HTML Access の使用

2015 年 3 月

VMware Horizon 6

このドキュメントは新しいエディションに置き換わるまで、ここで書いてある各製品と後続のすべてのバージョンをサポートします。このドキュメントの最新版をチェックするには、http://www.vmware.com/jp/support/pubs を参照してください。

JA-001116-06

vmware®

最新の技術ドキュメントは VMware の Web サイト（http://www.vmware.com/jp/support/）にあります
VMware の Web サイトでは最新の製品アップデートも提供されています。
このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

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

HTML Access の使用

本『HTML Access の使用』ガイドでは、クライアント システムにソフトウェアをインストールせずに仮想デスクトップに接続するために VMware Horizon™ （および View™）の HTML Access 機能をインストールして使用する方法について説明します。

最終的に Web ブラウザを使用してユーザーがリモート デスクトップにアクセスできるように、View Server およびリモート デスクトップ仮想マシンに HTML Access ソフトウェアをインストールするためのシステム要件および手順について説明しています。

重要　この情報は、View および VMware vSphere を使用した経験がある管理者を対象としています。View に慣れていないユーザーである場合、『View インストール ガイド』および『View 管理ガイド』のステップを追った基本手順の参照が必要な場合があります。

1 セットアップとインストール

HTML Access 用の View 環境のセットアップでは、View 接続サーバでの HTML Access をインストールし、必要なポートを開き、リモート デスクトップ仮想マシンで HTML Access コンポーネントをインストールする作業が含まれます。

エンド ユーザーは、サポートされるブラウザを開いて、View 接続サーバの URL を入力してリモート デスクトップにアクセスできます。

この章では次のトピックについて説明します。

HTML Access のシステム要件

HTML Access を使用すれば、クライアント システムでは、サポートされるブラウザ以外のソフトウェアは必要ありません。View の導入では、特定のソフトウェア要件を満たす必要があります。

クライアント システムのブラウザ

以下の Web ブラウザがサポートされます。

	Chrome	Internet Explorer	Safari	Mobile Safari	Firefox
HTML Access 2.6	38 および 39	10 および 11	6.2、7、および 8	iOS 7 以降	33
HTML Access 2.5	35、36、および 37	9 (限定サポート)、10、および 11	6.1.3 および 7	iOS 7 以降	30 および 31
HTML Access 2.4	33 および 34	9 (限定サポート)、10、および 11	6.1.3 および 7	iOS 7 以降	28 および 29

クライアント オペレーティング システム

- Windows XP SP3 (32 ビット)
- Windows 7 SP1 または SP (32 または 64 ビット)
- Windows 8.x デスクトップ (32 または 64 ビット)

- Windows Vista SP1 または SP2 (32 ビット)
- Mac OS X Snow Leopard (10.6.8)
- Mac OS X Lion (10.7)
- Mac OS X Mountain Lion (10.8)
- Mac OS X Mavericks (10.9)
- Mac OS X Yosemite (10.10)
- iOS 7.0 以降の iPad (したがって、iPad 1 はサポートされていません)
- Chrome OS 28。<x> 以降

リモート デスクトップ

以下のソフトウェアは、エンド ユーザーがアクセスする仮想マシンにインストールする必要があります：

- 単一ユーザーの View デスクトップのオペレーティング システム：View Agent 6.0.x を使用している場合は、Windows XP SP3（32 ビット）および Windows Vista（32 ビット）がサポートされます。View Agent 6.0.x 以降を使用している場合は、Windows 7（32 ビットまたは 64 ビット）および Windows Server 2008 R2 もサポートされます。View Agent 6.0.1 以降を使用している場合は、Windows 8 （32 ビットまたは 64 ビット）および Windows 8.1 （32 ビットまたは 64 ビット）リモート デスクトップもサポートされます。View Agent 6.1 以降を使用している場合は、Windows Server 2012 R2 もサポートされます。
- RDS ホスト上のセッションベースの View デスクトップのオペレーティング システム：View Agent 6.0.2 以降を使用している場合は、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2 がサポートされます。
- View Agent：HTML Access 2.6 には、View Agent 6.1 または View Agent 6.0.2 が必要です。HTML Access 2.5 には、View Agent 6.0.1 が必要です。HTML Access 2.4 には、View Agent 6.0 が必要です。

  インストール手順は、『View でのデスクトップとアプリケーションの設定』に記載されています。

重要　リモート デスクトップは仮想マシンである必要があります。View Agent を物理マシンにインストールすることもできますが、Blast プロトコルを HTML Access と共に使用する場合は、物理マシンにアクセスできません。View Agent は仮想マシンにインストールする必要があります。

プールの設定

HTML Access では、View Administrator で以下のプール設定が必要です：

- [1 台のモニタの最大解像度] 設定は [1920x1200] 以上にする必要があるため、リモート デスクトップは少なくとも 17.63MB のビデオ RAM が必要です。

  3D アプリケーションを使用する場合や、エンド ユーザーが Macbook を Retina Display や Google Chromebook Pixel と併用する場合には、「画面解像度 (P. 33)」 を参照してください。
- [HTML Access] 設定は有効にする必要があります。

構成手順は、「リモート デスクトップとプールの準備 (P. 12)」を参照してください。

View 接続サーバ

View 接続サーバと HTML Access オプションをサーバにインストールする必要があります。

- HTML Access 2.6 には、View 接続サーバ 6.1 または View 接続サーバ 6.0.x が必要です。View 接続サーバ 6.0.x を使用している場合は、サーバで個別の HTML Access インストーラも実行する必要があります。

- HTML Access 2.5 には、View 接続サーバ 6.0.1 が必要です。このバージョンの View 接続サーバでは、HTML Access 2.5 が組み込まれています。
- HTML Access 2.4 には、View 接続サーバ 6.0 が必要です。このバージョンの View 接続サーバでは、HTML Access 2.4 が組み込まれています。

デフォルトでは、HTML Access コンポーネントは View 接続サーバのインストーラですでに選択されています。インストール手順は、『View のインストール』マニュアルに記載されています。

HTML Access コンポーネントをインストールするときに、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自動的に構成するため、Windows ファイアウォールで [VMware Horizon View 接続サーバ (Blast-In)] ルールが有効になります。

セキュリティ サーバ

View セキュリティ サーバ： View 接続サーバと同じバージョンをセキュリティ サーバにインストールする必要があります。

企業のファイアウォールの外部からクライアント システムが接続する場合には、セキュリティ サーバを使用することを推奨します。セキュリティ サーバでは、クライアント システムで VPN 接続が必要にはなりません。

注意　1 つセキュリティ サーバは、最大で 800 個の Web クライアントへの接続を同時にサポートできます。

サードパーティ ファイアウォール

以下のトラフィックを許可するための規則を追加します：

- サーバ（セキュリティ サーバ、View 接続サーバ インスタンス、およびレプリカ サーバを含む）： TCP ポート 8443 へのインバウンド トラフィック。
- リモート デスクトップ仮想マシン： TCP ポート 22443 へのインバウンド トラフィック（サーバから）。

View 用の表示プロトコル

Blast

Web ブラウザを使用してリモート デスクトップにアクセスするときは、PCoIP または Microsoft RDP ではなく Blast プロトコルが使用されます。Blast は HTTPS (HTTP over SSL/TLS) を使用します。

HTML Access のための View 接続サーバおよびセキュリティ サーバの準備

エンド ユーザーが Web ブラウザを使用してリモート デスクトップに接続できるようにするには、管理者が特定のタスクを実行する必要があります。

エンド ユーザーが View 接続サーバまたはセキュリティ サーバに接続してリモート デスクトップにアクセスできるようになるには、HTML Access コンポーネントとともに View 接続サーバをインストールし、セキュリティ サーバをインストールする必要があります。

重要　一部のバージョンの HTML Access では、誤って HTML Access オプションなしで View 接続サーバをインストールし、後で HTML Access コンポーネントが必要になった場合には、View 接続サーバをアンインストールし、HTML Access オプションを選択してインストーラを再実行する必要があります。View 接続サーバをアンインストールするときには、AD LDS Instance VMwareVDMDS インスタンスと呼ばれる View LDAP 構成をアンインストールしないでください。

その他のバージョンの HTML Access の場合は、HTML Access のために別のインストーラを使用します。このため、View 接続サーバを再インストールする必要はありません。

表 1-1. HTML Access の各バージョンのインストーラ要件

HTML Access のバージョン	View 接続サーバのバージョン	インストール要件
2.6	6.1	個別のインストーラなし
2.6	6.0.x	個別の HTML Access インストーラ
2.5	6.0.x	個別のインストーラなし
2.4	6.0	個別のインストーラなし

以下は、HTML Access を使用するために管理者が実行する必要がある作業のチェックリストです。

1 View 接続サーバの複製されたグループを構成するサーバに、HTML Access オプションを使用して View 接続サーバをインストールします。

デフォルトでは、インストーラで HTML Access コンポーネントがすでに選択されています。インストールの説明については、『View インストール ガイド』を参照してください。

