Atrust

Atrust t68W シン・クライアント

ユーザーマニュアル

Internal Draft 0.02

著作権及び商標について

免責事項

Atrust Computer Corp. (“Atrust”) makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Atrust is not liable for technical or editorial errors or omissions contained herein. The information in this document is subject to change without notice.

本日本語マニュアルはソフトウェアによる翻訳を行っております。
内容は全て英語マニュアルを基準とし、もし万が一意味または文言に相違があった場合、英語版の意味または文言を有効とします。

商標について

Atrust is a trademark of Atrust Computer Corp.

Intel is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, Windows, Windows Server, RemoteFX, and MultiPoint are trademarks or registered trademarks of the Microsoft group of companies.

Citrix, ICA, XenApp, XenDesktop, and VDI-in-a-Box are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

VMware, VMware View, and VMware Horizon View are trademarks or registered trademarks of the VMware, Inc.

PCoIP is a registered trademark of Teradici Corporation in the United States and/or other countries.

Other product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective companies.

このユーザーマニュアルについて

このマニュアルでは、Atrust t68Wシンクライアントの設定、使用、管理、および保守の方法について詳しく説明しています。

マニュアルの構成及び内容

章	内容
1	Atrust t68Wシンクライアントの概要を示します。
2	Atrust t68Wシンクライアントを設定する方法の詳細な手順を説明します。
3	Atrust t68Wシンクライアントの使用方法の基礎を提供します。
4	クライアントの設定を構成し、Atrustクライアントセットアップコンソールでを Atrust t68Wシンクライアントをカスタマイズする方法について説明します。
付録	Atrust t68Wシンクライアントのメンテナンスに関する補足説明を提供します。
仕様	Atrust t68Wシンクライアントの主要コンポーネントに関する詳細情報を提供します。

チェック、ヒント及び重要

このマニュアルでは、以下の形式の注意事項、ヒント、および警告を使用して、重要な情報、有用なアドバイスを提供し、けがや装置の損傷やシステム上のデータの消失を防ぎます。

チェック

- このマークでは、この場面において重要な情報を記載しています。

ヒント

- このマークでは、有効なアドバイスを記載しています。

重要

- このマークでは、危険を伴う内容、デバイスのダメージ、データ消失の危険性等の重要な情報を記載しています。

スタイルコンベンション

このマニュアルでは、入力デバイス、ハードウェアパネル、またはアプリケーションインターフェイスの操作項目を参照しながら、以下のスタイルを使用します。

アイテム	表記	例
キーボードのキー	太字	**Ctrl + F2**, **Ctrl + Alt + Pause**, **Alt + Tab**
アプリケーションウィンドウメニュー、入力リスト	頭大文字	ICA Connection list, RDP Connection list, View Connection list
ウィンドウ上のボタンまたはタブ、ツールバー、タスクバー、またはメニュー	太字	**OK**, **Next**, **Save**, **Applications** tab
ウィンドウ、画面、リスト、またはメニューのオプション	太字	**Start the following program on connection**, **Remote Desktop Services**, **Better Appearance (32-bit)**, **Web Logon**
一連のオプションを選択	太字	**Applications** > **Citrix ICA**, **Applications** > **Remote Desktop**, **Applications** > **VMware View**, **System** > **UWF**

安全性および規制に関する情報

規制声明

連邦通信委員会の干渉声明
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC注意： Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

重要な注意点：

FCC放射暴露に関する声明
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

規制情報

WEEE (Waste Electrical and Electronic Equipment) Directive

In the European Union, this symbol indicates that this product should not be disposed of with household waste. It should be deposited at an appropriate facility to enable recovery and recycling. For proper disposal, please contact your local recycling or hazardous waste center.

安全情報

重要

- ユーザーの指示に記載されている電源装置のみを使用してください。

重要

- 電池を誤ったタイプに交換すると爆発の危険があります。 使用済みの廃棄物電池は指示に従って使用してください。

重要

- 安全のため、機器を機械的または電気的に改造しないでください。
- 機器のカバーを取り外したり、機器内部の部品に触れたりしないでください。 認可されたまたは認定された技術者がいない場合、装置内のあらゆるアクセスは、重大な傷害および損傷を引き起こす可能性があります。 問題が発生した場合は、販売店に連絡してください。
- 製品のマニュアルで許可されている修理のみを行うようにしてください。 認定されたサービス技術者が行っていない修理、交換、拡張、およびアップグレードは、けがをしたり、システムを損傷したり、保証を無効にする可能性があります。

目次

1

概要

この章では、Atrust t68Wシンクライアントの概要を説明します。

1.1 紹介

デスクトップ仮想化は、ITの設計と実装を再考する新しい視点を提供しますインフラ。 デスクトップ仮想化インフラストラクチャでは、ステーションはもはや煩雑なデスクトップではなく、ユーザーがサーバーから配信サービスにアクセスするためのエンドポイントデバイスです。

デスクトップ仮想化テクノロジーの導入により、次のようなメリットがあります。

- アプリケーション/デスクトップへのオンデマンドアクセス
- 作業環境の集中管理
- 大幅に削減されたエンドポイントソフトウェア/ハードウェアの問題
- シンプルなシステムメンテナンスとシステムセキュリティの向上
- 低コストのエンドポイントデバイスによる拡張性の向上

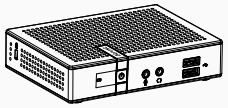
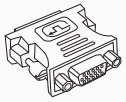
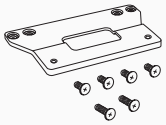
1.2 機能

Atrust t68Wシンクライアントの主な機能は次のとおりです。

- 業界をリードする企業の幅広いデスクトップ仮想化ソリューションのサポート：
  - Microsoft® Remote Desktop
  - Citrix® XenApp™、XenDesktop®、およびVDI-in-a-Box™
  - VMware® View™ および Horizon View™
- 高精細技術のサポート:
  - Microsoft® RemoteFX®
  - Citrix® HDX™
  - VMware® View™ PCoIP®
- さまざまなアプリケーション/デスクトップへの簡単なクリックアクセス
- ローカルクライアント管理コンソールとしての組み込みのAtrust Client Setup

1.3 パッケージ内容

パッケージ内容を確認してください。 すべてのアイテムがパッケージに含まれていることを確認します。 不足または破損しているアイテムがある場合は、直ちに販売店にご連絡ください。

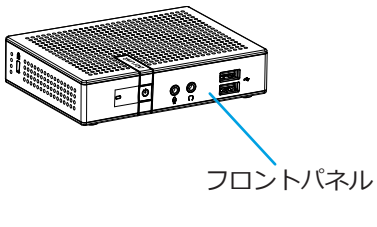
Atrust t68W	ACアダプター	クイックスタートガイド
		
DVI-IからVGAアダプタ	**VESAマウントキット（オプション）**	
		

チェック

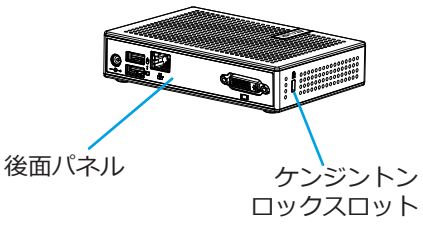
- パッケージにはクイックスタートガイドのハードコピーが入っていない場合があります。 この場合、PDF形式のソフトコピーが提供されます。

1.4 外観

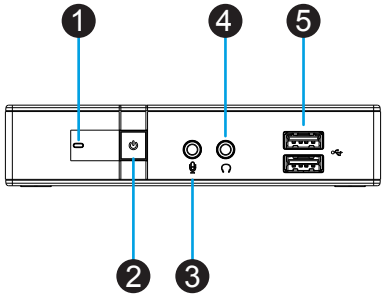
左正面図



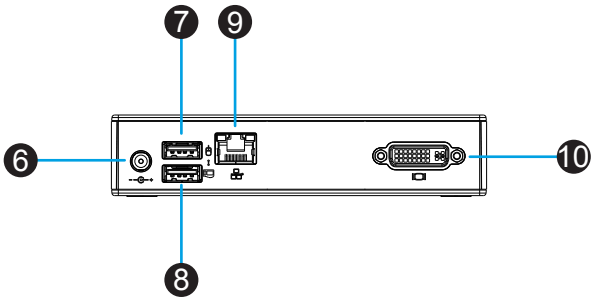
右背面図



1.5 パネルコンポーネント



フロントパネルのコンポーネント			
番号	標識	名称	説明
1		電源LED	電源の状態を示します。
2		電源ボタン	• を押してシンクライアントをオンにします。 • を押して、シンクライアントをシャットダウンします。 • スリープモードに入っているときに押すと、シンクライアントが起動します。
3		マイクポート	マイクに接続します。
4		ヘッドフォンポート	ヘッドフォンまたはスピーカーシステムのセットに接続します。
5		USBポート	USBデバイスに接続します。



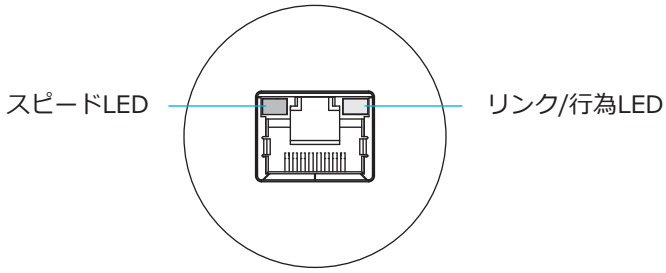
リアパネルのコンポーネント			
番号	**標識**	**名称**	**説明**
6		DC IN	ACアダプタに接続します。
7		USBポート	マウスに接続します。
8		USBポート	キーボードに接続します。
9		LANポート	ネットワークに接続します。
10		DVI-Iポート	モニターに接続します。

1.6 LEDインジケータ

お使いのt68Wには、電源の状態を示す電源LEDが装備されています。 LED信号の意味は次のとおりです。

LED	信号	説明
電源LED	オフ	クライアントはオフです。
	青	クライアントはオンです。
	オレンジ	クライアントはスリープモードになっています。

t68WのLANポートには、ネットワークの状態を示す2つのLEDインジケータがあります。 LED信号の意味は次のとおりです。



	スピードLED (伝送速度)	リンク/行為LED (リンク/送信アクティビティ)	説明
LED信号	オフ	オフ	クライアントはLANに接続されていません。
	オフ	黄色の点滅	クライアントは10 MbpsのLANに接続します。
	オレンジ	黄色の点滅	クライアントは100 MbpsのLANに接続します。
	緑	黄色の点滅	クライアントは1000 MbpsのLANに接続します。

