメラまたはマイクを使用できます。リアルタイム オーディオ ビデオは、標準的な会議アプリケーションおよびブラウザベースのビデオ アプリケーションと互換性があり、標準的な webcam、オーディオ USB デバイス、およびアナログ オーディオ入力をサポートします。

デフォルトのビデオ解像度は 320 x 240 ピクセルです。リアルタイム オーディオビデオのデフォルト設定は、ほとんどの Web カメラおよびオーディオ アプリケーションで適切に機能します。

リアルタイム オーディオビデオの設定変更の詳細については、Horizon でのリモート デスクトップ機能の構成の「リアルタイム オーディオ ビデオ グループ ポリシー設定の構成」を参照してください。

リモート デスクトップや公開アプリケーションがクライアント マシンの Web カメラやマイクに接続している場合、Web カメラやマイクがリモート デスクトップや公開アプリケーションで使用できるようになる前に、Chrome から許可を求められる場合があります。デバイスの使用を許可すると、Chrome は再度許可を要求しなくなります。

リモート デスクトップや公開アプリケーションのセッションでリアルタイム オーディオビデオを使用しており、セカンド デスクトップや公開アプリケーションへの接続するときに、セキュリティの警告が表示される場合（たとえば、有効な証明書がインストールされていないなど）、この警告を無視して 2 番目のリモート デスクトップや公開アプリケーションへの接続を続行すると、最初のセッションでリアルタイム オーディオビデオの動作が停止します。

Chromebook で優先する Web カメラまたはマイクロフォンの選択

リアルタイム オーディオビデオ機能で、ローカル クライアント システムに複数の Web カメラまたはマイクが接続されている場合、リモート デスクトップまたは公開アプリケーションで使用されるデバイスは 1 つだけです。優先する Web カメラまたはマイクを指定するには、Horizon Client for Chrome でリアルタイム オーディオ ビデオ機能を設定する必要があります。

使用可能な場合、優先 web カメラまたはマイクがリモート デスクトップまたは公開アプリケーションで使用されます。優先 Web カメラまたはマイクが使用できない場合は、他の Web カメラまたはマイクが使用されます。

前提条件

- USB Web カメラや USB マイクまたは他のタイプのマイクがインストールされ、ローカル クライアント システムで動作できる状態であることを確認します。
- サーバに接続します。

手順

1. デスクトップとアプリケーションの選択ウィンドウの右上隅にある [設定] ツールバー ボタンをクリックし、リアルタイム オーディオビデオ (RTAV) の設定までスクロールします。
2. [優先マイク] ドロップダウン メニューから、優先するマイクを選択します。
3. [優先 Web カメラ] ドロップダウン メニューから、優先する Web カメラを選択します。

結果

リモート デスクトップや公開アプリケーションを次回起動するときに、優先するように選択した Web カメラやマイクが、リモート セッションにリダイレクトされます。

リモート デスクトップの使用

リモート デスクトップ ウィンドウの上部メニュー バーを使用すると、リモート デスクトップで一般的なタスクを実行できます。

- リモート デスクトップで上部メニュー バーを開くには、リモート デスクトップ ウィンドウの上部にマウスを移動して上部メニュー バーを表示します。
- リモート デスクトップ内で Ctrl + Alt + Del キーボード ショートカットを使用するには、上部メニュー バーの [Ctrl + Alt + Delete を現在の作業領域へ送信] ボタンをクリックします。
- 全画面モードに切り替えるには、上部メニュー バーの [全画面表示] ボタンをクリックします。全画面モードを終了するには、上部メニュー バーの [全画面表示モードを中止] ボタンをクリックします。
- リモート デスクトップに USB デバイスをリダイレクトするには、上部のメニュー バーの [USB デバイスのリダイレクト] ボタンをクリックします。

- マルチモニタ モードを終了するには、上部メニュー バーの [マルチモニタ モードを中止] をクリックします。
- リモート デスクトップから切断するには、上部メニュー バーの [切断] ボタンをクリックするか、リモート デスクトップ ウィンドウの右上隅にある [X]（閉じる）ボタンをクリックします。
- Horizon Client に関する情報を表示するには、上部メニュー バーの [バージョン情報] ボタンをクリックします。

開いている別のリモート デスクトップに切り替えるには、そのリモート デスクトップ ウィンドウをクリックします。Alt + Tab キーを押すと、クライアント デバイスで開いているリモート デスクトップ（ローカル アプリケーションと公開アプリケーションを含む）の間を移動できます。選択したリモート デスクトップにフォーカスを移動するには、Alt キーを放します。