注意　HTML Access コンポーネントがインストールされているかどうかを確認するには、Windows オペレーティング システムの [プログラムのアンインストール] アプレットを開き、リストで View HTML Access を探してください。

2 個別の HTML Access インストーラが必要な場合、複製されたグループの View 接続サーバのホストで、View ダウンロード ページから HTML Access インストーラをダウンロードして、インストーラを実行します。

インストーラの名前は、`VMware-Horizon-View-HTML-Access_X64-<y.y.y>-<xxxxxx>.exe` です。<y.y.y> はバージョン番号、<xxxxxx> はビルド番号です。

3 セキュリティ サーバを使用する場合は、View セキュリティ サーバをインストールします。

インストールの説明については、『View インストール ガイド』を参照してください。

重要　View セキュリティ サーバのバージョンは、View 接続サーバのバージョンと一致している必要があります。

4 それぞれの View 接続サーバ インスタンスまたはセキュリティ サーバが、ユーザーが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セキュリティ証明書を持つことを確認します。

詳細については、『View インストール ガイド』を参照してください。

5 RSA SecurID または RADIUS 認証などの 2 要素認証を使用するには、View 接続サーバでこの機能が有効であることを確認してください。

詳細については、『View 管理ガイド』の 2 要素認証についてのトピックを参照してください。

6 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セキュリティ サーバおよび View 接続サーバのホストで 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 TCP ポート 22443 に（View 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、「HTML Access のファイアウォール ルール (P. 11)」を参照してください。

サーバのインストール後に View Administrator を確認すると、該当する View 接続サーバ インスタンスおよびセキュリティ サーバで [Blast Secure Gateway] 設定が有効になっていることがわかります。また、該当する View 接続サーバ インスタンスおよびセキュリティ サーバで Blast Secure Gateway 用に使用するように [Blast 外部 URL] 設定が自動的に構成されています。デフォルトでは、URL に、安全なトンネルの外部 URL の FQDN とデフォルト ポート番号 8443 が含まれています。URL に、この View 接続サーバ ホストまたはセキュリティ サーバ ホストに到達するためにクライアント システムが使用できる FQDN とポート番号が含まれている必要があります。詳細については、『View インストール ガイド』の「View 接続サーバ インスタンスの外部 URL を設定する」を参照してください。

注意 HTML Access を VMware Workspace Portal と一緒に使用すると、ユーザーが HTML5 ブラウザから自分のデスクトップに接続できます。Workspace Portal のインストールおよび View 接続サーバで使用するための構成についての詳細は、Workspace Portal のマニュアルを参照してください。View 接続サーバを SAML 認証サーバとペアにする詳細については、『View 管理ガイド』を参照してください。

HTML Access のファイアウォール ルール

クライアント Web ブラウザが HTML Access を使用してセキュリティ サーバ、View 接続サーバ インスタンス、およびリモート デスクトップに接続できるようにするには、ファイアウォールが特定の TCP ポートのインバウンド トラフィックを許可する必要があります。

HTML Access 接続は 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、View 接続サーバ インスタンスまたはセキュリティ サーバ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自動的に構成するため、Windows ファイアウォールで [VMware Horizon View 接続サーバ (Blast-In)] ルールが有効になります。

表 1-2. HTML Access 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	セキュリティ サーバまたは View 接続サーバ インスタンス	TCP 443	View に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 でセキュリティ サーバまたは View 接続サーバ 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	View への最初の接続後に、クライアント デバイスの Web ブラウザは TCP ポート 8443 上の Blast Secure Gateway に接続します。2 番目の接続を実行できるようにするために、セキュリティ サーバまたは View 接続サーバ インスタンスで Blast Secure Gateway を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 が有効にされ、ユーザーがリモート デスクトップを選択すれば、Blast Secure Gateway はデスクトップの 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、View 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 View デスクトップを選択すると、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、View Agent のインストールに含まれています。

リモート デスクトップとプールの準備

エンド ユーザーがリモート デスクトップにアクセスできるようにするには、まず管理者が特定のプールの設定を構成し、データセンタのリモート デスクトップ仮想マシンに View Agent をインストールする必要があります。

Horizon Client ソフトウェアがクライアント システムにインストールされていない場合は、HTML Access クライアントが代わりになります。

注意　Horizon Client ソフトウェアは、HTML Access クライアントよりも多くの機能と優れたパフォーマンスを提供します。たとえば、HTML Access クライアントではリモート デスクトップで一部のキーの組み合わせが機能しませんが、Horizon Client ではこれらのキーの組み合わせが機能します。

開始する前に

- vSphere インフラストラクチャと View コンポーネントが HTML Access のシステム要件を満たすことを確認してください。

  「HTML Access のシステム要件 (P. 7)」を参照してください。

- HTML Access コンポーネントがホストの View 接続サーバにインストールされていること、および View 接続サーバ インスタンスと任意のセキュリティ サーバの Windows ファイアウォールによって、TCP ポート 8443 でインバウンド トラフィックが許可されることを確認してください。

  「HTML Access のための View 接続サーバおよびセキュリティ サーバの準備 (P. 10)」を参照してください。

- サードパーティのファイアウォールを使用する場合、View Server からデータセンタの View デスクトップの TCP ポート 22443 にインバウンド トラフィックを許可するための規則を設定します。

- デスクトップ ソースとして使用する予定の仮想マシンにサポートされているオペレーティング システムと VMware Tools がインストールされていることを確認します。

  サポートされているオペレーティング システムの一覧については、「HTML Access のシステム要件 (P. 7)」 を参照してください。

- デスクトップ プールの作成とデスクトップへのユーザーの資格付与を行う手順を理解しておいてください。『View でのデスクトップとアプリケーションの設定』のデスクトップ プールの作成についてのトピックを参照してください。

- エンド ユーザーがリモート デスクトップにアクセス可能であることを確認するには、クライアント システムに Horizon Client ソフトウェアがインストールされていることを確認します。ブラウザから接続を試みる前に Horizon Client ソフトウェアを使用して接続試験を行います。

  Horizon Client のインストール手順については、https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html の Horizon Client のマニュアル サイトを参照してください。

- リモート デスクトップにアクセスするために、サポートされているブラウザのいずれかがあることを確認します。「HTML Access のシステム要件 (P. 7)」を参照してください。

手順

1. リンク クローン プール用のソースとして使用する予定の親仮想マシンまたはフル クローン プール用に使用する予定の仮想マシン テンプレートに、View Agent をインストールします。

   View Agent ソフトウェアには、HTML Access コンポーネントが含まれています。

2. リンクされたクローン プールを作成している場合、vSphere Client を使用して親仮想マシンのスナップショットを作成します。

3 View Administrator を使用してこの仮想マシンからプールを作成し、デスクトップ プールの追加ウィザードが完了したら [HTML Access] 設定を有効にします。

HTML Access は仮想マシン デスクトップ プールでサポートされ、HTML Access 2.6 の場合には、RDS ホストにおけるセッションベースのデスクトップ プールでもサポートされます。RDS ホストにおけるリモートの、ホスト型アプリケーションはサポートされません。

4 このプール設定では、[1 台のモニタの最大解像度] 設定が [1,920x1,200] 以上であることを確認します。

5 ユーザーにこのプールに対する資格を付与します。

6 Horizon Client を使用して、このプールからデスクトップにログインします。

この手順では、HTML Access の使用を試みる前に、プールが正常に動作することを確認してください。

7 サポートされるブラウザを開き、View 接続サーバ インスタンスを指定する URL を入力します。

例：

```
https://horizon.mycompany.com
```

URL では必ず **`https`** を使用してください。

8 表示される Web ページで、Horizon Client ソフトウェアの場合と同じように、[VMware Horizon HTML Access] をクリックしてログインします。

9 表示されるデスクトップの選択画面で、デスクトップ アイコンをクリックします。

これで、オペレーティング システムに Horizon Client ソフトウェアがインストールされていない、またはインストールできないクライアント デバイスを使用しているときに、Web ブラウザからリモート デスクトップにアクセスできるようになりました。

次に進む前に

セキュリティの強化のため、リモートデスクトップで Blast エージェントによる証明機関からの SSL 証明書を使用することがセキュリティ ポリシーで必須とされている場合は 「HTML Access Agent を構成して新しい SSL 証明書を使用 (P. 13)」 を参照してください。

HTML Access Agent を構成して新しい SSL 証明書を使用

業界またはセキュリティの規定に準拠するため、HTML Access Agent で生成されるデフォルトの SSL 証明書を Certificate Authority (CA) によって署名される証明書に置き換えることができます。

View 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、デフォルトの証明書を View に接続するために HTML Access を使用するブラウザに示します。

注意　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 View 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。各デスクトップでレジストリ値を設定する必要もあり、これによって HTML Access Agent は新しい証明書を使用することができます。

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、VMware は各デスクトップで一意の証明書を構成することを推奨しています。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。これを行うと、多くのデスクトップが同一の証明書を持つ結果となります。

手順

1 Horizon View デスクトップで証明書のスナップインを MMC に追加する (P. 14)

Windows ローカル コンピュータ証明書ストアに証明書を追加できる前に、HTML Access Agent がインストールされる View 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。