1.7 はじめに

UWF（Unified Write Filter）について

Atrust Client SetupコンソールまたはWindows 10 IoT Enterpriseオペレーティングシステムによるクライアント設定を開始する前に、セッション中にシステムの変更がシステムの再起動後にデフォルトで保持されないことに注意してください。 これは、システムにUWF（Unified Write Filter）という特別な機能があるためです。

デフォルトでは、t68WはUWF対応です。 ユニファイド書き込みフィルタ（UWF）は、セクタベースの書き込みフィルタで、保護されたボリュームへのすべての書き込み試行をインターセプトし、それらの書き込み試行を仮想オーバーレイにリダイレクトします。 UWFでは、すべてのシステム変更は変更が行われたセッションにのみ影響します。 再起動後、すべての変更は破棄されます。

Atrust Client Setupコンソールを使用してデフォルトを変更できます。 システムを変更する前に、このユーザーマニュアルの関連するセクションを最初にお読みになることを強くお勧めします。

重要

- ご使用のシステムを変更する前に、「4.2.10 UWFの設定（Unified Write Filter）」（52ページ）を参照してください。

チェック

- シンクライアントデバイスとして、t68Wは主にサーバー上のリモートまたは仮想デスクトップへのアクセス用です。 制限付きで保護された（UWF対応）ハード・ディスク・スペースでは、t68Wにデータを保管することは推奨されません。 代わりに、リモート/仮想デスクトップ、リムーバブルストレージデバイス、またはネットワーク上のストレージスペースを使用できます。
- 保護されたボリュームにファイルをコピーする必要がある場合は、そのサイズが空きメモリ（オーバーレイ）の容量よりも小さいことを確認してください。 そうしないと、システムが予期しない結果になるか、応答しなくなる可能性があります。

既定のユーザーアカウントについて

Windows 10のIoT Enterpriseには、標準のユーザーアカウントと標準のユーザーアカウントの2つの既定のユーザーアカウントがあります。 デフォルトの資格情報は、次のように表示されます。

種類	アカウント名	パスワード
Administrator	Administrator	Atrustadmin
Standard user	User	Atrustuser

チェック

- パスワードは大文字と小文字を区別します。

システム起動時の動作について

システムが起動するたびに、既定のユーザーアカウントに関する既定の標準ユーザーアカウントを使用して、Windows 10のIoT Enterpriseオペレーティングシステムに自動的にログインします。

1.8 t68Wによるサービスアクセス

Atrust t68Wを使用すると、Microsoft、Citrix、およびVMwareのデスクトップ仮想化ソリューションにマウスでクリックするだけでアクセスできます。 アクセスのショートカットには、標準とカスタマイズの2種類があります。 前者はデフォルトでWindows 10 IoT Enterpriseのデスクトップで利用可能です。 後者は、Atrust Client Setupコンソールを使用して作成およびカスタマイズできます。

標準のデスクトップショートカット

標準デスクトップショートカットを使用してオンデマンドアプリケーションまたはデスクトップにアクセスする方法については、第3章「入門」（17ページ）または「クイックスタートガイド」（t68W）を参照してください。

カスタマイズされたデスクトップショートカット

アクセスのショートカットを作成およびカスタマイズする方法については、第4章「クライアント設定の構成」（31ページ）を参照してください。

2

t68Wをセットアップ

この章では、t68Wシンクライアントのセットアップ方法の詳細な手順を説明します。

2.1 t68Wの位置づけ

t68Wの位置を決めるには2つの方法があります。

- スタンドを置いて、机や望む場所に**直立**させてください。
- VESAマウントキットを使用して**モニタ**の背面に取り付けます。

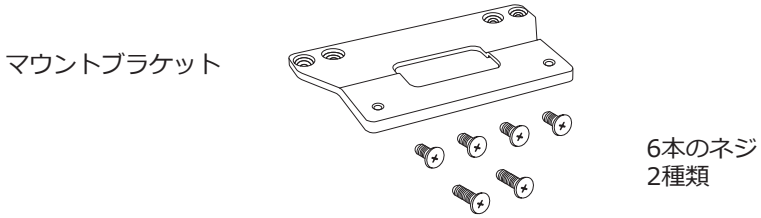
> **チェック**
> - VESAマウントキットは、t68Wのオプションアクセサリです。 パッケージにはVESAマウントキットが含まれていない可能性があります。 必要に応じて販売店にお問い合わせください。

t68Wをモニターの背面に取り付けるには、以下の手順に従ってください：

ステップ1： t68W用のVESAマウントキットを理解する
ステップ2： あなたのt68Wをマウントする

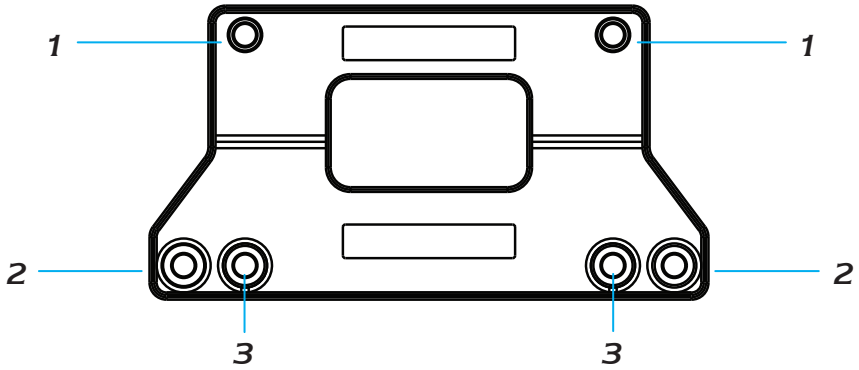
ステップ1：t68W用のVESAマウントキットを理解する

t68WのVESAマウントキットは、ブラケットと6本のネジで構成されています。



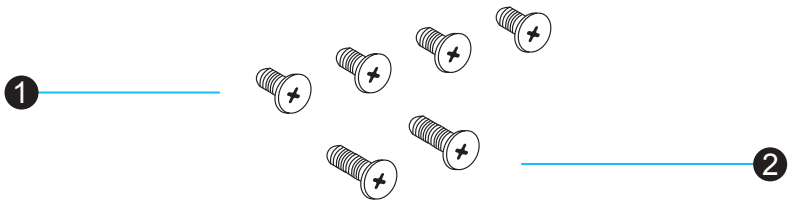
マウントブラケット

t68W用マウントブラケットのVESAマウント穴については、次の図および説明を参照してください。



マウントホール	説明
1	ブラケットをt68Wに固定するためのVESAマウント穴。
2	モニターにブラケットを固定するためのVESAマウント穴（100 mmの距離）。
3	モニターにブラケットを固定するために使用されるVESA取り付け穴（75 mmの距離を使用）。

マウントスクリュー

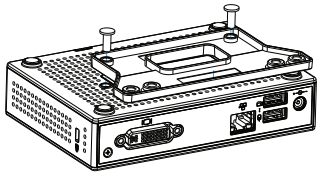


ねじタイプ	番号	説明
1	4	ブラケットをt68Wおよびモニターに固定するためのネジ。
2	2	タイプ1のネジでブラケットとt68Wをモニターにしっかりと固定できない場合は、ブラケットをモニターに固定するために使用されるネジがより長い。

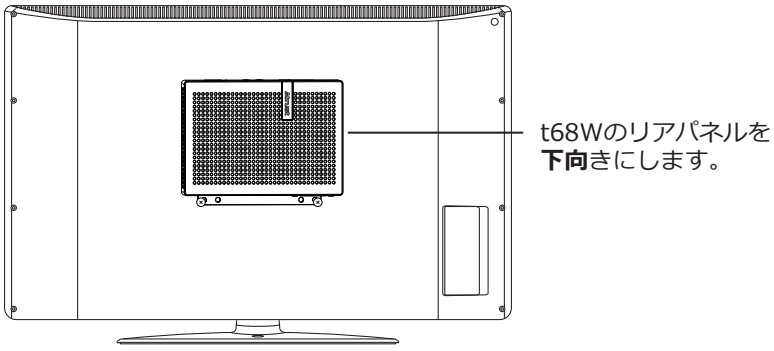
ステップ2：あなたのt68Wをマウントする

t68Wをモニターの背面に取り付けるには、以下を実行してください。

1. t68WをVESAマウント穴のある面を上にして平らな面に置きます。
2. ブラケット側にアトラストが下向きになっている状態で、ブラケットの2つのマウント穴をt68Wの2つのマウント穴に合わせて、ブラケットが前方に出て、フロントパネルよりも後方に近づくようにしてから、ブラケットを固定します あなたのt68Wには 1 タイプの2本のネジが付いています。



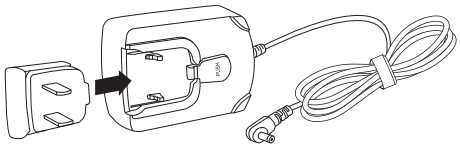
3. ブラケットの取り付け穴をモニター背面の取り付け穴に合わせ、ブラケットを 1 または 2 のネジ2本でモニターに固定します。 t68Wのリアパネルが**下向**きになっていることを確認します。



2.2 ACアダプタの組み立て

ACアダプターをt68W用に組み立てるには、以下を実行してください。

1. シンクライアントパッケージを開梱し、ACアダプタとその取り外したプラグを取り出します。
2. カチッと音がするまでプラグをACアダプタに差し込みます。



チェック

- 付属のプラグは、地域によって異なる場合があります。

2.3 接続

t68Wを接続するには、以下を実行してください：

1. t68Wをイーサネットケーブルでローカルネットワークに接続します。
2. キーボードとマウスをt68Wに接続します。
3. モニターを接続して**電源を入れ**ます。

チェック

- VGAモニターのみが使用可能な場合は、付属のDVI-I to VGAアダプターを使用してt68Wとモニターを接続してください。
- シンクライアントの電源を入れる**前**に、モニタを接続して電源を入れる必要があります。 そうしないと、クライアントがモニタに適切な解像度を設定できないことがあります。