リモート デスクトップからのログオフの詳細については、ログオフまたは切断を参照してください。リモート デスクトップの再起動の詳細については、リモート デスクトップの再起動を参照してください。リモート デスクトップのリセットの詳細については、リモート デスクトップまたは公開アプリケーションのリセットを参照してください。

公開アプリケーションの使用

Horizon Client は、公開アプリケーションの使用に役立つナビゲーション機能を提供します。

- 公開アプリケーションを最大化または最小化するには、他のアプリケーションと同じように [最大化] ボタンまたは [最小化] ボタンをクリックします。
- 最小化された公開アプリケーションをリストアするには、クライアント デバイスでシェルフ アイコンをクリックするか、セッション管理センターの画面で公開アプリケーション セッションを選択して、[リストア] ボタンをクリックします。キオスク モードの場合、セッション管理センターを使用して、最小化された公開アプリケーションをリストアする必要があります。詳細については、キオスク モードでの公開アプリケーションの使用を参照してください。
- 公開アプリケーションをリセットするには、リモート デスクトップまたは公開アプリケーションのリセットを参照してください。

開いている別の公開アプリケーションに切り替えるには、公開アプリケーション ウィンドウをクリックします。Alt + Tab キーを押すと、クライアント デバイスで開いている公開アプリケーション（ローカル アプリケーションとリモート デスクトップを含む）の間を移動できます。選択した公開アプリケーションにフォーカスを移動するには、Alt キーを放します。

キオスク モードでの公開アプリケーションの使用

キオスク モードで公開アプリケーションを使用している場合、特定のタスクをセッション管理センターで行う必要があります。

- セッション管理センターの画面を開くには、デスクトップとアプリケーションの選択ウィンドウの右上隅にある [設定] ツールバー ボタンをクリックし、[セッション管理センター] の横にある [開く] をクリックします。リモート デスクトップ セッションを開いている場合は、デスクトップとアプリケーションの選択ウィンドウにアクセスする前に、リモート デスクトップ セッションを閉じる必要があります。
- キオスク モードで、最小化された公開アプリケーションをリストアするには、セッション管理センターの画面で公開アプリケーション セッションを選択して、[リストア] ボタンをクリックします。

- キオスク モードで公開アプリケーションを切り換えるには、セッション管理センターの画面で公開アプリケーション セッションを選択して、[リストア] ボタンをクリックします。
- キオスク モードでセッション管理センターの画面を閉じるには、セッション管理センターの画面右上隅にある [X]（閉じる）ボタンをクリックします。

テキストとイメージのコピー アンド ペースト

デフォルトでは、クライアント デバイスのプレーン テキストと HTML 形式のリッチ テキストをコピーして、リモート デスクトップまたは公開アプリケーションに貼り付けることができます。

Horizon 管理者がこの機能を有効にしている場合、リモート デスクトップまたは公開アプリケーションからプレーン テキストや HTML 形式のリッチ テキストをコピーし、貼り付けることができます。

Horizon 管理者は、クライアント デバイスからリモート デスクトップまたは公開アプリケーションへのコピー アンド ペースト操作のみを許可する、リモート デスクトップまたは公開アプリケーションからクライアント デバイスへのコピー アンド ペースト操作のみを許可する、その両方を許可する、またはどちらも許可しないように、この機能を構成できます。

イメージやリッチ テキストをコピーして貼り付ける場合、次の制限があります。

- クリップボード ソースが Google Docs などの Google アプリケーションの場合、クライアント デバイスが Google の Web サイトにアクセスできれば、イメージをコピーして貼り付けることができます。
- クライアント デバイスからイメージとリッチ テキスト（またはプレーン テキスト）をまとめてコピーして、リッチ テキストにしか対応していないコピー先（WordPad など）を貼り付けると、イメージは破棄され、テキストのみが貼り付けられます。Microsoft Word など、コピー先のアプリケーションが HTML / XML 形式のリッチ テキストをサポートしている場合、このような制限はありません。
- Horizon 管理者は、コピー アンド ペーストする時に、グループ ポリシーを使用してクリップボードの形式を制限できます。Microsoft Office のチャートおよび Smart Art データと Microsoft の文字効果データについては、クリップボードの形式フィルタ ポリシーはサポートされません。クリップボードの形式フィルタ ポリシーについては、Horizon でのリモート デスクトップ機能の構成ドキュメントを参照してください。スマート ポリシーを使用したリモート デスクトップのコピー アンド ペーストの動作の制御は、サポートされていません。