2 HTML Access Agent の証明書を Windows 証明書ストアにインポート (P. 14)

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デスクトップでこの手順を実行します。

3 HTML Access Agent のルート証明書と中間証明書のインポート (P. 15)

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。

4 Windows レジストリで証明書の拇印を設定 (P. 16)

HTML Access Agent に Windows 証明書ストアにインポートされた CA によって署名された証明書を使用することを許可するには、Windows レジストリ キーに証明書の拇印を構成する必要があります。デフォルトの証明書を CA によって署名された証明書に置き換える各デスクトップで、この手順を行う必要があります。

Horizon View デスクトップで証明書のスナップインを MMC に追加する

Windows ローカル コンピュータ証明書ストアに証明書を追加できる前に、HTML Access Agent がインストールされる View 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。

開始する前に

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 View デスクトップで、[Start（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、[File（ファイル）] - [Add/Remove Snap-in（スナップインの追加と削除）] を選択します。

3 [スナップインの追加と削除] ウィンドウで、[Certificates（証明書）] を選択して [Add（追加）] をクリックします。

4 [証明書のスナップイン] ウィンドウで、[Computer account（コンピュータ アカウント）] を選択し、[Next（次へ）] をクリックして [Local computer（ローカル コンピュータ）] を選択し、次に [Finish（完了）] 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。

次に進む前に

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 の証明書を Windows 証明書ストアにインポート (P. 14)」を参照してください。

HTML Access Agent の証明書を Windows 証明書ストアにインポート

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デスクトップでこの手順を実行します。

開始する前に

- View 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。「Horizon View デスクトップで証明書のスナップインを MMC に追加する (P. 14)」を参照してください。

手順

1. View デスクトップの MMC ウィンドウで、[Certificates (Local Computer)証明書 (ローカル コンピュータ)] ノードを展開して [Personal（個人）] フォルダを選択します。
2. Actions（操作） ペインで、[More Actions（その他の操作）] - [All Tasks（すべてのタスク）] - [Import（インポート）] に移動します。
3. [Certificate Import（証明書のインポート）] ウィザードで、[Next（次へ）] をクリックして証明書が保存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、[Open（開く）] をクリックします。

   証明書のファイル タイプを表示するには、[File name（ファイル名）] ドロップダウン メニューからファイル フォーマットを選択できます。
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. [Mark this key as exportable（このキーをエクスポート可能にマーク）] を選択します。
7. [Include all extendable properties（すべての拡張可能なプロパティを含む）] を選択します。
8. [Next（次へ）] をクリックし、[Finish（完了）] をクリックします。

   新しい証明書は、[Certificates (Local Computer)証明書 (ローカル コンピュータ）] - [Personal（個人）] - [Certificates（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 キーが含まれることを確認します。
   a. [Certificates (Local Computer) (ローカル コンピュータ）] - [Personal（個人）] - [Certificates（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. Certificate Information（証明書情報） ダイアログ ボックスの General（一般） タブに以下の文が表示されることを確認します。**この証明書に対応するプライベート キーがあります。**

次に進む前に

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 (P. 15)」を参照してください。

適切なレジストリ キーを証明書の拇印で構成します。「Windows レジストリで証明書の拇印を設定 (P. 16)」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. View デスクトップの MMC ウィンドウで、[Certificates (Local Computer)証明書 (ローカル コンピュータ)] ノードを展開して [Trusted Root Certification Authorities（信頼されたルート証明機関）] - [Certificates（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、証明書チェーンに中間証明書がなければ、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. [Trusted Root Certification Authorities（信頼されたルート証明機関）] - [Certificates（証明書）] フォルダを右クリックし、[All Tasks（すべてのタスク）] - [Import（インポート）] をクリックします。
3. [Certificate Import（証明書のインポート）] ウィザードで、[Next（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、[Open（開く）] をクリックします。

5 [Next（次へ）] をクリックし、[Next（次へ）] をクリックし、そして [Finish（完了）] をクリックします。

6 サーバ証明書が中間 CA によって署名されていた場合、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 [Certificates (Local Computer)証明書 (ローカル コンピュータ）] - [Intermediate Certification Authorities（中間証明機関）] - [Certificates（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。

次に進む前に

適切なレジストリ キーを証明書の拇印で構成します。「Windows レジストリで証明書の拇印を設定 (P. 16)」を参照してください。

Windows レジストリで証明書の拇印を設定

HTML Access Agent に Windows 証明書ストアにインポートされた CA によって署名された証明書を使用することを許可するには、Windows レジストリ キーに証明書の拇印を構成する必要があります。デフォルトの証明書を CA によって署名された証明書に置き換える各デスクトップで、この手順を行う必要があります。

開始する前に

CA によって署名された証明書が Windows 証明書ストアにインポートされることを確認します。「HTML Access Agent の証明書を Windows 証明書ストアにインポート (P. 14)」を参照してください。

手順

1 HTML Access Agent がインストールされる View デスクトップの MMC ウィンドウで、[Certificates (Local Computer)（証明書（ローカル コンピュータ））] - [Personal（個人）] - [Certificates（証明書）] フォルダに移動します。

2 Windows 証明書ストアにインポートした CA によって署名された証明書をダブルクリックします。

3 Certificates（証明書）ダイアログ ボックスで、Details（詳細）タブをクリックしてスクロールダウンし、[Thumbprint（拇印）] アイコンを選択します。

4 選択した拇印をテキスト 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`

注意　拇印をコピーする場合、先行するスペースを含めないでください。先行するスペースを拇印とともにレジストリ キーに不注意にペーストすると（手順 7）、証明書が正しく構成できない場合があります。この問題は、先行するスペースがレジストリ値テキスト ボックスに表示されない場合であっても発生します。

---

5 HTML Access Agent がインストールされたデスクトップで Windows Registry Editor 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` 値を変更し、証明書の拇印をテキスト ボックスにペーストします。

8 VMware Blast サービスを再起動して変更を有効にします。

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

ユーザーが HTML Access からデスクトップに接続すると、HTML Access Agent は、CA によって署名された証明書をユーザーのブラウザに示します。

HTML Access ソフトウェアのアップグレード

最新バージョンの HTML Access をインストールして、最新の更新および機能向上を入手します。

最新バージョンの HTML Access にアップグレードするには、複製されたグループのすべてのインスタンスに最新バージョンの View 接続サーバがインストールされていることを確認する必要があります。

HTML Access の一部のリリースでは、View 接続サーバの対応するメンテナンス リリースがリリースされていないため、個別の HTML Access インストーラが必要です。次の表に、個別のインストーラが必要な HTML Access のバージョンを示します。

表 1-3. HTML Access の各バージョンのインストーラ要件

HTML Access のバージョン	View 接続サーバのバージョン	インストール要件
2.6	6.1	個別のインストーラなし
2.6	6.0.x	個別の HTML Access インストーラ
2.5	6.0.x	個別のインストーラなし
2.4	6.0	個別のインストーラなし

HTML Access のアップグレードを完了するには、該当する親仮想マシンまたはデスクトップ プール用の仮想マシン テンプレートで View Agent インストーラの最新バージョンを実行する必要もあります。View Agent のバージョンは、View 接続サーバのバージョンに対応している必要があります。

重要　現在、View Agent インストーラには、Horizon 6.0 (with View) より前のリリースの Remote Experience Agent に付属していた HTML Access エージェント コンポーネントが含まれています。Remote Experience Agent は、Horizon View Feature Pack の一部でした。Remote Experience Agent でインストールされた機能をアップグレードするには、View Agent インストーラを実行してください。このインストーラを実行すると、Remote Experience Agent が削除され、次にアップグレードが行われます。何らかの理由で Remote Experience Agent を手動で削除する場合は、新バージョンの View Agent のインストーラを実行する前に削除してください。

View 接続サーバから HTML Access をアンインストール

他の Windows ソフトウェアを削除するために使用するのと同じ方法で HTML Access を削除できます。

手順

1　HTML Access がインストールされている View 接続サーバのホストで、Windows [コントロール パネル] の [プログラムの追加と削除] を開きます。

2　[VMware Horizon View HTML Access] を選択して [アンインストール] をクリックします。

3　(オプション) そのホストの Windows ファイアウォールで、TCP ポート 8443 がインバウンド トラフィックを許可しないことを確認します。

次に進む前に

ペアのセキュリティ サーバの Windows ファイアウォールの TCP ポート 8443 に対するインバウンド トラフィックを非許可にします。適用可能な場合は、サードパーティ ファイアウォールで規則を変更して、すべてのペアのセキュリティ サーバおよびこの View 接続サーバのホストで TCP ポート 8443 に対するインバウンド トラフィックを非許可にします。

VMware によって収集されるデータ

所属する企業がカスタマー エクスペリエンス向上プログラムに参加している場合、VMware はクライアントの特定フィールドのデータを収集します。機密情報が含まれるフィールドは、匿名扱いとなります。

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。View 管理者がカスタマー エクスペリエンス向上プログラムへの参加を決めた場合、VMware はお客様のご要望に対する VMware の対応を改善する目的で、現在ご使用の配置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 View 接続サーバに送信され、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。