4. パッケージに同梱のACアダプタを使用して、t68Wをコンセントに接続します。

チェック

- 付属のACアダプターの組み立て方法については、「2.2 ACアダプタの組み立て」（15ページ）を参照してください。

5. 必要に応じて、他の周辺機器をt68Wに接続します。

3

入門

この章では、t68Wの使い方の基本について説明します。

3.1 標準のショートカット

仮想デスクトップまたはアプリケーションサービスには、デスクトップ上の標準ショートカットを使用するだけでアクセスできます。

番号	ショートカット	説明	参照先
1	Citrix Receiver	ダブルクリックしてCitrixサービスにアクセスします。 **注意:** Citrix環境でセキュアなネットワーク接続が実装されていない場合、この新しいバージョンのCitrix Receiverを使用してCitrixサービスにアクセスできない場合があります。 また、Citrixでは、Webブラウザ経由でサービスにアクセスすることもできます。 Citrix Receiverに問題がある場合は、組み込みのInternet Explorerを使用してみてください（この章の手順を参照）。	3.2
2	Remote Desktop Connection	Microsoftリモートデスクトップサービスにアクセスするには、ダブルクリックします。	3.3
3	VMware Horizon View Client	VMware ViewおよびVMware Horizon Viewサービスにアクセスするには、ダブルクリックします。	3.4

3.2 Citrixサービスへのアクセス

Internet ExplorerでCitrixサービスにアクセス

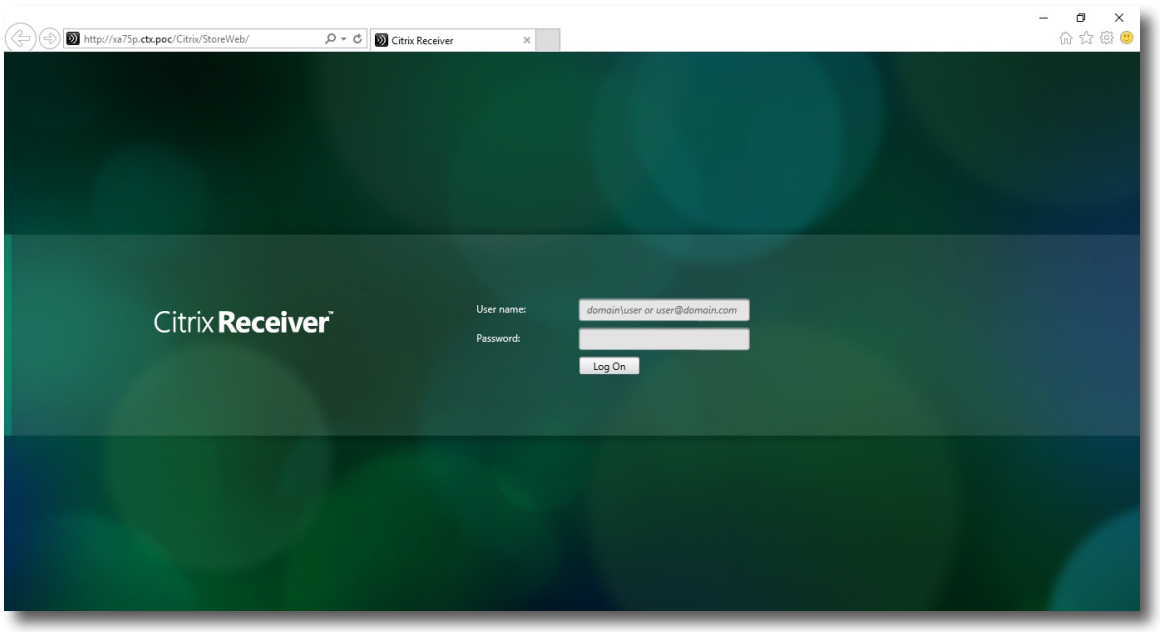
Internet ExplorerでCitrixサービスにすばやくアクセスするには、次の操作を行ってください。

1. [**Start**] のアイコンをクリックしてInternet Explorerを開きます。
2. CitrixサービスにアクセスできるサーバーのIPアドレス/ URL / FQDNを入力します。

> **チェック**
> - XenDesktop 7.0以降では、IT管理者に相応しいIPアドレス/ URL / FQDNを問い合わせてください。

3. オンラインの指示に従って必要なデータを提供し、Citrixサービスにアクセスします。

ログオン画面の例
XenDesktop / XenApp 7.5 Platinum

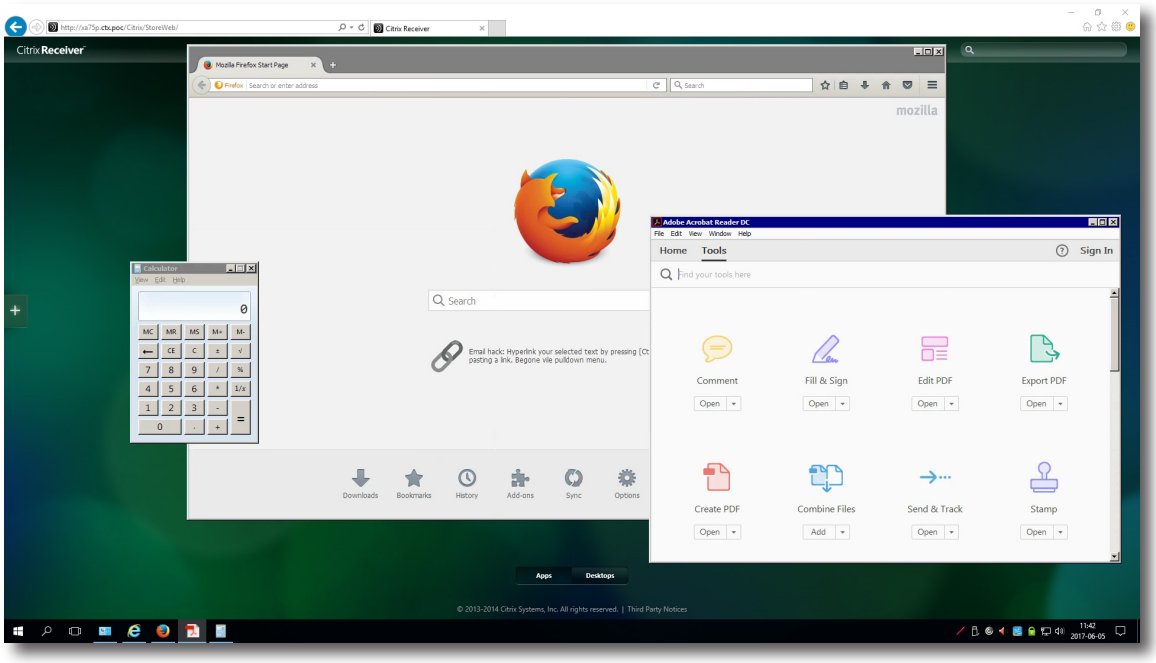


仮想デスクトップの例

Windows 7 Ultimate
(t68Wで起動)

仮想アプリケーションの例

電卓、Firefox、およびAdobe Reader
(t68Wで起動)



Citrix ReceiverのショートカットによるCitrixサービスへのアクセス

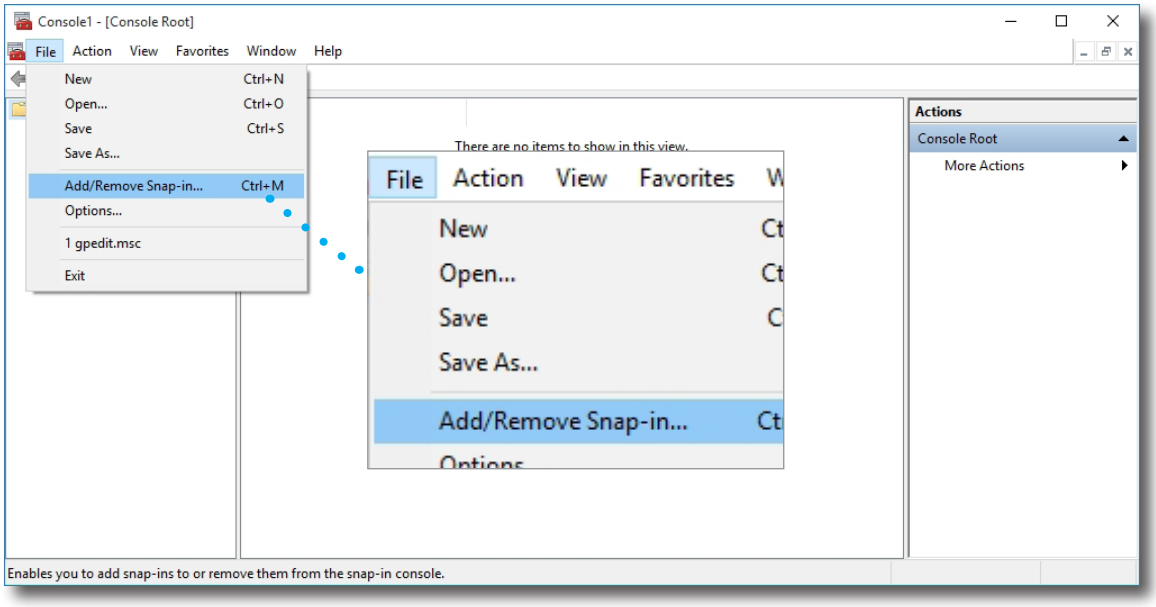
Citrix Receiverのショートカットを使用してCitrixサービスにアクセスするには、次の手順を実行します。