リモート デスクトップまたは公開アプリケーションからクライアント デバイスにコピーできるのは、最大で 64 KB のデータまでです。この制限を超えるプレーン テキストは切り詰められます。リッチ テキストはプレーン テキストに変換されます。

どのタイプのコピー アンド ペーストの操作でも、クリップボードは最大で 1 MB のデータを処理できます。プレーン テキストとリッチ テキスト データを合わせたサイズが最大クリップボード サイズより小さければ、フォーマットされたテキストが貼り付けられます。リッチ テキストは多くの場合に分割できないため、テキストとフォーマットのサイズが最大クリップボード サイズより大きい場合は、リッチ テキストが破棄されてプレーン テキストが貼り付けられます。1 回の操作では選択したフォーマット テキストすべてを貼り付けできない場合は、1 回の操作でコピー アンド ペーストを行うサイズを小さくする必要があります。

コピー アンド ペースト アクティビティの記録

クリップボード監査機能を有効にすると、Horizon Agent は、コピーアンドペースト アクティビティに関する情報をエージェント マシンのイベント ログに記録します。デフォルトでは、クリップボード監査機能は無効になっています。

クリップボード監査機能を有効にするには、[クリップボード監査の設定] グループ ポリシー設定を使用する必要があります。

オプションで、[クライアントが監査をサポートしていないときに、クライアント側へのクリップボードのリダイレクトをブロックするかどうかを設定します] グループ ポリシー設定を使用して、クリップボード監査機能をサポートしていないクライアントでクリップボード リダイレクトをブロックするかどうか指定できます。

クリップボード リダイレクトのグループ ポリシー設定の詳細については、Horizon でのリモート デスクトップ機能の構成を参照してください。

この機能を使用するには、エージェント マシンに Horizon Agent 7.7 以降が必要です。

コピーアンドペースト アクティビティの情報が記録されるイベント ログの名前は VMware Horizon RX Audit です。エージェント マシンでイベント ログを表示するには、Windows イベント ビューアを使用します。イベント ログを一元的に表示するには、VMware Log Insight または Windows Event Collector を設定します。Log Insight の詳細については、https://docs.vmware.com/jp/vRealize-Log-Insight/index.html を参照してください。Windows Event Collector の詳細については、Microsoft のドキュメントを参照してください。

リモート デスクトップまたは公開アプリケーションとクライアントの間でのファイルの転送

クライアント デバイスからリモート デスクトップまたは公開アプリケーションにファイルを転送できます。リモート デスクトップまたは公開アプリケーションからクライアント システムにファイルを転送できる場合もあります。

ファイルをアップロードするには、クライアント システムからリモート デスクトップまたは公開アプリケーションのウィンドウにファイルをドラッグします。アップロードが完了すると、ファイルが `C:\Users\`*`username`*`\Documents` フォルダに表示されます。

ファイルをダウンロードするには、Ctrl + C キーを押して、リモート デスクトップまたは公開アプリケーションでファイルを選択します。ファイルの転送を確認すると、クライアント デバイスの `Downloads` ディレクトリにファイルが表示されます。

Horizon 管理者は、VMware Blast の [ファイル転送を設定] グループ ポリシー設定を変更することにより、ファイルの転送を許可、禁止、または一方向のみ許可するように設定できます。このグループ ポリシー設定の値は次のとおりです。

- [アップロードとダウンロードの両方を無効にする] の値が選択されている場合、いずれの方向にもファイルを転送できません。
- [ファイルのアップロードのみを有効にする] が選択されている場合（デフォルトの設定）、クライアント システムからリモート デスクトップまたは公開アプリケーションにのみファイルを転送できます。
- [ファイルのダウンロードのみを有効にする] が選択されている場合は、リモート デスクトップまたは公開アプリケーションからクライアント システムにのみファイルを転送できます。

サーバからクライアントの方向で [クリップボード リダイレクトの設定] グループ ポリシー設定が無効になっている場合、ファイルのダウンロードも無効になります。

これらのグループ ポリシー設定の詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。

この機能には次の制限があります。

- ダウンロードできるファイルは最大で 500 MB までです。アップロードできるファイルは最大で 2 GB までです。
- フォルダまたはサイズがゼロのファイルのダウンロードまたはアップロードはできません。
- リモート セッションでファイルを転送中に、別のリモート セッションとの接続を試みてセキュリティ警告が表示されたときに、この警告を無視してリモート セッションとの接続を続行すると、最初のセッションで実行中のファイル転送が中止されます。

クライアント ドライブのリダイレクトによるローカル フォルダおよびドライブの共有

クライアント ドライブ リダイレクト機能を使用すると、ローカル クライアント システムのフォルダまたはドライブをリモート デスクトップや公開アプリケーションと共有できます。