VMware カスタマー エクスペリエンス向上プログラムに参加するには、View 接続サーバ をインストールする管理者が View 接続サーバ 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 View Administrator でオプションを設定します。

表 1-4. カスタマー エクスペリエンス向上プログラムのために収集されたクライアント データ

説明	フィールド名	このフィールドは匿名になるか	値の例
アプリケーションを開発した企業	**<クライアント–ベンダー>**	いいえ	VMware
製品名	**<クライアント–製品>**	いいえ	VMware Horizon HTML Access
クライアント製品のバージョン	**<クライアント–バージョン>**	いいえ	2.6.0-<build_number>
クライアントのバイナリ アーキテクチャ	**<クライアント–アーキテクチャ>**	いいえ	以下のような値があります。 ■ ブラウザ ■ arm
ブラウザのネイティブ アーキテクチャ	**<ブラウザ–アーキテクチャ>**	いいえ	以下のような値があります。 ■ Win32 ■ Win64 ■ MacIntel ■ iPad
ブラウザ ユーザー エージェント文字列	**<ブラウザ–ユーザー–エージェント>**	いいえ	以下のような値があります。 ■ Mozilla/5.0 (Windows NT 6.1; WOW64) ■ AppleWebKit/703.00 （KHTML、Gecko など） ■ Chrome/3.0.1750 ■ Safari/703.00
ブラウザの内部バージョン文字列	**<ブラウザ–バージョン>**	いいえ	以下のような値があります。 ■ 7.0.3（Safari 用） ■ 29.0（Firefox 用）
ブラウザのコア実装	**<ブラウザ–コア>**	いいえ	以下のような値があります。 ■ Chrome ■ Safari ■ Firefox ■ MSIE（Internet Explorer 用）
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	**<ブラウザ–は–ハンドヘルド>**	いいえ	true

エンド ユーザー用に HTML Access を構成 2

HTML Access の URL を入力する時にエンド ユーザーに表示される Web ページの外観を変更できます。イメージ品質を制御するグループ ポリシ、使用されるポート、および他の項目も設定することができます。

この章では次のトピックについて説明します。

エンド ユーザー用に VMware Horizon Web ポータル ページを構成する

この Web ページを構成して、Horizon Client ダウンロード用のアイコン、または HTML Access 経由でリモート デスクトップに接続するアイコンの表示と非表示を切り替えることができます。このページの他のリンクも構成できます。

デフォルトでは、View Portal ページに、ネイティブ Horizon Client のダウンロードおよびインストールのアイコンと、HTML Access 経由で接続するためのアイコンの両方が表示されます。ただし、社内の Web サーバへのリンクを表示したり、特定のクライアント バージョンをサーバで使用できるようにしたりしたい場合もあるでしょう。異なる URL をポイントするようにページを再構成することができます。

特定のクライアント オペレーティング システム用にインストーラ リンクを作成できます。たとえば、Mac OS X システムからポータル ページを参照すると、ネイティブ Mac OS X インストーラのリンクが表示されます。Windows クライアントの場合は、32 ビット版インストーラのリンクと 64 ビット版インストーラのリンクを個別に作成できます。

重要　View 接続サーバ 5.x 以前のリリースからのアップグレードで HTML Access コンポーネントをインストールしておらず、Horizon Client ダウンロード用の社内サーバを指定するポータル ページを編集してある場合、View 接続サーバ 6.0 以降をインストールすると、これらのカスタマイズが表示されなくなることがあります。Horizon 6 以降では、HTML Access コンポーネントが View 接続サーバのアップグレード時に自動的にインストールされます。

View 5.x 用に別途 HTML Access コンポーネントをインストールした場合、Web ページに行ったカスタマイズはすべて保持されています。HTML Access コンポーネントをインストールしなかった場合、カスタマイズはすべて非表示になります。以前のリリース用のカスタマイズは、使用されなくなった `portal-links.properties` ファイルに入っています。

手順

1 View 接続サーバ ホストで、テキスト エディタを使用して `portal-links-html-access.properties` ファイルを開きます。

このファイルの場所は `<CommonAppDataFolder>\VMware\VDM\portal\portal-links-html-access.properties` です。Windows Server 2008 オペレーティング システムでは、<CommonAppDataFolder> ディレクトリは `C:\ProgramData` です。Windows Explorer で `C:\ProgramData` フォルダを表示するには、[フォルダ オプション] ダイアログ ボックスを使用して非表示のフォルダを表示する必要があります。

注意 `portal-links.properties` ファイル（`portal-links-html-access.properties` ファイルと同じ `<CommonAppDataFolder>\VMware\VDM\portal\` ディレクトリにある）に入っている View 5.x 以前用のカスタマイズです。

2 構成プロパティを編集し、適切に設定します。

デフォルトでは、インストーラ アイコンと HTML Access アイコンの両方が有効で、リンクは VMware Web サイトのクライアント ダウンロード ページを参照します。アイコンを無効にする（Web ページからアイコンを削除する）には、プロパティを `false` に設定します。

オプション	プロパティ設定
HTML Access を無効にする	`enable.webclient=false` このオプションが false に設定されているにもかかわらず `enable.download` オプションが true に設定されていると、ユーザーは Web ページでネイティブの Horizon Client インストーラのダウンロードを求められます。両オプションが false に設定されていると、次のメッセージが表示されます。**「この接続サーバへのアクセスについての説明は、ローカルの管理者にお問い合わせください。」**
Horizon Client のダウンロードを無効にする	`enable.download=false` このオプションが false に設定されているにもかかわらず `enable.webclient` オプションが true に設定されていると、ユーザーに HTML Access のログイン Web ページが表示されます。両オプションが false に設定されていると、次のメッセージが表示されます。**「この接続サーバへのアクセスについての説明は、ローカルの管理者にお問い合わせください。」**
Horizon Client をダウンロードするための Web ページの URL を変更します	`link.download=https://`<url-of-web-server> 独自の Web ページを作成する予定がある場合は、このプロパティを使用します。

オプション	プロパティ設定

特定のインストーラ用のリンクを作成する	以下に示すのは完全 URL の例ですが、インストーラ ファイルが次の手順の説明のように View 接続サーバの `C:\Program Files\VMware\VMware View\Server\broker\webapps\` ディレクトリの `downloads` ディレクトリにある場合は、相対 URL を使用できます。
	■ 32 ビット Windows インストーラ:
	`link.win32=https://<server>/downloads/VMware-Horizon-Client.exe`
	■ 64 ビット Windows インストーラ:
	`link.win64=https://<server>/downloads/VMware-Horizon-Client.exe`
	■ Linux インストーラ:
	`link.linux=https://<server>/downloads/VMware-Horizon-Client.tar.gz`
	■ Mac OS X インストーラ:
	`link.mac=https://<server>/downloads/VMware-Horizon-Client.dmg`
	■ iOS インストーラ:
	`link.ios=https://<server>/downloads/VMware-Horizon-Client-iPhoneOS.zip`
	■ Android インストーラ:
	`link.android=https://<server>/downloads/VMware-Horizon-Client-AndroidOS.apk`

ログイン画面およびデスクトップ セレクタ画面のヘルプ リンクの URL を変更する	`link.help` デフォルトの場合、このリンクは VMware の Web サイトにホストされているヘルプ システムを参照します。ヘルプ リンクは画面の右上隅に表示されます。 HTML Access ログイン画面およびデスクトップ セレクタ画面の場合、ヘルプ リンクは疑問符のアイコンです。

3 (オプション) Horizon Client ツールバーのヘルプ リンクの URL を変更します。

デスクトップにログインすると、ヘルプ リンクはクライアントの右端のドロップダウン メニューにある [ヘルプ] コマンドになります。このリンクの URL を変更するには、該当フォルダ内の該当ファイル内の `HELP_URL_VIEW` プロパティを編集します。

オプション	説明
HTML Access 2.6 の場合	View 接続サーバ ホストでは、このファイルが次の場所にあります。 `<ViewConnectionServer-InstallDir>\webapps\portal\desktop\locale\`
HTML Access 2.4 と 2.5 の場合	リモート デスクトップのオペレーティング システム（View Agent がインストールされている場所）では、このファイルが次の場所にあります。 `C:\Program Files\VMware\VMware Blast\web\locale\`

たとえば英語を使用している場合、`en.json` ファイル内の `HELP_URL_VIEW` プロパティを編集します。

4 ユーザーに VMware Web サイト以外の場所からインストーラをダウンロードさせるには、インストーラ ファイルを置くことになる HTTP サーバにインストーラ ファイルを配置します。

この場所は、前の手順の `portal-links-html-access.properties` ファイルで指定した URL に対応している必要があります。たとえば、View 接続サーバ ホストの `downloads` フォルダにファイルを配置するには、以下のパスを使用します。

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

これで、インストーラ ファイルに対するリンクで `/downloads/<client-installer-file-name>` というフォーマットの相対 URL を使用できます。

5 View Web コンポーネント サービスを再起動します。

RDS ホストからのデスクトップの有効化

HTML Access 2.6 を使用すると、管理者は Microsoft RDS （リモート デスクトップ セッション）ホストがセッション ベースのデスクトップを提供できるように View 接続サーバを構成することができます。