1. 管理者アカウントで使用可能なCitrixサービスに必要な安全証明書をインポートします。 必要な支援については、IT管理者に相談してください。

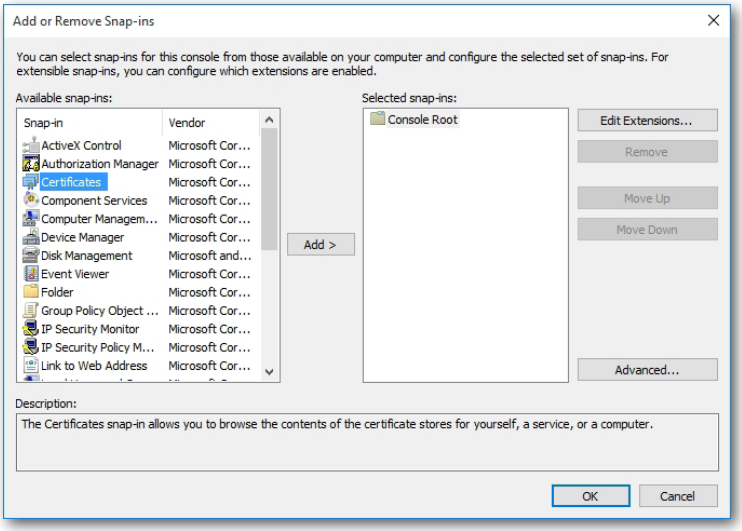
   a) デスクトップの左下にある  をクリックします。

   b) 開いたウィンドウに [**mmc**] と入力し、[**Enter**] キーを押します。

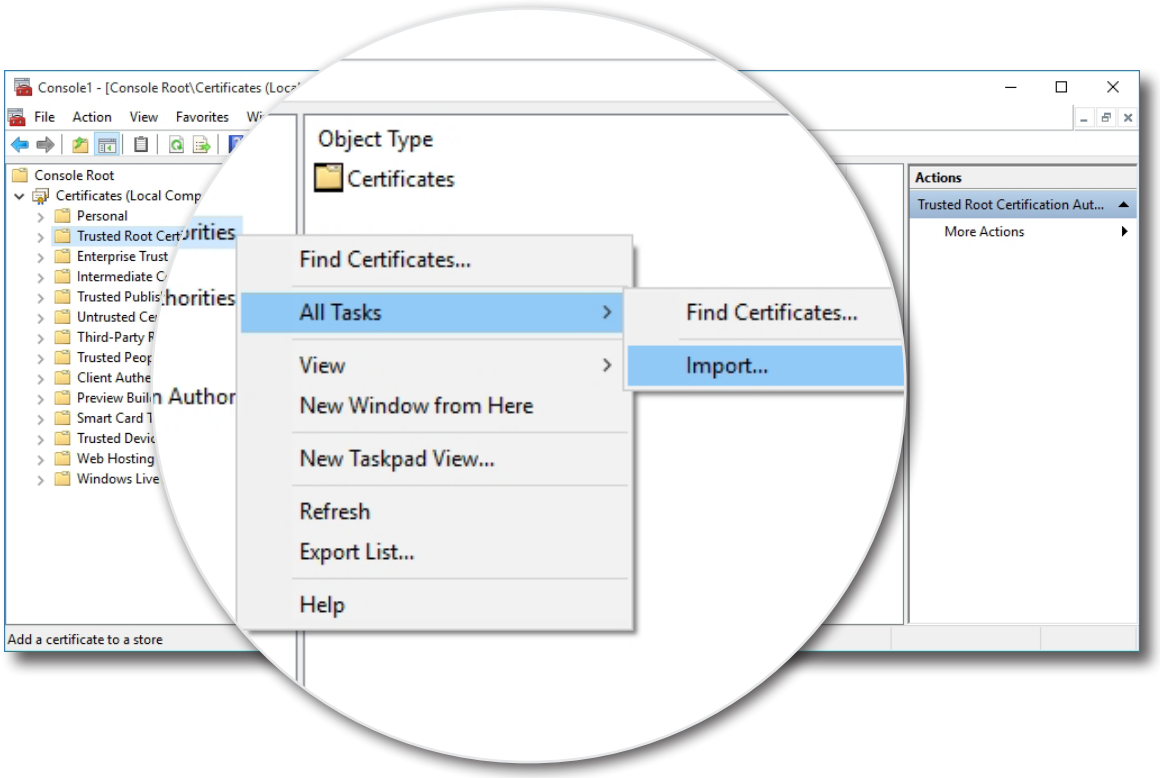
   c) コンソールウィンドウで、[File] メニューの [**Add/Remove Snap-in**] をクリックします。



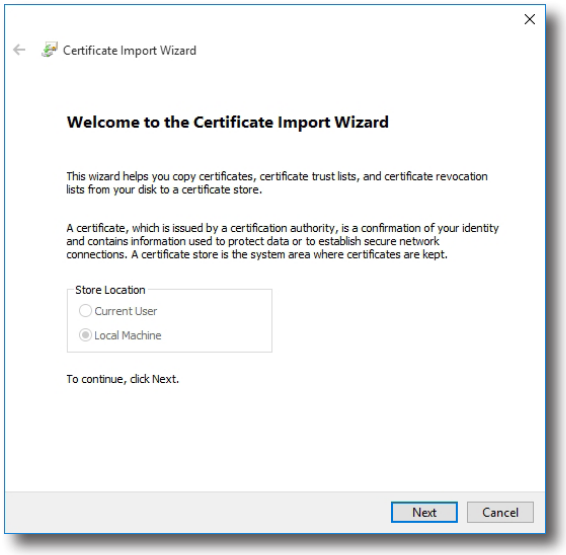
d) 開いたウィンドウで、[**Certificates**] > [**Add**] > [**Computer account**] > [**Local computer**] > [**OK**] をクリックして、証明書スナップインを追加します。



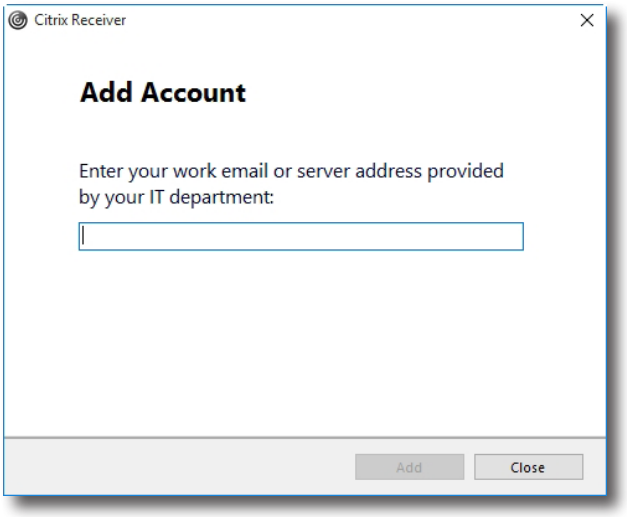
e) コンソールウィンドウで、証明書のグループツリーをクリックして展開し、[**Trusted Root Certification Authorities**] を右クリックして、ポップアップメニューで [**All Tasks**] > [**Import**] を選択します。



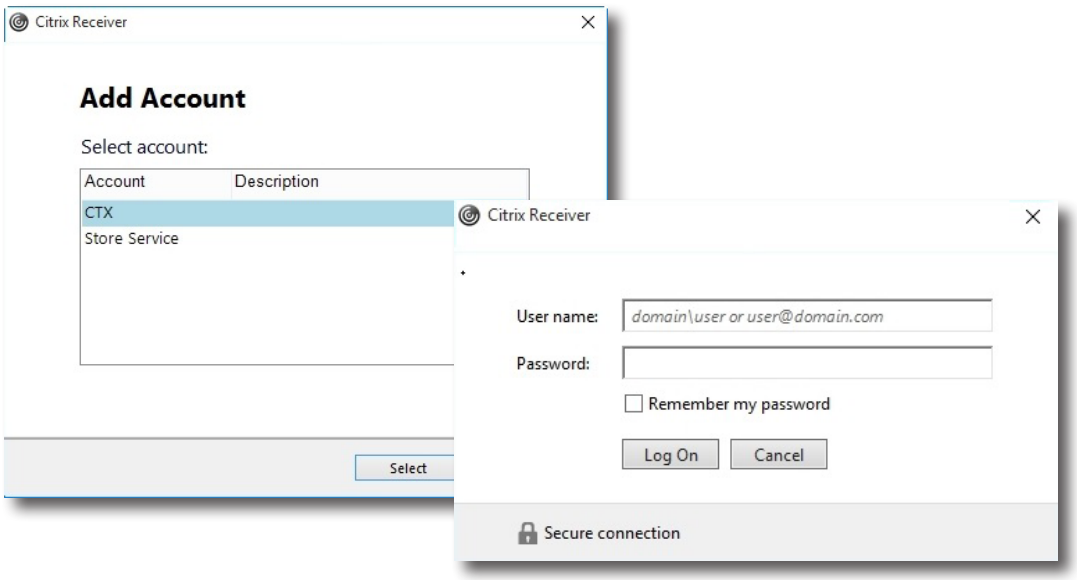
f) 証明書のインポートウィザードに従って証明書をインポートし、完了したらコンソールウィンドウを閉じます。



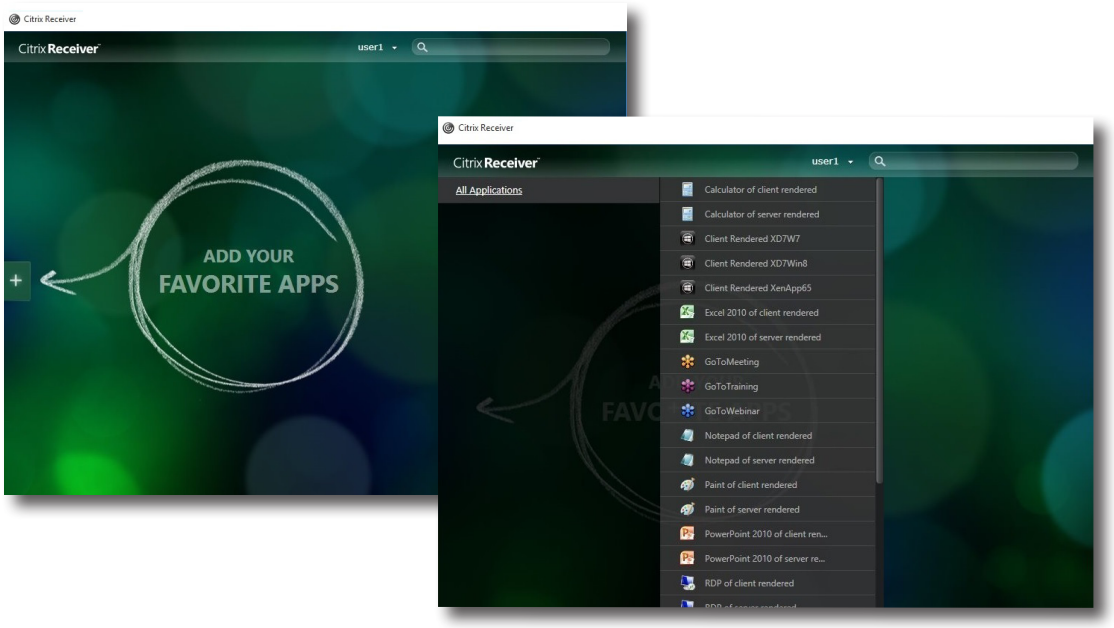
2. デスクトップ上の**Citrix Receiver** をダブルクリックします。
3. 作業用電子メールまたはサーバーアドレスの入力を求めるウィンドウが表示されます。 ここで提供する適切な情報については、IT管理者に相談し、必要なデータを入力してから、[**Add**] をクリックして続行してください。