共有ドライブには、マッピングされたドライブおよび USB ストレージ デバイスを含めることができます。

クライアント ドライブ リダイレクト機能には次の制限があります。

- Windows レジストリ キーの設定 `ForcedByAdmin`、`default shares`、`permissions` を使用してクライアント ドライブ リダイレクトを設定することはできません。
- TCP および UDP サイド チャネルはサポートされていません。エージェント マシンがいずれかのサイド チャネルを使用するように設定されている場合は、クライアント ドライブ リダイレクト機能を使用できません。
- Dynamic Environment Manager ポリシーはサポートされていません。
- ネットワーク リカバリはサポートされていません。セッションを切断して再度接続しない限り、ネットワーク接続後にクライアント ドライブ リダイレクトを使用することはできません。
- クライアント ドライブ リダイレクト機能は、1 回に 1 つのリモート セッションでのみ使用できます。複数のリモート セッションでは使用できません。
- リモート デスクトップの共有フォルダまたはファイルのプロパティは変更できません。

前提条件

フォルダおよびドライブをリモート デスクトップまたは公開アプリケーションと共有するには、Horizon 管理者がクライアント ドライブのリダイレクト機能を有効にする必要があります。これには、Horizon Agent をインストールして、エージェントの [クライアント ドライブ リダイレクト] オプションを有効にする作業も含まれます。ポリシーの設定を行って、クライアント ドライブ リダイレクトの動作を制御することも含まれる場合があります。詳細については、Horizon でのリモート デスクトップ機能の構成を参照してください。

手順

1. デスクトップとアプリケーションの選択ウィンドウの右上隅にある [設定] ツールバー ボタンをクリックし、[設定] ウィンドウで [フォルダの共有を有効にする] オプションをオンにします。
2. 共有する特定のフォルダまたはドライブを選択するには、[選択] をクリックして、[追加] をクリックします。フォルダまたはドライブ検索して選択し、[OK] をクリックします。

   複数のフォルダまたはドライブを追加できますが、1 回に選択できるのは 1 項目だけです。フォルダまたはドライブを削除するには、[フォルダの共有] ダイアログ ボックスでフォルダ名またはドライブ名の横にある [X] をクリックします。
3. 設定を保存するには、[OK] をクリックします。

   フォルダ共有の設定は、すべてのリモート デスクトップと公開アプリケーションに適用されます。

結果

リモート デスクトップでは、共有したフォルダとドライブのネットワーク上の場所が表示されます。たとえば、`test1` という名前のフォルダを共有した場合、リモート デスクトップに `test1(Z:)` のようにネットワーク上の場所が表示されます。共有フォルダまたはドライブのデバイスも表示されます。デバイス名は、*`folder`* `on Horizon` の形式になります（例：`test1 on Horizon`）。

公開アプリケーションでは、[ファイル] - [開く] の順に選択するか、[ファイル] - [名前を付けて保存] の順に選択すると、共有フォルダまたはドライブに移動できます。

リモート デスクトップでの USB デバイスの使用

USB リダイレクト機能を使用すると、ローカルに接続された USB デバイスをリモート デスクトップで使用できます。リモート デスクトップに複数の USB デバイスをリダイレクトできます。USB デバイスを公開デスクトップと公開アプリケーションにリダイレクトすることはできません。

Chrome OS の制限により、多くの USB デバイスをリモート デスクトップにリダイレクトすることはできません。このリリースで VMware が動作確認した USB デバイスは次のとおりです。他のデバイスがサポートされる場合もあります。USB デバイスがサポートされていない場合、デバイスにリダイレクトすると、Horizon Client からエラー メッセージが返されます。

- プリンタ
  - Brother MFC 8710 DW
  - Brother QL-720NW
  - HP LaserJet Pro M201dw
  - HP LaserJet Pro MFP M426dfw
  - HP LaserJet P2055d
  - HP Deskjet 3525
  - HP OfficeJet 200 Mobile
  - Ricoh SP C261SNFw

- Samsung C43x Print Series
- Xerox WorkCentre 6515
- Xerox Workcentre 3225/DNI Printer
- Zebra Label printer GC420-1005G0-000

- スキャナ
  - AmbirScanPro 490i
- ヒューマン インターフェイス デバイス (HID)
  - Wacom 520A
  - Wacom 500B

前提条件

- この機能を使用するには、Chrome OS 87 以降が必要です。
- Horizon 管理者は、リモート デスクトップに USB リダイレクト機能を構成する必要があります。