開始する前に

お使いのバージョンの Windows オペレーティング システムでの ADSI Edit ユーティリティの使用方法については、Microsoft TechNet Web サイトを参照してください。Windows Server 2012 RDS ホストを使用している場合、[ロールと機能を追加] で、Remote Server Administration Tools (RSAT) から AD DS と LDS ツールをインストールする必要がある場合があります。

手順

1 View 接続サーバ ホスト上で ADSI Edit ユーティリティを起動します。

2 [接続設定] ダイアログ ボックスで、[DC=vdi,DC=vmware,DC=int] を選択するか接続します。

3 [コンピュータ] ペインで、**`localhost:389`** を選択または入力するか、View 接続サーバ ホストの完全修飾ドメイン名 (FQDN) を入力し、続いてポート 389 を入力します。

例：**`localhost:389`** または **`mycomputer.mydomain.com:389`**

4 プールがすでに作成されている場合、オブジェクト [OU=Applications] の下でプールの名前を検索し、[pae-ServerProtocolLevel] 属性に [BLAST] を追加します。

5 オブジェクト [OU=Server Groups] の下でファームの名前を検索し、[pae-ServerProtocolLevel] 属性に [BLAST] を追加します。

ファーム アイテムが HTML Access Web Client に表示されます。

URI を使用した構成 HTML Access Web Client

Uniform Resource Identifier (URI) を使用して作成できるリンク付きの Web ページや電子メールでは、エンド ユーザーがクリックすると HTML Access Web client が起動したり、View 接続サーバに接続したり、特定の構成オプションを持つ特定のデスクトップを起動したりできます。

エンド ユーザー用の Web または電子メールのリンクを作成することで、リモート デスクトップへの接続プロセスを簡素化できます。部分的または以下のすべての情報を提供する URI を作成することでこれらのリンクを作成すれば、エンド ユーザーは入力する必要がありません。

- View 接続サーバ のアドレス
- View 接続サーバ のポート番号
- Active Directory ユーザー名
- Active Directory ユーザー名と異なる場合、RADIUS または RSA SecurID ユーザー名
- ドメイン名
- デスクトップ表示名
- セッションの参照、リセット、ログオフ、開始を含むアクション

HTML Access の URI を作成するための構文

構文には、サーバを指定するためのパス部分、および必要に応じてユーザー、デスクトップ、デスクトップのアクションまたは構成オプションを指定するためのクエリが含まれます。

URI 仕様

以下の構文を使用して HTML Access Web Client を起動するための URI を作成します。

```
https://[<varname id="VARNAME_E0F8F9951BC4471D9871655A18782C9E">authority-part</varname>][?<varname id="VARNAME_217F9AF17A3745369FD8E2154505D735">query-part</varname>]
```

重要　URI を含む HTML のハイパーリンクやボタンをコーディングする場合、リンクに `target='_Blank'` は使用しないでください。このコードは新しいブラウザ ウィンドウを開くために使用されますが、Internet Explorer 9、10、11 では問題が発生します。`href` でこのコードを使用した場合、ユーザーが [切断] メニュー項目を選択すると、デスクトップが切断された直後にクライアントが再接続を試みます。さらに、ユーザー名とドメイン名も設定されません。

<authority-part>

サーバ アドレス、および必要に応じて非デフォルト ポート番号を指定します。サーバ名は、DNS 構文に一致する必要があります。

ポート番号を指定するには、以下の構文を使用します:

```
<varname id="VARNAME_1BAB6153D2834B1490509093A1961D1F">server-address</varname>:<varname id="VARNAME_2296A4E54893485C852FFE94067114D7">port-number</varname>
```

<query-part>

使用するための設定オプション、または実行するデスクトップ アクションを指定します。クエリは大文字と小文字の区別がありません。複数のクエリを使用するには、クエリの間にアンパサンド (&) を使用します。クエリが違いに競合する場合、リストの最後のクエリが使用されます。次の構文を使用します:

```
<varname id="VARNAME_48A6B3A0E1184943BC1206017B78B9D5">query1</varname>=<varname id="VARNAME_9B9916FF3D3540D4AA5622F9C828F072">value1</varname>[&<varname id="VARNAME_6BCA2912EC454A5683D586754BF89DCE">query2</varname>=<varname id="VARNAME_F698C39E83D34D639C943ACDF828BAFE">value2</varname>...]
```

query-part を作成するときは、以下のガイドラインに注意してください。

- サポートされているクエリを 1 つも使用しない場合は、デフォルトの VMware Horizon Web ポータル ページが表示されます。
- クエリ部分では、一部の特殊文字がサポートされていません。それらの文字には URL エンコーディング形式を使用する必要があります。番号記号 (#) には **%23**、パーセント記号 (%) には **%25**、アンパサンド (&) には **%26**、アット マーク (@) には **%40**、バックスラッシュ (\) には **%5C** を使用します。

  URL エンコーディングの詳細については、http://www.w3schools.com/tags/ref_urlencode.asp を参照してください。

- クエリ部分で、非 ASCII 文字は UTF-8 [STD63] に基づいて最初にエンコードされる必要があり、次に対応する UTF-8 シーケンスの各オクテットは、URI 文字として表されるパーセントでエンコードされる必要があります。

  ASCII 文字のエンコードについての詳細は、http://www.utf8-chartable.de/ の URL エンコーディング資料を参照してください。

サポートされるクエリ

このトピックでは、HTML Access Web client でサポートされるクエリを示します。デスクトップ クライアントやモバイル クライアントなどの複数のクライアント タイプ用に URI を作成する場合は、クライアント システムの各タイプの『VMware Horizon Client の使用』を参照してください。

domainName リモート デスクトップに接続しているユーザーに関連付けられているドメイン。

userName リモート デスクトップに接続している Active Directory ユーザー。

tokenUserName RSA または RADIUS ユーザー名。RSA または RADIUS ユーザー名が Active Directory ユーザー名と異なる場合に限ってこのクエリを使用します。このクエリを指定せず、RSA または RADIUS 認証が必要である場合、Windows ユーザー名が使用されます。

desktopId デスクトップ表示名。この名前は、デスクトップ プールの作成時に View Administrator で指定した名前です。表示名にスペースが含まれている場合、ブラウザは **%20** を自動的に使用してスペースを表します。

操作

表 2-1. アクション クエリで使用できる値

値	説明
参照	指定したサーバにホストされている使用可能なデスクトップのリストを表示します。このアクションを使用している場合、デスクトップを指定する必要はありません。
スタート セッション	指定したデスクトップを起動します。アクション クエリが提供されず、デスクトップ名が提供されなければ、**スタート セッション**がデフォルト アクションとなります。
リセット	指定したデスクトップをシャットダウンして再起動します。保存されてないデータは失われます。リモート デスクトップのリセットは、物理 PC のリセット ボタンを押すことに相当します。
ログオフ	リモート デスクトップのゲスト OS からユーザーをログオフします。

URI の例

URI でハイパーテキスト リンクまたはボタンを作成し、これらのリンクを電子メールまたは Web ページに含めることができます。エンド ユーザーはこれらのリンクをクリックして、たとえば、指定した起動オプションで特定のリモート デスクトップを起動できます。

URI 構文の例

各 URI の例に続いて、URI リンクをクリック後にエンド ユーザーに表示される事柄について説明します。クエリでは、大文字と小文字が区別されません。たとえば、**domainName** または **domainname** を使用できます。

1 `https://view.mycompany.com?domainName=finance&userName=fred`

  HTML Access Web Client が起動され、`view.mycompany.com` サーバに接続します。ログイン ボックスで、[ユーザー名] テキスト ボックスに [fred] という名前が入力され、[ドメイン] テキスト ボックスに [finance] が入力されます。ユーザーはパスワードを入力する必要があるだけです。

2 `https://view.mycompany.com?desktopId=Primary%20Desktop&action=start-session`

HTML Access Web Client が起動され、**view.mycompany.com** サーバに接続します。ログイン ボックスが表示され、ユーザー名、ドメイン名、およびパスワードが求められます。ログインに成功すると、クライアントはディスプレイ名が [Primary Desktop（プライマリ デスクトップ）] として表示されるデスクトップに接続し、ユーザーはゲスト OS にログインされます。

3 **https://view.mycompany.com:7555?desktopId=Primary%20Desktop**

この URI は前の例と同じ効果がありますが、View 接続サーバに 7555 の非デフォルト ポートを使用するところが異なります（デフォルトのポートは 443 です）。デスクトップ ID が提供されるので、デスクトップは **start-session** アクションが URI に含まれていない場合であっても起動されます。

4 **https://view.mycompany.com?desktopId=Primary%20Desktop&action=reset**

HTML Access Web Client が起動され、**view.mycompany.com** サーバに接続します。ログイン ボックスが表示され、ユーザー名、ドメイン名、およびパスワード求められます。ログインに成功すると、クライアントによって、プライマリ デスクトップのリセット操作の確認を求めるダイアログ ボックスが表示されます。