4. 複数のストアが利用可能な場合は、目的のストアアカウントを選択し、開いているウィンドウに資格情報を入力して、[**Log On**] をクリックします。



5. 提供された資格情報のお気に入りのアプリケーション（仮想デスクトップとアプリケーション）を追加できるウィンドウが表示されます。 クリックして、目的のアプリケーションを選択します。 選択したアプリケーションがそのウィンドウに表示されます。

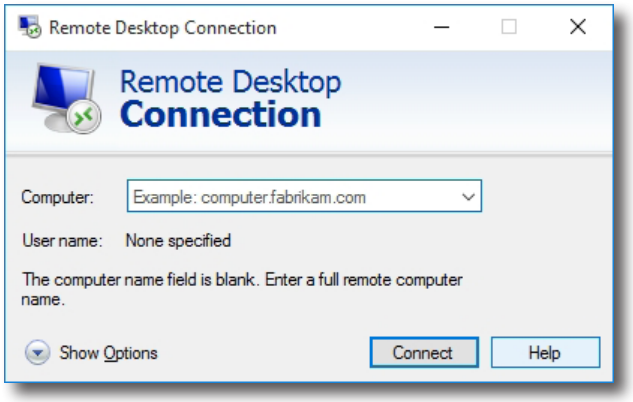


6. これで目的のアプリケーションを起動できます。 仮想デスクトップまたはアプリケーションが画面に表示されます。

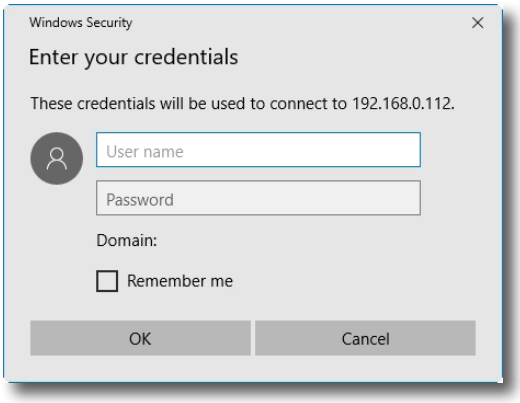
3.3 Microsoftリモートデスクトップサービスへのアクセス

リモートデスクトップサービスにすばやくアクセスするには、以下を実行してください。

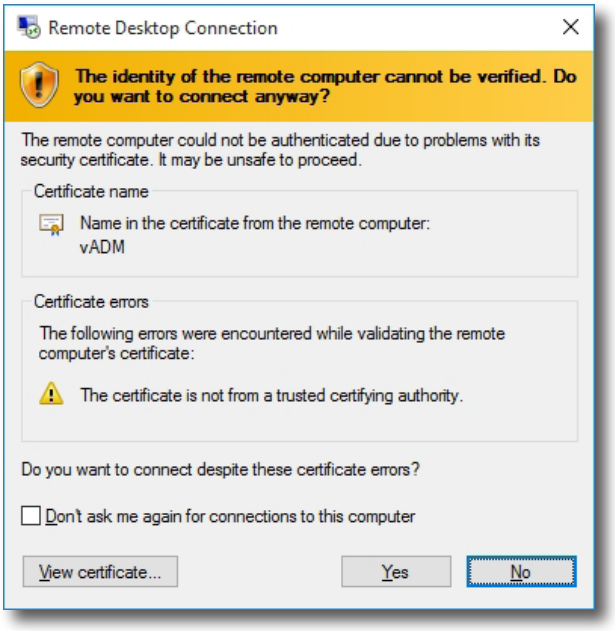
1. デスクトップの [**Remote Desktop Connection**]  をダブルクリックします。
2. 開いたウィンドウにリモートコンピュータの名前またはIPアドレスを入力し、[**Connect**] をクリックします。



3. 資格情報を入力し、[**OK**] をクリックします。



4. ウィンドウにリモートコンピュータに関する証明書メッセージが表示されることがあります。 詳細についてはIT管理者に相談し、最初に接続が安全であることを確認してください。 バイパスするには、[**Yes**] をクリックして続行します。

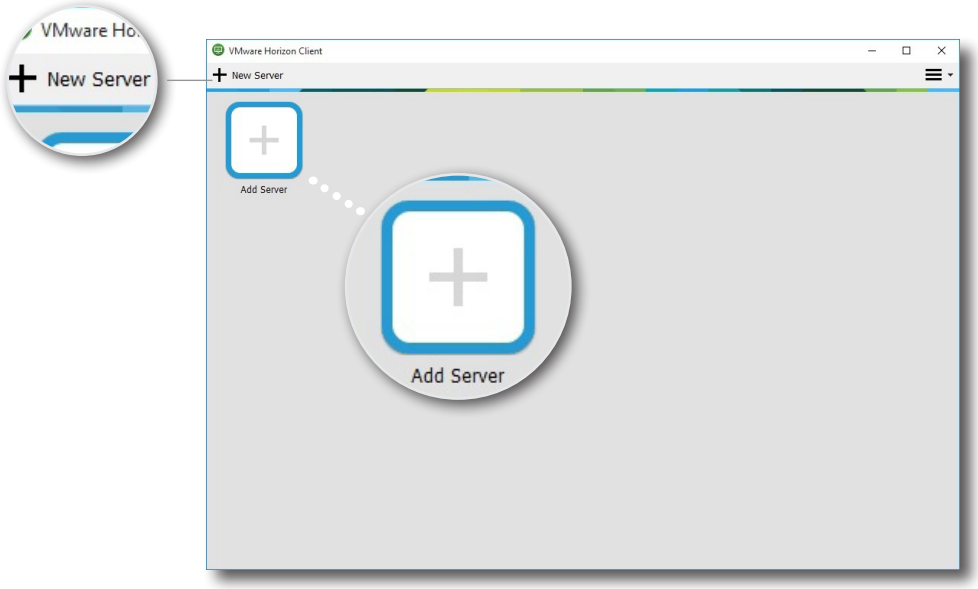


5. リモートデスクトップが画面に表示されます（デフォルトでは全画面表示）。

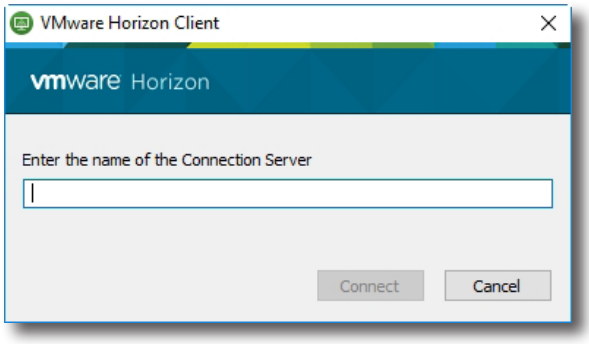
3.4 VMware ViewおよびHorizon Viewサービスへのアクセス

VMware ViewまたはHorizon Viewのサービスにすばやくアクセスするには、次の手順を実行してください。

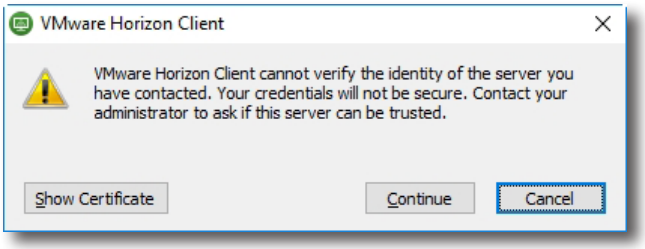
1. デスクトップ上の **VMware Horizon View Client**  をダブルクリックします。
2. View Connection Serverの名前またはIPアドレスを追加できるウィンドウが表示されます。
3. [**Add Server**] アイコンをダブルクリックするか、左上隅の [**New Server**] をクリックします。



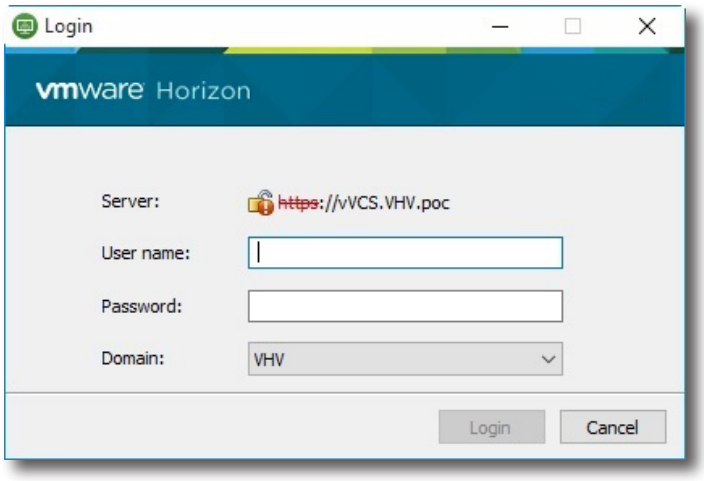
4. View Connection Serverの名前またはIPアドレスの入力を求めるウィンドウが表示されます。 必要な情報を入力し、[**Connect**] をクリックします。