リモート デスクトップの USB リダイレクト機能の構成の詳細については、Horizon でのリモート デスクトップ機能の構成の「Chrome および HTML Access クライアントの USB リダイレクトの構成」を参照してください。

手順

1. USB デバイスを Chromebook に接続します。
2. Horizon Client を起動して、リモート デスクトップに接続します。
3. リモート デスクトップ ウィンドウの上部にマウスを移動します。上部のメニュー バーが表示されたら、[USB デバイスのリダイレクト] ボタンをクリックします。
4. [デバイスを追加] をクリックします。
5. USB デバイスのリストからデバイスを選択して、[選択] をクリックします。

   デバイスがサポートされている場合、デバイスはリモート デスクトップにリダイレクトされ、セッションで使用できます。デバイスがサポートされていない場合は、エラー メッセージが表示されます。
6. （オプション） [デバイスを追加] を再度クリックして、別の USB デバイスをリダイレクトします。
7. リモート デスクトップから USB デバイスを解放するには、[解放] をクリックします。

リモート デスクトップまたは公開アプリケーションからの印刷

VMware Integrated Printing 機能を使用すると、リモート デスクトップまたは公開アプリケーションから、ネットワーク プリンタまたはローカル接続のプリンタで印刷することができます。

この機能を使用するには、仮想マシンまたは RDS ホストに Horizon Agent がインストールされている必要があります。また、VMware Integrated Printing オプションが有効になっている必要があります。詳細については、Horizon での仮想デスクトップのセットアップまたは Horizon での公開されたデスクトップとアプリケーションのセットアップを参照してください。

Horizon 管理者は、[デスクトップ以外のクライアントでプリンタ リダイレクトを無効にする] グループ ポリシー設定を使用して、VMware Integrated Printing 機能を無効にできます。詳細については、Horizon でのリモート デスクトップ機能の構成を参照してください。

VMware Integrated Printing 機能の印刷設定を行う

リモート デスクトップで VMware Integrated Printing 機能の印刷設定を行うことができます。VMware Integrated Printing 機能を使用すると、Windows リモート デスクトップに追加のプリンタ ドライバをインストールすることなく、リモート デスクトップからローカルまたはネットワーク プリンタを使用できます。この機能で使用可能なプリンタごとに、データ圧縮、印刷品質、両面印刷、カラーなどの環境設定を行うことができます。

シングル ユーザー仮想マシン デスクトップの場合、仮想プリンタはデフォルトで *<printer_name>*(*vdi*) と表示されます。公開デスクトップまたは公開アプリケーションの場合、仮想プリンタはデフォルトで *<printer_name>*(v*<session_ID>*) と表示されます。

Horizon Agent 7.12 以降では、グループ ポリシーを使用して、リダイレクトされるクライアント プリンタの命名規則を変更できます。詳細については、ご使用の Horizon Agent バージョンの Horizon でのリモート デスクトップ機能の構成を参照してください。

前提条件

VMware Integrated Printing を使用するには、Horizon 管理者がリモート デスクトップの VMware Integrated Printing 機能をインストールする必要があります。このタスクでは、Horizon Agent インストーラで [VMware Integrated Printing] オプションを有効にします。Horizon Agent のインストール方法については、Horizon での仮想デスクトップのセットアップまたは Horizon での公開されたデスクトップとアプリケーションのセットアップドキュメントを参照してください。VMware Integrated Printing 機能の構成については、Horizon でのリモート デスクトップ機能の構成を参照してください。

リモート デスクトップに VMware Integrated Printing 機能がインストールされているかどうかを確認するには、リモート デスクトップのファイル システムに `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-server.exe` ファイルと `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-service.exe` ファイルが存在することを確認します。

この機能には、Horizon Agent 7.12 以降が必要です。

手順

1. Windows リモート デスクトップで、[コントロール パネル] - [ハードウェアとサウンド] - [デバイスとプリンタ] の順に移動します。
2. [デバイスとプリンタ] ウィンドウで仮想プリンタを右クリックし、コンテキスト メニューから [プリンタ プロパティ] を選択します。
3. [全般] タブで、[環境設定] をクリックします。
4. [印刷設定] ダイアログ ボックスで、異なるタブを選択して使用する設定を指定します。
5. 変更内容を保存するには、[OK] をクリックします。

異なるクライアント デバイスでの公開アプリケーションの複数のセッションの使用

公開アプリケーションの複数セッション モードを有効にすると、異なるクライアント デバイスからサーバにログインしたときに、同じ公開アプリケーションの複数のセッションを使用できます。