注意　このアクションは、View 管理者がエンド ユーザーにマシンのリセットを許可している場合にのみ使用できます。

HTML コードの例

URI を使用してハイパー リンクおよびボタンを作成し、電子メールまたは Web ページに含めることができます。以下の例は、[Test Link（テスト リンク）] と言うハイパー リンクおよび [TestButton] と言うボタンのコードを記述するために最初の URI の例から URI を使用する方法を示します。

```
<html>
<body>

<a href="https://view.mycompany.com?domainName=finance&userName=fred">Test
Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'https://view.mycompany.com?domainName=finance&userName=fred'"></form> <br>

</body>
</html>
```

注意　次のコードのように、リンクに **target='_Blank'** は使用しないでください。

```
<a href="https://view.mycompany.com?desktopId=Primary%20Desktop&action=start-session"
target="_Blank">Test Link</a>
```

target='_Blank' は新しいブラウザ ウィンドウを開くために使用されますが、Internet Explorer 9、10、11 では問題が発生します。**href** でこのコードを使用した場合、ユーザーが [切断] メニュー項目を選択すると、デスクトップが切断された直後にクライアントが再接続を試みます。さらに、ユーザー名とドメイン名も設定されません。

HTML Access グループ ポリシー設定の構成

リモート デスクトップでの HTML Access の動作を制御するグループ ポリシー設定を構成できます。これらの設定を適用するには、HTML Access ADM テンプレート ファイルを Active Directory のグループ ポリシー オブジェクト (GPO) に追加します。

開始する前に

- View Agent 6.0 以降がリモート デスクトップにインストールされていることを確認します。View Agent 6.0 以降には、HTML Access コンポーネントが含まれています。以前のリリースでは、HTML Access コンポーネントを入手するために、Remote Experience Agent をインストールする必要がありました。

- HTML Access グループ ポリシー設定用に Active Directory GPO が作成されていることを確認します。GPO は、リモート デスクトップを含む OU にリンクする必要があります。Active Directory で View グループ ポリシー設定を行う一般情報については、『View 管理ガイド』の「ポリシーの構成」を参照してください。
- Active Directory サーバで、Microsoft MMC およびグループ ポリシー オブジェクト エディタ スナップインが使用できることを確認します。
- HTML Access グループ ポリシー設定について理解しておきます。「HTML Access グループ ポリシー設定 (P. 27)」を参照してください。

手順

1 VMware Horizon 6 のダウンロード サイト http://www.vmware.com/go/downloadview から View GPO Bundle `.zip` ファイルをダウンロードします。

ファイル名は `VMware-Horizon-View-Extras-Bundle-<x.x.x>-<yyyyyyy>.zip` で、<x.x.x> はバージョン、<yyyyyyy> はビルド番号を表します。View のグループ ポリシー設定用の ADM ファイルと ADMX ファイルはすべて、このファイルで提供されています。

2 ファイルを Active Directory サーバにコピーして解凍します。

HTML Access GPO は、`Blast-enUS.adm` ADM テンプレート ファイルに含まれています。

3 Active Directory サーバで GPO を編集します。

オプション	説明
Windows 2008 または 2012	a [スタート] - [管理ツール] - [グループ ポリシー管理] を選択します。 b ドメインを展開し、グループ ポリシ設定を作成した GPO を右クリックして、[[編集]] を選択します。
Windows 2003	a [スタート] - [すべてのプログラム] - [管理ツール] - [Active Directory ユーザーおよびコンピュータ] を選択します。 b リモート デスクトップを含む OU を右クリックし、[プロパティ] を選択します。 c [グループ ポリシ] タブで、[開く] をクリックして Group Policy Management プラグインを開きます。 d 右ペインで、グループ ポリシー設定に作成した GPO を右クリックし、[Edit（編集）] を選択します。

[Group Policy Object Editor（グループ ポリシー オブジェクト エディタ）] ウィンドウが表示されます。

4 グループ ポリシー オブジェクト エディタで、[Computer Configuration（コンピュータの構成）]の下の [Administrative Templates（管理用テンプレート）]を右クリックし、[Add/Remove Templates（テンプレートの追加と削除）]を選択します。

5 [[追加]] をクリックして `Blast-enUS.adm` ファイルを参照し、[[開く]] をクリックします。

6 [Close（閉じる）]をクリックして、ADM テンプレート ファイルのポリシー設定を GPO に適用します。

[VMware Blast] フォルダは、[[管理テンプレート]] - [[従来の管理用テンプレート]] の下の左側のペインに表示されます。

7 HTML Access グループ ポリシー設定を構成します。

8 ポリシー設定がリモート デスクトップに適用されていることを確認します。

a デスクトップで `gpupdate.exe` コマンドを実行します。

b デスクトップを再起動します。

HTML Access グループ ポリシー設定

HTML Access ADM テンプレート ファイル **Blast-enUS.adm** には、リモート デスクトップに適用できるグループ ポリシー設定が含まれます。テンプレート ファイルが Active Directory にインポートされると、HTML Access グループ ポリシー設定がグループ ポリシー エディタの **VMware Blast** フォルダに格納されます。

表 2-2. HTML Access グループ ポリシー設定

設定	説明
空の画面	リモート仮想マシンが、HTML Access セッション中に View の外から見ることができるかどうかを制御します。たとえば、管理者は vSphere Web Client を使用して、ユーザーが HTML Access を介してデスクトップに接続されている間に仮想マシンでコンソールを開く場合があります。 この設定が有効にされるか構成されない場合で、HTML Access セッションがアクティブである間に誰かが View の外からリモート仮想マシンにアクセスを試みる場合、リモート仮想マシンは空の画面を表示します。 この設定を無効にすると、前述のような状況のリモート仮想マシンでは、リモートでアクセスする第 2 のユーザーに対してアクティブな View デスクトップ セッションが表示されます。
セッションのガーベッジ コレクション	破棄されたリモート セッションのガーベッジ コレクションを制御します。この設定を有効にすると、ガーベッジ コレクションの間隔としきい値を構成できます。 間隔は、ガーベッジ コレクタが実行される頻度を制御します。間隔は、ミリ秒単位で設定します。 しきい値は、セッションが破棄された後でそれが削除候補となる前までに必要となる経過時間を決定します。しきい値は、秒単位で設定します。
オーディオ再生	リモート デスクトップでオーディオ再生を許可するかどうかを制御します。デフォルトの場合、この設定は有効です。
イメージ品質	リモート ディスプレイのイメージ品質を制御します。低画質、中画質、および高画質の 3 種類のイメージ品質プロファイルがあります。利用可能な帯域幅、最近使用したフレームレート、現在のフレームで最近変更された部分のサイズの制限の範囲で、エンコーダは可能な限り最高品質レベルを使用しようとします。エンコーダは、クライアント画面のどの部分が低画質または中画質であるのかを追跡し、それらの領域を画像を少しずつ上げて高画質に近づけます。 この設定を有効にすると、低品質、中画質、および高品質の JPEG 設定を異なる値に個別に変更できます。実際の低画質、中画質、および高画質の設定で使用される JPEG 画質レベルは、0 ～ 100 の範囲の数値として個々に構成できます。 彩度のサブサンプリングは、選択された JPEG 品質レベルに対応して有効になります。JPEG 品質が 80 以上に設定されると、彩度のサンプリングがオフになり、比率は使用可能な最高値 YUV-4:4:4 に設定されます。JPEG 品質が 79 以下に設定されると、比率は YUV-4:2:0 に設定されます。 ■ [低品質 JPEG]。デフォルトでは、この値は 25 です。低い JPEG 彩度のサブサンプリングを様々な比率に設定することもできます。デフォルトでは、低い比率は使用可能な最低値 4:1:0 に設定されています。 ■ [中品質 JPEG]。デフォルトの場合、この値は 35 です。低い JPEG 彩度のサブサンプリングを様々な比率に設定することもできます。デフォルトの場合、低い比率は使用可能な最低値 4:2:0 に設定されています。 ■ [高品質 JPEG]。デフォルトでは、この値は 90 です。高い JPEG 彩度のサブサンプリングを様々な比率に設定することもできます。デフォルトでは、高い比率は使用可能な最高値 4:4:4 に設定されています。

表 2-2. HTML Access グループ ポリシー設定 (続き)

設定	説明
クリップボード リダイレクトの構成	クリップボード リダイレクトを許可する方向を決定します。テキストのみをコピーおよび貼り付けできます。次のいずれかの値を選択できます。 ■ [クライアントからサーバの方向のみ有効] (すなわち、クライアント システムからリモート デスクトップにのみ、コピーおよび貼り付けを許可します。) ■ [どちらの方向も無効] ■ [どちらの方向も有効] ■ [サーバからクライアントの方向のみ有効] (すなわち、リモート デスクトップからクライアント システムにのみ、コピーおよび貼り付けを許可します。) この設定は View Agent にのみ適用されます。 シングルユーザー リモート デスクトップの場合、この設定が無効または構成されていない場合、デフォルト値は [クライアントからサーバの方向のみ有効] です。RDS ホスト上のセッションベースのリモート デスクトップ (HTML Access 2.6 で使用可能) の場合、この設定が無効または構成されていない場合、デフォルト値は [どちらの方向も無効] です。
HTTP サービス	Blast Agent サービス用のセキュアな (HTTPS) TCP ポートに変更可能です。デフォルトのポートは 22443 です。 この設定を有効にしてポート番号を変更します。この設定を変更する場合は、影響を受けるリモート デスクトップ (View Agent のインストール先) のファイアウォールの設定も更新する必要があります。