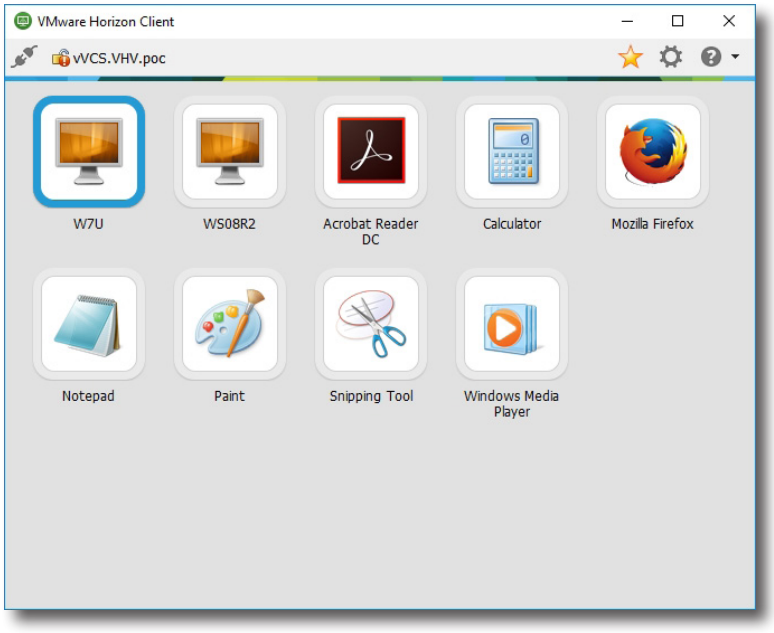
5. ウィンドウにリモートサーバーに関する証明書メッセージが表示されることがあります。 詳細についてはIT管理者に相談し、最初に接続が安全であることを確認してください。 バイパスするには、[**Continue**] をクリックします。



6. ウェルカムメッセージが表示されたウィンドウが表示されることがあります。 [**OK**] をクリックして続行します。
7. 開いたウィンドウにユーザー名とパスワードを入力し、[**Login**] をクリックします。



8. 使用可能なデスクトップまたはアプリケーションの資格情報のウィンドウが表示されます。 目的のデスクトップまたはアプリケーションをダブルクリックして選択します。



9. デスクトップまたはアプリケーションが画面に表示されます。

4

クライアント設定の構成

この章では、高度な設定を構成し、t68WをAtrust Client Setupでカスタマイズする方法について説明します。

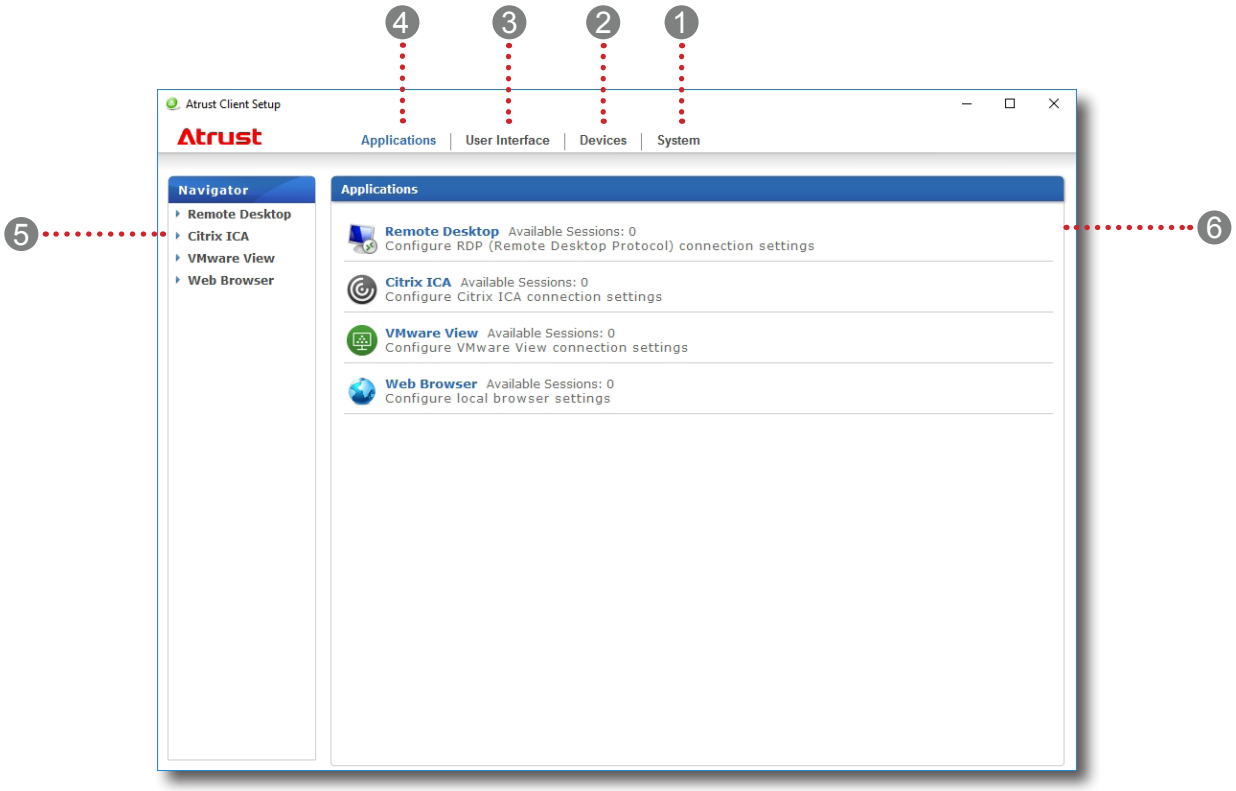
4.1 Atrust Client Setup

4.1.1 インタフェースの概要

t68Wシンクライアント上のAtrust Client Setupにアクセスするには、以下を実行してください。

1. 管理者アカウントでt68Wにログインします（デフォルトについては（8ページ）を参照）。
2. 開始画面で [**Atrust Client Setup**] をクリックします。
3. [Atrust Client Setup] ウィンドウが表示されます。

インタフェースの概要



インタフェース要素		
番号	**名称**	**説明**
1	System tab	クリックすると、クライアントの操作とメンテナンスの設定を行います。
2	Devices tab	クリックすると、クライアントの外部デバイスの設定を行います。
3	User Interface tab	クリックすると、クライアントのユーザーインターフェイスを構成します。
4	Applications tab	クリックすると、クライアントを介したサービスアクセスの設定が構成されます。
5	Navigation area	選択したタブの下にある設定項目を選択するか、選択した設定項目の設定項目を選択する場合にクリックします。
6	Configuration area	設定項目または項目が選択されたときに設定値を設定します。

4.1.2 使用可能なタスク一覧

次の表は、4つの主要設定カテゴリの下の各設定項目の簡単な説明を示しています。

タブ	設定項目	参照先	ページ
System	• パスワードの設定 • リモートアシスタンス設定の構成 • ファームウェアの更新 • スナップショットを撮る • アプライアンスモードの有効化/無効化 • UWF（Unified Write Filter）設定の構成 • 自動登録の設定	4.2 システム設定の構成	35
Devices	• USBストレージデバイスの設定を構成 • オーディオデバイスの設定を構成	4.3 外部デバイス設定の構成	55
User Interface	• サービスアクセスショートカットの表示の設定	4.4 ユーザーインターフェイス設定の構成	58
Applications	• Microsoft RDP接続設定の構成 • Citrix ICA接続設定の構成 • VMware View接続設定の構成 • Webブラウザのセッション設定の構成	4.5 サービスアクセス設定の構成	60

チェック

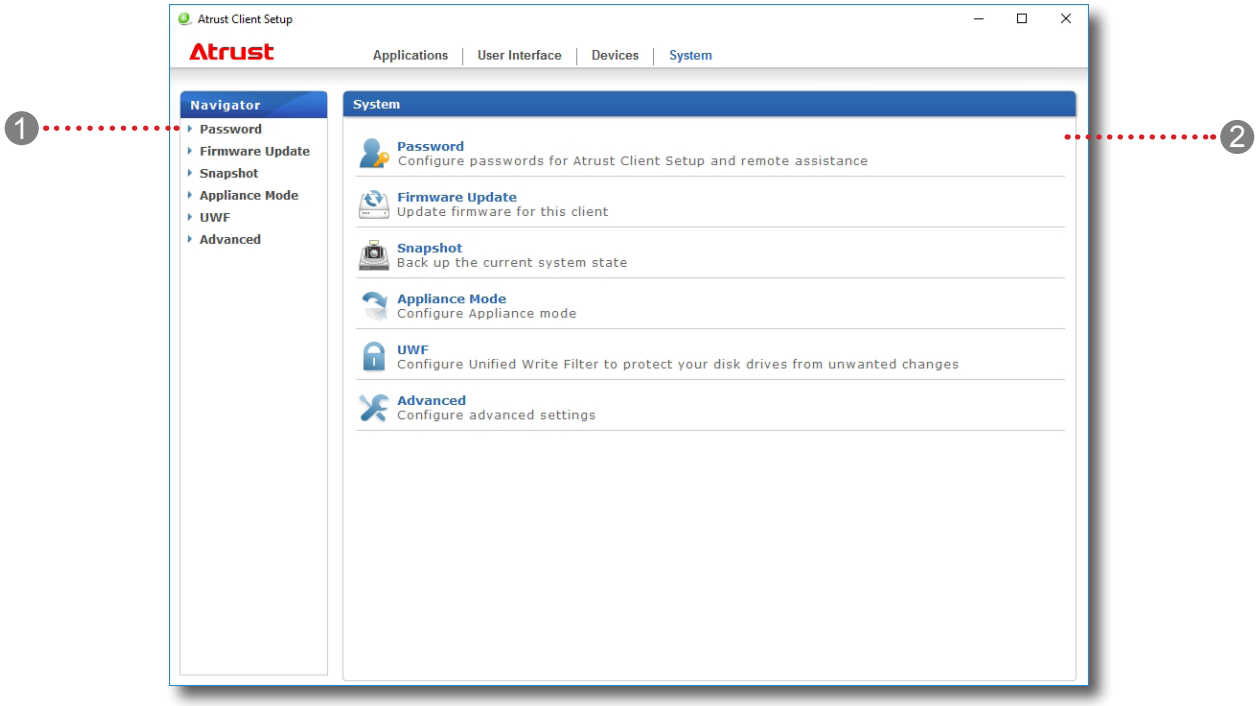
- 上記の表は、Windows 10 IoT Enterpriseを実行するAtrust t68Wシンクライアントにのみ適用されます。 他のWindows 10 IoT Enterpriseベース、Windows Embeddedベース、Linuxベース、およびARM Linuxベースのシンクライアント用のAtrust Client Setupコンソールの使用可能な設定カテゴリとアイテムは、異なる場合があります。

4.2 システム設定の構成

4.2.1 システムタブの概要

[**System**] タブでは、クライアントの操作および保守の設定を構成できます。 [**System**] タブの使用可能な設定にアクセスするには、[Atrust Client Setup] タブをクリックします。