たとえば、クライアント A で公開アプリケーションを複数セッション モードで開き、同じ公開アプリケーションをクライアント B で開くと、クライアント A で公開アプリケーションが開いたまま、クライアント B で公開アプリケーションの新しいセッションが開きます。複数セッション モードが無効になっている場合（単一セッション モードの場合）は、クライアント A の公開アプリケーションのセッションが切断され、クライアント B で再接続されます。

複数セッション モード機能には次の制限があります。

- Skype for Business など、複数のインスタンスをサポートしていないアプリケーションの場合、複数セッション モードは機能しません。
- 複数セッション モードで公開アプリケーションを使用しているときにアプリケーション セッションが切断されると、自動的にログアウトされ、未保存のデータは失われます。

前提条件

Horizon 管理者は、アプリケーション プールの複数セッション モードを有効にする必要があります。Horizon 管理者が許可しない限り、ユーザーは公開アプリケーションの複数セッション モードを変更できません。Horizon での公開されたデスクトップとアプリケーションのセットアップを参照してください。この機能には、Horizon 7 のバージョン 7.7 以降が必要です。

手順

1. サーバに接続します。
2. デスクトップとアプリケーションの選択ウィンドウの右上隅にある [設定] ツールバー ボタンをクリックします。[マルチ起動] 設定までスクロールし、[設定] をクリックします。

   リモート デスクトップまたは公開アプリケーションを以前に開始した場合は、サイドバーにある [メニューを開く] ボタンをクリックし、[設定] をクリックして [マルチ起動] 設定までスクロールします。複数セッション モードで使用できる公開アプリケーションがない場合、[マルチ起動] 設定はグレーアウトされます。
3. 複数セッション モードで使用する公開アプリケーションを選択して、[OK] をクリックします。

   Horizon 管理者が公開アプリケーションに複数セッション モードを適用している場合、この設定を変更することはできません。

リモート デスクトップと公開アプリケーションのサウンドの調整

デフォルトでは、リモート デスクトップおよびアプリケーションでの音声の再生が有効になっていますが、Horizon 管理者がポリシーを設定することで、音声の再生を無効にできます。リモート デスクトップや公開アプリケーションで音声を再生するときに、いくつかの制限が適用されます。

- 音量を上げるには、リモート デスクトップのサウンド コントロールではなく、クライアント システムのサウンド コントロールを使用します。
- 時々、音声がビデオと同期しなくなることがあります。

- ネットワーク トラフィックが集中していたり、ブラウザが大量のタスクを実行していると、音質が低下することがあります。

ショートカット キーの組み合わせ

使用する言語に関係なく、一部のキーの組み合わせはリモート デスクトップまたは公開アプリケーションに送信できません。

Chrome によって、一部のキーおよびキーの組み合わせをクライアント システムおよび送付先システムの両方に送信することができます。他のキーおよびキーの組み合わせについては、ローカルでの入力だけが処理され、送付先システムには送信されません。

以下のキーおよびキーの組み合わせは、リモート デスクトップで動作しない場合があります。

- Ctrl + T
- Ctrl + W
- Ctrl + N
- コマンド キー
- Alt + Enter
- Ctrl + Alt + *任意のキー*

  重要： Ctrl + Alt + Del キーを入力するには、サイドバーの先頭にある [Ctrl+Alt+Delete を送信] ツールバー ボタンを使用します。

- Caps Lock + *modifier_key*（Alt または Shift など）
- Chromebook のファンクション キー
- Windows キーの組み合わせ

リモート デスクトップで Windows キーを有効にした場合、リモート デスクトップで次の Windows キーの組み合わせが動作します。この機能を有効にするには、サイドバーにある [[設定] ウィンドウを開く] ツールバー ボタンをクリックして、[デスクトップで Windows キーを有効にします] をオンにします。

[デスクトップで Windows キーを有効にします] をオンにした後、Ctrl+Search キーを押して、Windows キーの押下をシミュレーションします。

これらのキーの組み合わせは、公開アプリケーションで動作しません。これらのキーの組み合わせは、Windows Server 2012 R2 と Windows Server 2016 のリモート デスクトップと公開デスクトップで動作します。

Windows 8.x や Windows Server 2012 R2 オペレーティング システムのリモート デスクトップで動作するいくつかのキーの組み合わせは、Windows 7 または Windows 10 オペレーティング システムのリモート デスクトップでは動作しません。

表 3-1. Windows 10 リモート デスクトップと Windows Server 2016 リモート デスクトップの Windows キー ショートカット