リモート デスクトップの使用 3

クライアントには、ドロップダウン ツールバーとメニューが用意されているので、リモート デスクトップから簡単に切断したり、Ctrl+Alt+Delete キーの組み合わせに相当するメニュー コマンドを使用したりすることができます。

この章では次のトピックについて説明します。

機能サポート一覧

ブラウザベースの HTML Access クライアントからリモート デスクトップにアクセスする場合、一部の機能は使用できません。

表 3-1. HTML Access を通してサポートされる機能

機能	Windows 8.x リモート デスクトップ	Windows 7 リモート デスクトップ	Windows XP リモート デスクトップ	Windows Vista リモート デスクトップ	Windows Server 2008 R2 デスクトップ
RSA SecurID または RADIUS	X	X	X	X	X
シングル サインオン	X	X	X	X	X
RDP 表示プロトコル					
PCoIP 表示プロトコル					
Blast プロトコル	X	X	X	X	X
USB アクセス					
リアルタイム オーディオ ビデオ (RTAV)					

表 3-1. HTML Access を通してサポートされる機能 (続き)

機能	Windows 8.x リモート デスクトップ	Windows 7 リモート デスクトップ	Windows XP リモート デスクトップ	Windows Vista リモート デスクトップ	Windows Server 2008 R2 デスクトップ
Wyse MMR					
Windows 7 MMR					
仮想印刷					
ロケーション ベースの印刷					
スマート カード					
複数のモニタ					

上記の機能の詳細および制限事項については、『View アーキテクチャ プランニング ガイド』を参照してください。

RDS ホストでのセッションベースのデスクトップの機能サポート

RDS ホストは、Windows リモート デスクトップ サービスと View 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。

HTML Access 2.6 があれば、Microsoft RDS （リモート デスクトップ セッション）ホスト上のリモート セッションベースのデスクトップにアクセスすることもできます。次の表は、HTML Access を使用した場合に RDS ホストから使用可能な機能を示しています。Horizon Client for Windows など、ネイティブでインストールされた Horizon Client を使用している場合は、追加の機能が使用できます。

表 3-2. View Agent 6.0.2 がインストールされた RDS ホストでサポートされている機能

機能	物理マシン上の Windows Server 2008 R2 RDS ホスト	仮想マシン上の Windows Server 2008 R2 RDS ホスト	物理マシン上の Windows Server 2012 RDS ホスト	仮想マシン上の Windows Server 2012 RDS ホスト
RSA SecurID または RADIUS	X	X	X	X
シングル サインオン	X	X	X	X
Blast プロトコル	X	X	X	X
仮想印刷				
ロケーション ベースの印刷				
複数のモニタ				

各ゲスト OS のどのエディションがサポートされるか、またはどのサービス パックがサポートされるかについての詳細は、『View 6.x インストール ガイド』の「View Agent でサポートされているオペレーティング システム」のトピックを参照してください。

国際化

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、および韓国語で利用可能です。

クライアント システム、ブラウザ、およびリモート デスクトップで使用する必要がある言語パックについての詳細は、「国際キーボード (P. 33)」を参照してください。

リモート デスクトップに接続する

使用を許可されているリモート デスクトップに接続するには、Active Directory の認証情報を使用します。

開始する前に

- Active Directory 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 認証ユーザー名とパスコードなどのログインに必要な認証情報を取得します。
- ログイン用のドメイン名を取得します。

手順

1. RSA SecurID の認証情報または RADIUS の認証証明書の入力を求められた場合は、ユーザー名とパスコードを入力して [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。
2. 再度、RSA SecurID 認証情報または RADIUS 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 および、過去に生成され、入力したものと同じ番号は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 サーバの構成設定が変更された時にのみ、必要になります。
3. [ログイン] ダイアログ ボックスで Active Directory のユーザー名、パスワード、およびドメイン名を入力し、[サイン イン] をクリックします。
4. 複数のリモート デスクトップを使用する資格が付与されている場合は、アクセスするリモート デスクトップのアイコンをクリックします。

   リモート デスクトップがブラウザに表示されます。

次に進む前に

Safari ブラウザを使用してデスクトップに接続するとすぐに切断され、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れます。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 (P. 31)」を参照してください。

自己署名付ルート証明書の信頼

Safari ブラウザを使用している場合、リモート デスクトップに接続した直後に切断され、[デスクトップの切断] ダイアログ ボックスが表示されることがあります。この場合は、ブラウザを使用して自己署名セキュリティ証明書を承認し、リモート デスクトップに再接続することができます。

この問題は、Blast Secure Gateway が使用されていない場合に発生する可能性があります。

手順

1. [デスクトップの切断] ダイアログ ボックスの [ここをクリックしてセキュリティ証明書を承認] リンクをクリックします。
2. 次に表示されるプロンプトで [証明書の表示] ボタンをクリックします。
3. 表示される [Blast] ペインで、[信頼] ドロップダウン リストをクリックして展開します。
4. [この証明書を使用する場合] ドロップダウン リストで [常に信頼する] を選択し、[続行] をクリックします。
5. 入力を求められたらパスワードを入力し、[設定の更新] をクリックします。
6. [デスクトップ選択] ウィンドウで、リモート デスクトップをクリックします。

リモート デスクトップに再接続され、ログインします。

製品の制限

HTML Access で提供される Web client には、音声の再生とキーボードについて製品の制限があります。

- Windows XP および Windows Vista リモート デスクトップでは、オーディオ再生がサポートされていません。
- HTML Access 2.6 では Internet Explorer 9 はサポートされません。HTML Access 2.4 と 2.5 の場合、Internet Explorer 9 がサポートされますが、このバージョンのブラウザは HTML Access で提供される HTML5 機能の多くをサポートしません。(HTML Access 2.4 または 2.5 でも) Internet Explorer 9 でサポートされない機能としては、オーディオ再生、クリップボード リダイレクト、マウス カーソルの変更、フル画面モードなどがあります。
- Internet Explorer ブラウザ、または iPad や Android のタブレットなどのハンドヘルド デバイスを使用する場合、マウス ポインタの種類がポインタの場所によって動的に変化しません。

  使用できないものには、ビジー時、ドラッグ時、リサイズ時のカーソルがあります。たとえば、Internet Explorer ブラウザやモバイル デバイスのブラウザでリモート デスクトップの Web ページのリンクにマウス ポインタを重ねても、マウス ポインタはハンド アイコンに変化しません。ウィンドウの端にマウス ポインタを移動しても、ポインタはサイズ変更矢印に変化しません。テキストを編集する場合、ポインタはカーソルに変化しません。動作は実行できますが、ポインタはそのままの状態です。
- 一部の修飾キー、特殊キー、およびキーの組み合わせは、リモート デスクトップで機能しません。これらの詳細、および国際キーボードの使用については、「キーボードの制限 (P. 32)」 および 「国際キーボード (P. 33)」 を参照してください。

キーボードの制限

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 デスクトップに送信できません。

Web ブラウザによって、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。システムで動作するキーの組み合わせは、ブラウザ ソフトウェア、クライアント オペレーティング システム、および言語設定によって異なります。

以下のキーおよびキーの組み合わせは動作しない場合があります：

- Ctrl+T
- Ctrl+W
- Ctrl+N
- Windows キー
- コマンド キー
- Alt+Enter
- Ctrl+Alt+<any_key>
- Caps Lock+<modifier_key> (Alt または Shift など)
- ファンクション キー (Chromebook を使用する場合)

重要　<Ctrl> + <Alt> + <Del> を入力するには、クライアント メニュー バーの右端にあるドロップ ダウン メニューから [Ctrl+Alt+Del の送信] を選択します。

国際キーボード

英語以外のキーボードとロケールを使用している場合、クライアント システム、ブラウザおよびリモート デスクトップで特定の設定を使用する必要があります。一部の言語では、リモート デスクトップで IME (Input Method Editor) を使用する必要があります。

ローカル設定および入力方法を正しくインストールすれば、以下の言語で文字を入力できます：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、および韓国語。

表 3-3. 必要な入力言語設定

言語	ローカル クライアント システムの入力言語	ローカル クライアント システムで IME が必要かどうか	リモート デスクトップのブラウザと入力言語	リモート デスクトップで IME は必要か
英語	英語	いいえ	英語	いいえ
フランス語	フランス語	いいえ	フランス語	いいえ
ドイツ語	ドイツ語	いいえ	ドイツ語	いいえ
簡体中国語	簡体中国語	英語入力モード	簡体中国語	はい
繁体中国語	繁体中国語	英語入力モード	繁体中国語	はい
日本語	日本語	英語入力モード	日本語	はい
韓国語	韓国語	英語入力モード	韓国語	はい