システムタブの概要



インタフェース要素		
番号	**名称**	**説明**
1	ナビゲーション領域	[**System**] タブの設定項目をクリックして選択します。
2	構成領域	設定項目を選択したときの設定値を設定します。

4.2.2 使用可能なタスク一覧

タブ	設定	アイコン	説明	参照先	ページ
システム	パスワード		クリックすると、Atrust Client Setupへのアクセスが保護されます。 クリックすると、リモートアシスタンスの設定を行います。	4.2.3 4.2.4	37 38
	ファームウェアアップデート		リモート管理コンピュータの助けを借りてファームウェアをローカルに更新する場合にクリックします。 この機能は、クライアントがAtrust Device Managerコンソールで管理されている場合にのみ適用されます。	4.2.5	40
	スナップショット		クリックすると、クライアントのスナップショット（システムイメージ）を取得し、一括デプロイメントまたはシステムリカバリを実行します。	4.2.6 4.2.7 4.2.8	42 43 46
	アプライアンスモード		自動RDP / ICA / Viewセッションを許可/禁止するアプライアンスモードを有効または無効にする場合にクリックします。 アプライアンスモードでは、クライアントは目的のRDP / ICA / Viewセッションで起動し、セッションを終了した後に設定されたアクションを実行します。	4.2.9	49
	UWF		UWF（Unified Write Filter）設定を構成する場合にクリックします。 UWFオプションを有効にすると、ディスクボリュームの対象となるすべての書き込みがRAMキャッシュにリダイレクトされます。 すべてのシステム変更は、変更が行われたセッションにのみ影響します。	4.2.10	52
	アドバンスド		クリックすると、自動登録などの詳細設定を行います。	4.2.11	54

チェック

- Atrust Device Managerは、リモートおよび大規模なクライアント管理コンソールであり、デスクトップ仮想化インフラストラクチャ内の多数のエンドポイントデバイスをリモートで管理するのに役立ちます。 Atrust Device Managerの詳細については、Atrust Device Managerのユーザーズマニュアルを参照してください。

4.2.3 Atrust Client Setupへのアクセスを保護

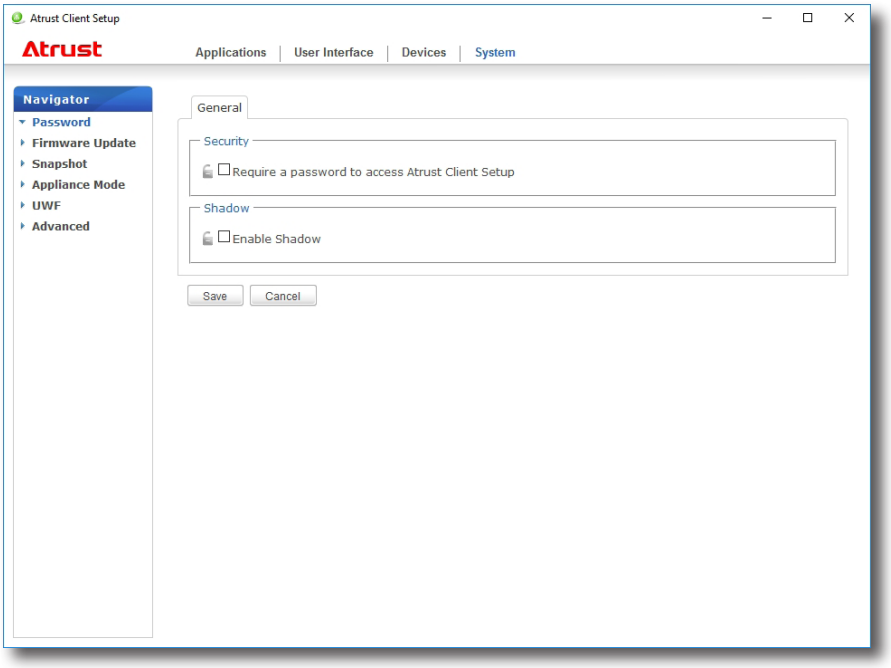
パスワード設定でAtrust Client Setupへのアクセスをパスワードで保護することができます。

Atrust Client Setupへのアクセスを保護するには、以下を実行してください。:

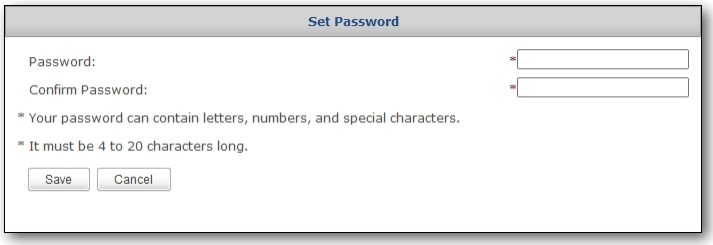
チェック

- システム管理者（および管理者のみ）は、Atrust Client Setupップにアクセスできます。 Atrust Client Setupへのアクセスを保護しない場合は、管理者権限でAtrust Client Setupにアクセスできます。 ここでパスワードが設定されている場合、管理者はAtrust Client Setupに入るためにそのパスワードが必要になります。

1. Atrust Client Setupで、[**System**] > [**Password**] の順にクリックします。



2. [Security] セクションの [**Require a password to access Atrust Client Setup**] をクリックしてオンにします。
3. パスワードを設定するためのウィンドウが表示されます。



4. 目的のパスワードを入力し、[**Save**] をクリックして確認します。
5. [**Save**] をクリックしてすべての変更を保存します。

4.2.4 リモートアシスタンスのシャドウ設定の構成

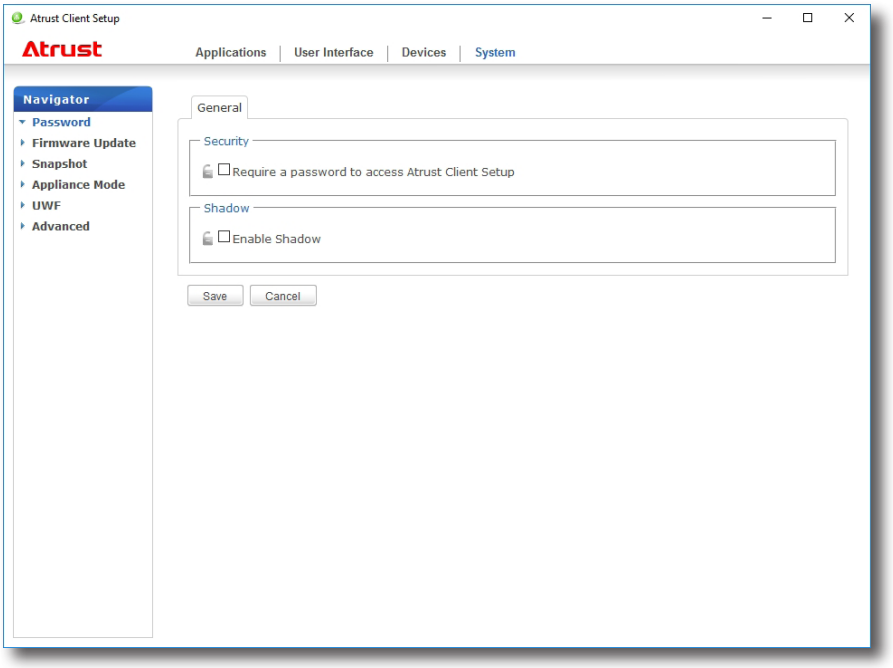
シャドウ機能を使用すると、管理者は、クライアントユーザーがリモートで問題を解決したり、ローカル設定を構成したりするのを支援することができます。 この機能を有効にすると、管理者はローカルユーザーと同様にリモートコンピュータからクライアントを監視および制御できます。

チェック

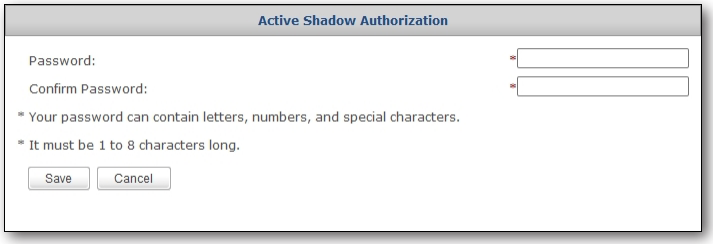
- リモートコンピュータでシャドウ機能を使用するには、Atrust Device ManagerとJavaソフトウェアをリモートコンピュータにインストールし、クライアントをAtrust Device Managerの管理対象グループに追加する必要があります。 詳細な手順については、Atrust Device Managerのユーザーズマニュアルを参照してください。

シャドウ機能を有効にしてリモートアシスタンスのパスワードを設定するには、次の操作を行います。

1. Atrust Client Setupで、[**System**] > [**Password**] の順にクリックします。



2. [Shadow] セクションで、[**Enable Shadow**] をクリックします。
3. シャドウ機能が有効になり、リモートアシスタンスのパスワードを設定するウィンドウが表示されます。



チェック

- リモートコンピュータでは、管理者は、Atrust Device Managerコンソールで使用できるシャドウ機能（リモートアシスタンス）を使用するためにこのパスワードが必要になります。 詳細については、Atrust Device Managerのユーザーズマニュアルを参照してください。

4. 目的のパスワードを入力し、[**Save**] をクリックして確認します。
5. [**Save**] をクリックしてすべての変更を保存します。

チェック

- シャドウ機能が有効になっていると、t68Wでタスクバーの通知領域にアイコン  が表示されます。 この機能が現在リモートコンピュータから実行されている場合、アイコンの色は黄色  に変わります。