キー	アクション	制限
Win	スタートを開くまたは閉じます。	
Win + A	アクション センターを開きます。	
Win + E	ファイル エクスプローラーを開きます。	
Win + G	ゲームが開いているときに、ゲーム バーを開きます。	
Win + H	[共有] チャームを開きます。	
Win + I	[設定] チャームを開きます。	
Win + K	[接続] クイック アクションを開きます。	
Win + M	すべてのウィンドウを最小化します。	
Win + R	[ファイル名を指定して実行] ダイアログ ボックスを開きます。	
Win + S	[検索] を開きます。	
Win + X	[クイック リンク] メニューを開きます。	
Win + ,（カンマ）	リモート デスクトップを一時的に表示します。	
Win + Enter	ナレーターを開きます。	

表 3-2. Windows 8.x および Windows Server 2012 R2 リモート デスクトップの Windows キー ショートカット

キー	アクション	制限
Win + F1	Windows ヘルプとサポートを開きます。	
Win	[スタート] ウィンドウを表示または非表示にします。	
Win + B	通知領域にフォーカスを設定します。	
Win + C	チャーム パネルを開きます。	
Win + D	リモート デスクトップを表示または非表示にします。	
Win + E	ファイル エクスプローラーを開きます。	
Win + H	[共有] チャームを開きます。	
Win + I	[設定] チャームを開きます。	
Win + K	[デバイス] チャームを開きます。	
Win + M	すべてのウィンドウを最小化します。	
Win + Q	アプリケーションの検索がサポートされている場合、開いているアプリ内または任意の場所を検索するため、[検索] チャームを開きます。	
Win + R	[ファイル名を指定して実行] ダイアログ ボックスを開きます。	
Win + S	Windows と Web を検索するため、[検索] チャームを開きます。	
Win + X	[クイック リンク] メニューを開きます。	
Win + Z	アプリケーションで利用可能なコマンドを表示します。	
Win + ,（カンマ）	このキーの組み合わせを押し続けている限り、リモート デスクトップを一時的に表示します。	Windows 2012 R2 オペレーティング システムでは動作しません。

表 3-2. Windows 8.x および Windows Server 2012 R2 リモート デスクトップの Windows キー ショートカット （続き）

キー	アクション	制限
Win + Shift + M	リモート デスクトップで最小化されたウィンドウを元に戻します。	
Win + Home	アクティブなリモート デスクトップのウィンドウ以外のすべてのウィンドウを最小化します (Win + Home キーをもう一度押すとすべてのウィンドウが元に戻ります)。	
Win + Enter	ナレーターを開きます。	

表 3-3. Windows 7 リモート デスクトップの Windows キーのショートカット

キー	アクション	制限
Win	[スタート] メニューを開くまたは閉じます。	
Win + D	リモート デスクトップを表示または非表示にします。	
Win + M	すべてのウィンドウを最小化します。	
Win + E	`Computer` フォルダを開きます。	
Win + R	[ファイル名を指定して実行] ダイアログ ボックスを開きます。	
Win + Home	アクティブなリモート デスクトップのウィンドウを除くすべてのウィンドウを最小化します。	
Win + G	実行中のリモート デストップ ガジェットを順に切り換えます。	
Win + U	[コンピューターの簡単操作センター] を開きます。	

利用可能な言語

Horizon Client のユーザー インターフェイスとドキュメントは、英語、日本語、フランス語、ドイツ語、簡体字中国語、繁体字中国語、韓国語、およびスペイン語で利用可能です。これらの言語で文字を入力することもできます。

トラブルシューティング

4

Horizon Client の大部分の問題は、リモート デスクトップや公開アプリケーションをリセットするか、Horizon Client を再インストールすると解決できます。

この章には、次のトピックが含まれています。

リモート デスクトップの再起動

リモート デスクトップのオペレーティング システムが応答しない場合、リモート デスクトップの再起動が必要になることがあります。リモート デスクトップの再起動は、Windows オペレーティング システムの再起動コマンドと似ています。通常、リモート デスクトップのオペレーティング システムは、再起動の前に未保存データを保存するように求めます。

Horizon 管理者がリモート デスクトップの再起動機能を有効にしている場合にのみ、リモート デスクトップを再起動できます。

デスクトップの再起動機能を有効にする操作の詳細については、Horizon での仮想デスクトップのセットアップまたは Horizon での公開されたデスクトップとアプリケーションのセットアップを参照してください。

手順

- デスクトップとアプリケーションの選択画面の右上隅にある [設定] ツールバー ボタンをクリックします。セッション管理センターを開いてリモート デスクトップ セッションを選択し、[再起動] をクリックします。