画面解像度

リモート デスクトップが適切な容量のビデオ RAM で構成されていれば、クライアントでリモート デスクトップのサイズをクライアント ウィンドウのサイズに合わせて変更できます。ビデオ RAM のデフォルト設定は 36 MB で、3D アプリケーションを使用しなければ、最小要件の 16 MB よりも快適な環境となります。

重要　3D レンダリング機能を使用するには、Windows 7 以降の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。

- vSphere 5.0 以降で利用できる、ソフトウェア アクセラレータによるグラフィック機能によって、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) によって、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 96 MB です。

3D レンダリングが有効である場合、モニタの最大数は 1 で最大解像度は 1920 x 1200 です。Blast 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 の計算に似ています。ガイドラインについては、『View アーキテクチャ プランニング』のトピック「仮想デスクトップのメモリ要件の計算」の「PCoIP を使用する場合の特定のモニタ構成の RAM サイジング」を参照してください。

Retina ディスプレイの Macbook や Google Chromebook Pixel など、ピクセル密度解像度が高いブラウザや Chrome 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 デスクトップを設定できます。クライアント メニュー バーの右端にあるドロップダウン メニューから、[高解像度モードに切り替え] コマンドを選択します。このメニュー バーを表示するには、ウィンドウの上中央にあるタブの下矢印をクリックします。

HTML Access では、ドロップダウン メニューから [フル画面表示に切り替え] コマンドも選択できます。

重要　フル画面モードで高解像度モードを使用するには、Windows 7 以降の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。Blast 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 の計算に似ています。ガイドラインについては、『View アーキテクチャ プランニング』のトピック「仮想デスクトップのメモリ要件の計算」の「PCoIP を使用する場合の特定のモニタ構成の RAM サイジング」を参照してください。

音声

WebSocket をサポートする Chrome デバイスまたはブラウザを使用する場合、リモート デスクトップで音声を再生できますが、いくつか制限があります。

デフォルトでは、リモート デスクトップでの音声の再生が有効になっていますが、View 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。

以下のガイドラインを考慮してください。

- オーディオ再生は Windows XP および Windows Vista リモート デスクトップではサポートされていません。
- 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 (I/O) を実行中であったりすると、音質が低下することがあります。使用するブラウザを変えると改善されることがあります。

テキストのコピーおよび貼り付け

View 管理者は、クライアント システムからリモートデスクトップに対してのみ、またはリモート デスクトップからクライアント システムに対してのみ、あるいは双方向でのコピーおよび貼り付けの操作を許可するように、この機能を設定できます。制限事項がいくつかあります。

この機能は、WebSocket をサポートする Chrome デバイスやブラウザを使用する場合に利用できます。

管理者は、View Agent をリモート デスクトップに関連付けるグループ ポリシー オブジェクト (GPO) を使用して、コピーおよび貼り付けの機能を構成できます。詳細については、「HTML Access グループ ポリシー設定 (P. 27)」を参照してください。

Horizon Client からリモート デスクトップ、またはその逆方向に、任意の非 ASCII 文字を含むプレーン テキストまたはフォーマットされたテキストをコピーできますが、貼り付けされたテキストはプレーン テキストになります。最大 5,000 文字をコピーおよび貼り付けできます。

画像をコピーおよび貼り付けできません。リモート デスクトップとクライアント コンピュータのファイル システム間では、ファイルもコピーおよび貼り付けできません。

コピーおよび貼り付け機能を使用する

テキストをコピーおよび貼り付けするには、クライアント メニュー バーの右端にあるドロップダウン メニューから、[テキストの貼り付け] と [コピーしたテキストの取得] コマンドを使用する必要があります。

開始する前に

- View 管理者は、ユーザーにクライアント システムからリモート仮想デスクトップへのコピーおよび貼り付けを許可するというデフォルトのポリシーを有効なままにするか、コピーおよび貼り付けを許可するそれ以外のポリシーを構成する必要があります。詳細については、「HTML Access グループ ポリシー設定 (P. 27)」を参照してください。
- WebSocket をサポートする Chrome デバイスやブラウザを使用する必要があります。このテクノロジーをサポートしていないブラウザには、[テキストの貼り付け] と [コピーしたテキストの取得] というメニュー コマンドが表示されません。

手順

- クライアント システムからリモート デスクトップにテキストをコピーするには、以下の手順を実行します。
  a クライアント システムでテキストをコピーします。
  b リモート デスクトップの内側で、ウィンドウの上中央にあるタブの下矢印をクリックして、メニュー バーを表示します。

c クライアント メニュー バーの右端にあるドロップダウン メニューから、[テキストの貼り付け] を選択します。

d 表示されるダイアログ ボックスにテキストを貼り付けます。

e マウス カーソルをテキストを貼り付けるアプリケーションに位置付けます。

f [貼り付け] ダイアログ ボックスの [貼り付け] をクリックしてから、ダイアログ ボックスを閉じます。

テキストがアプリケーションに貼り付けされます。

- リモート デスクトップからクライアント システムにテキストをコピーするには、以下の手順を実行します。

a リモート デスクトップでテキストをコピーします。

b リモート デスクトップの内側で、ウィンドウの上中央にあるタブの下矢印をクリックして、メニュー バーを表示します。

c クライアント メニュー バーの右端にあるドロップダウン メニューから、[コピーしたテキストの取得] を選択します。

ドロップダウン メニューに [コピーしたテキストの取得] コマンドが表示されない場合は、お使いのブラウザが WebSocket をサポートしていないか、またはこのプロシージャの前提条件に記載したように、View 管理者がリモート デスクトップからクライアント システムへのテキストのコピーを許可するようにセットアップを構成していないことを意味します。

d [コピーしたテキストの取得] ダイアログ ボックスで、テキストを再度選択してコピーします。

これで、テキストがクリップボードにコピーされました。

e クライアント システムで、通常の方法でテキストを貼り付けます。

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、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、リモート 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。

リモート デスクトップを開いていなくても、リモート デスクトップ オペレーティング システムからログオフできます。この機能を使用すると、デスクトップに Ctrl+Alt+Del を送信してから [ログオフ] をクリックするのと同じ結果になります。

注意 Windows のキーの組み合わせ Ctrl+Alt+Del は、リモート デスクトップではサポートされていません。Ctrl+Alt+Del の代わりに、クライアント メニュー バーの右端にあるドロップ ダウン メニューから [Ctrl+Alt+Del の送信] を選択することもできます。メニュー バーを表示するには、ウィンドウの上中央にあるタブの下矢印をクリックします。

手順

- View Server からログアウトし、デスクトップから（ログアウトせずに）切断します。

オプション	アクション
デスクトップのオペレーティング システムで	クライアント メニュー バーの右端にあるドロップダウン メニューから [切断] を選択し、画面の右上隅にある [ログアウト] ボタンをクリックします。
デスクトップ選択画面から	画面の右上隅にある [ログアウト] ボタンをクリックします。

- デスクトップ オペレーティング システム内の [スタート] メニューで [ログオフ] を選択して、デスクトップからログオフし、切断します。

- ログアウトせずに切断します。

オプション	アクション
クライアントも終了する	ブラウザ タブを閉じます。
同じサーバの異なるリモート デスクトップを選択する	クライアント メニュー バーの右端にあるドロップ ダウン メニューから [切断] を選択し、別のリモート デスクトップを選択します。
異なるサーバのリモート デスクトップを選択する	ドロップ ダウン メニューから[切断]を選択し、ブラウザに他のサーバの URL を入力します。

注意　View 管理者は、切断されたときに自動的にログアウトするようにデスクトップを構成できます。その場合、デスクトップで開いているプログラムは停止します。

- リモート デスクトップを開いていなくても、デスクトップ オペレーティング システムからログオフできます。

  この手順を使用すると、リモート デスクトップで開いているファイルが保存されずに閉じられます。

  a　デスクトップ選択画面で、デスクトップ アイコンの [ログオフ] ボタンをクリックします。

  b　入力を要求されたら、リモート デスクトップにアクセスするための認証情報を入力します。

デスクトップのリセット

デスクトップ オペレーティング システムが応答しなくなった場合、デスクトップのリセットが必要な場合があります。リセット操作を実行すると、デスクトップがシャットダウンおよび再起動されます。保存されてないデータは失われます。

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ためにその PC のリセット ボタンを押す操作に相当します。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、保存されずに閉じられることになります。

デスクトップをリセットできるのは、View 管理者がこの機能を有効にしている場合のみです。

手順

- [リセット] コマンドを使用します。

オプション	操作
デスクトップのオペレーティング システムで	選択 クライアント メニュー バーの右端にあるドロップ ダウン メニューから [切断] を選択し、デスクトップ アイコンの下の [リセット] をクリックします。
デスクトップ選択画面から	デスクトップ アイコンの[リセット] ボタンをクリックします。

リモート デスクトップのオペレーティング システムは再起動されます。クライアントがデスクトップから切断されます。

次に進む前に

リモート デスクトップに接続する前に、システムが完全に起動するまで待機します。

インデックス

ひ

ふ

も

り

る

ろ