  また、シェルフでリモート デスクトップのアイコンを右クリックして、[セッション管理センター] をクリックしても、セッション管理センターを開くことができます。

  注： リモート デスクトップに接続して切断した場合を除き、セッション管理センターにリモート デスクトップ セッションは表示されません。

結果

リモート デスクトップのオペレーティング システムが再起動し、クライアントがリモート デスクトップから切断され、ログオフされます。

次のステップ

システムが完全に再起動するまで待機してから、リモート デスクトップへの再接続します。

リモート デスクトップまたは公開アプリケーションのリセット

デスクトップ オペレーティング システムが応答を停止し、リモート デスクトップを再起動しても問題が解決しない場合は、リモート デスクトップをリセットする必要がある場合があります。

リモート デスクトップをリセットする操作は、物理的な PC を強制的に再起動するときに PC のリセット ボタンを押す操作と同じです。リモート デスクトップで開いているすべてのファイルが閉じられますが、保存されません。

公開アプリケーションをリセットすると、未保存のデータを保存せずにアプリケーションを終了します。実行中のすべての公開アプリケーションをリセットすることも、特定の公開アプリケーション セッションをリセットすることもできます。

Horizon 管理者がリモート デスクトップのリセット機能を有効にしている場合にのみ、リモート デスクトップをリセットできます。

デスクトップのリセット機能を有効にする操作の詳細については、Horizon での仮想デスクトップのセットアップまたは Horizon での公開されたデスクトップとアプリケーションのセットアップを参照してください。

手順

1. 実行中のすべての公開アプリケーションをリセットするには、デスクトップとアプリケーションの選択画面の右上隅にある [設定] ツールバー ボタンをクリックします。[実行中のすべてのアプリケーションをリセットします] までスクロールして、[リセット] をクリックします。
2. 公開アプリケーション セッションをリセットするには、デスクトップとアプリケーションの選択画面の右上隅にある [設定] ツールバー ボタンをクリックします。セッション管理センターを開き、アプリケーション セッションの [リモート アプリケーション] ボタンを選択して、[終了する] をクリックします。

   また、シェルフで公開アプリケーションのアイコンを右クリックして、[セッション管理センター] をクリックしても、セッション管理センターを開くことができます。
3. リモート デスクトップをリセットするには、デスクトップとアプリケーションの選択画面の右上隅にある [設定] ツールバー ボタンをクリックします。セッション管理センターを開いてリモート デスクトップ セッションを選択し、[リセット] をクリックします。

   また、シェルフで公開アプリケーションのアイコンを右クリックして、[セッション管理センター] をクリックしても、セッション管理センターを開くことができます。

結果

リモート デスクトップをリセットすると、リモート デスクトップのオペレーティング システムが再起動し、クライアントがリモート デスクトップから切断され、ログオフされます。公開アプリケーションをリセットすると、そのアプリケーションは終了します。

次のステップ

システムが完全に再起動するまで待機してから、リモート デスクトップや公開アプリケーションに再接続します。

Horizon Client for Chrome のアンインストール

VMware Horizon Client for Chrome アプリケーションは、他の Chromebook アプリケーションと同じ方法で削除します。

手順

1 Chromebook にログインします。

2 VMware Horizon Client アプリケーションを右クリックして、[アンインストール] を選択します。

次のステップ

VMware Horizon Client for Chrome アプリケーションを再インストールする場合は、 Horizon Client for Chrome のインストールまたはアップグレードを参照してください。

ログ収集の有効化

ログ収集を有効にすると、Horizon Client は、VMware による Horizon Client の問題のトラブルシューティングに役立つログ情報を収集します。

リモート デスクトップまたは公開アプリケーションに接続した後に、ログの収集を有効にすることはできません。

前提条件

サーバに接続します。

手順

1 デスクトップとアプリケーションの選択ウィンドウの右上隅にある [設定] ツールバー ボタンをクリックします。

2 ログの収集を有効にするには、[設定] ウィンドウで [ログの収集を有効にする] オプションを有効にし、ログ レベルに [基本]、[デバッグ] または [トレース] を選択します。

   ログ ファイルのパスが [設定] ウィンドウの [ログの収集を有効にする] オプションの下に表示されます。

3 ログ ファイルのパスを変更するには、デフォルトのパスをクリックして、ログ ファイルを保存するフォルダを選択し、[保存] を選択します。

   新しいパスが [設定] ウィンドウの [ログの収集を有効にする] オプションの下に表示されます。

4 [設定] ウィンドウを閉じるには、[閉じる] をクリックします。

結果

Horizon Client を終了するまで、Horizon Client はログ情報を継続的に収集し、保存します。