4.2.5 管理コンピュータからのファームウェアの更新

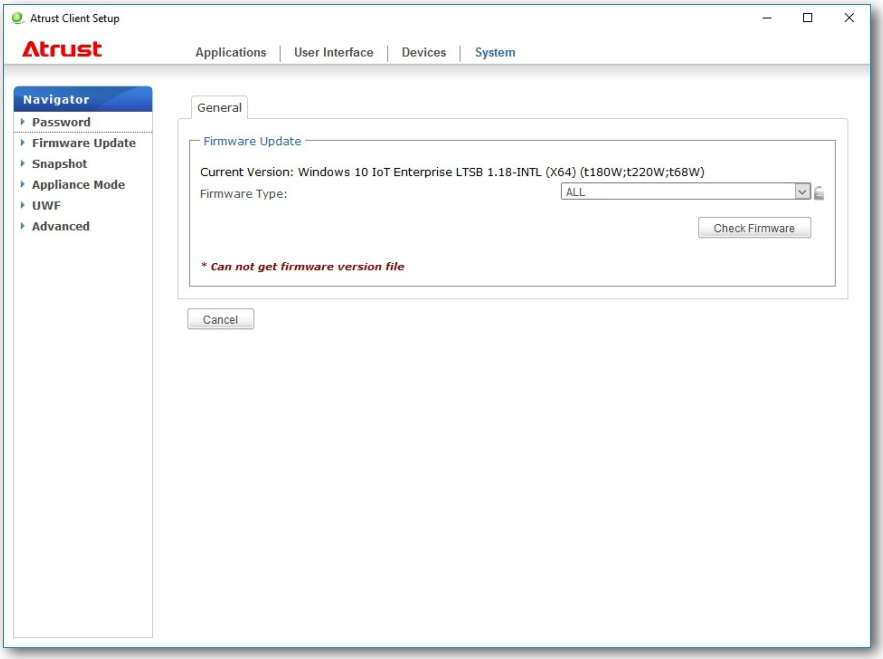
アップデートファームウェアを使用すると、リモート管理コンピュータからクライアントファームウェアをアップデートして、クライアントデバイスを最新の状態にすることができます。

チェック

- クライアントがリモートコンピュータにインストールされているAtrust Device Managerの管理対象グループに追加され、クライアントファームウェアファイルがAtrust Device Managerにインポートされていることを確認します。 これらは、この機能の前提条件です。
- ファームウェアアップデートとAtrust Device Managerの詳細については、Atrust Device Managerのユーザーズマニュアルを参照してください。

リモート管理コンピュータからクライアントファームウェアを更新するには、以下を実行してください。

1. Atrust Client Setupで、[**System**] > [**Firmware Update**] の順にクリックします。

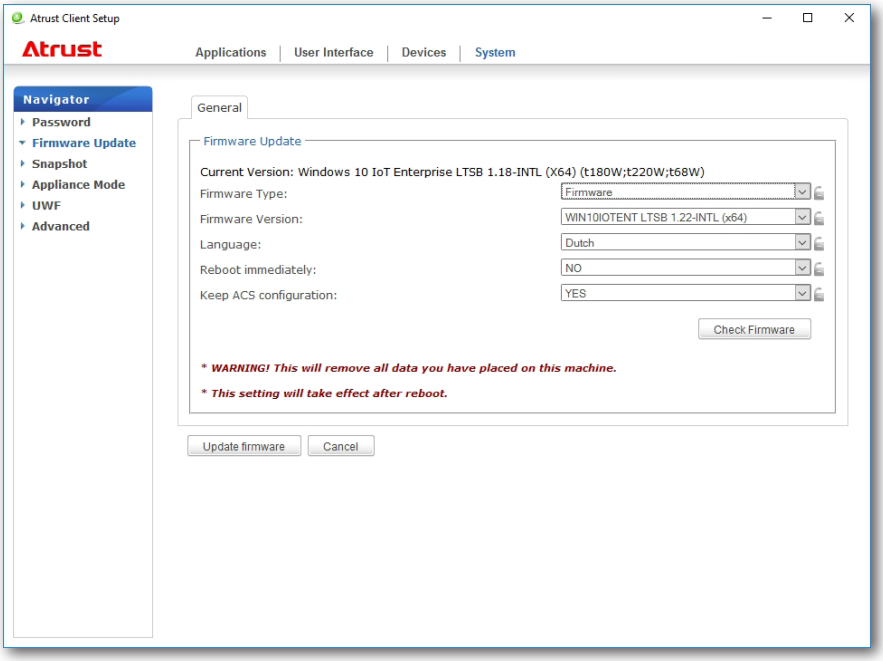


2. [Firmware Update] セクションで、[Firmware Type] ドロップダウンメニューをクリックして [**Firmware**] を選択し、[**Check Firmware**] をクリックします。
3. 完了すると、Firmwareリストがロードされたことを通知するウィンドウが表示されます。 [OK] をクリックして続行します。

チェック

- 使用可能なファームウェアのバージョンは、リモートAtrust Device Managerにインポートされたバージョンの数によって異なります。

4. ドロップダウンメニューをクリックして、目的のファームウェアのバージョンとその他のオプションを選択します。



ファームウェアアップデートオプション	
項目	**説明**
ファームウェアの種類	クリックして、目的のファームウェアタイプを選択します。 **タイプ** / **説明** すべて / すべてのファームウェアタイプ、**ファームウェア**および**スナップショット**。 ファームウェア / クライアントのシステムイメージ。 スナップショット / 同じモデルの別のクライアントから来たクライアントのシステムイメージ。 **注意:** モデルのファームウェアバージョンでは、オプションが使用できない場合があります。
ファームウェアのバージョン	ファームウェアリストから目的のファームウェアバージョンをクリックして選択します。
言語	Atrust Client Setupコンソールを含むシステムのインタフェース言語をクリックして選択します。 **注意:** 使用可能な言語は、ファームウェアのバージョンによって異なる場合があります。
すぐに再起動	ファームウェアを更新するためにすぐにシステムを再起動するか、後でシステムを手動で再起動するかを選択します。
ACS設定を維持	クライアント設定をAtrust Client Setupの下に保持するかどうかを選択する場合にクリックします。 **注意:** [**Yes**] を選択すると、ファームウェアの更新後も、Atrust Client Setupのすべてのクライアント設定は変更されません。 [**No**] を選択すると、すべての設定が出荷時のデフォルト設定に戻ります。 **注意:** クライアントがAtrust Device Managerで管理されていて、ここで [**No**] が選択されている場合、ファームウェアの更新後にAtrust Device Managerがクライアントの管理に失敗します。 Atrust Device Managerの詳細については、Atrust Device Managerのユーザーズマニュアルを参照してください。

5. [**Update firmware**] をクリックして選択を確定します。 システムは再起動後にファームウェアの更新を開始します。

4.2.6 一括展開またはシステム復旧のためのスナップショットの作成

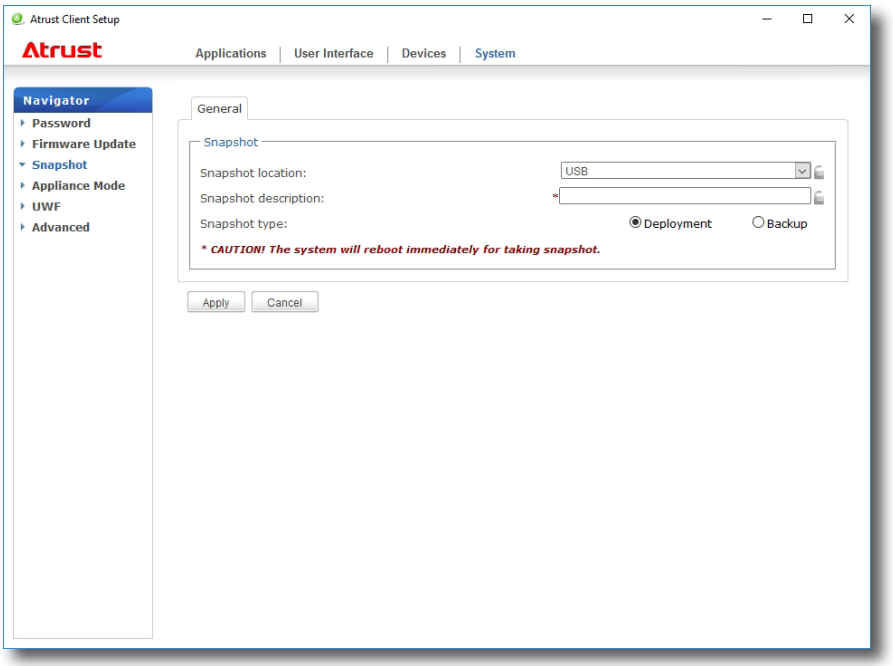
スナップショットとは、クライアントのシステムイメージで、一括デプロイやシステムリカバリにそのイメージを使用できるようにします。 このイメージは、リモート管理コンピュータまたはローカルに接続されたUSBフラッシュドライブに保存できます。

チェック

- システムイメージをリモートコンピュータに保存するには、そのコンピュータにAtrust Device Managerがインストールされていることと、クライアントがAtrust Device Managerの管理対象グループに追加されていることを確認します。

クライアントからスナップショットを取得するには、以下を実行してください。

1. Atrust Client Setupで、[**System**] > [**Snapshot**] の順にクリックします。



2. [Snapshot] セクションで、ドロップダウンメニューをクリックして、スナップショットを保存する場所を選択します。 [**Network**] と [**USB**] の2つのオプションがあります。

   - スナップショットファイルセットをリモートコンピュータに保存するには、[**Network**] を選択してください。
   - ローカルに接続されたUSBフラッシュドライブにスナップショットファイルセットを保存するには、[**USB**] を選択してください。

3. スナップショットの目的の説明を入力し、そのタイプを [**Deployment**] または [**Backup**] を選択します。

チェック

- 一括デプロイメント用のスナップショットを取ると（デプロイメントが選択されます）、スタートアップの動作がデフォルト（デフォルトの標準ユーザーアカウントで自動ログイン）にリセットされます。 詳細は、「1.7 はじめに」（8ページ）を参照してください。
- さらに、コンピュータセキュリティ識別子（SID）とコンピュータ名を含むシステム固有の情報はすべて、システム準備（**Sysprep**）ツールを自動的に実行することによってシステムイメージからリセットまたは削除されます。

4. スナップショットの撮影を開始するには、[**Apply**] をクリックします。
5. 確認を求めるメッセージが表示されます。 [**Yes**] をクリックして確認します。
6. プロセスが**自動**的に完了すると、システムが再起動します。

チェック

- プロセスが自動的に完了するのを待ちます。 スナップショットを作成するには数分が必要で、システムの再起動が必要です。 さらに、展開が選択されている場合、Sysprepプロセスはデスクトップに表示されず、バックグラウンドでのみ実行されます。

4.2.7 作成されたスナップショットを使用したシステムの導入

スナップショットは、ネットワーク経由またはUSBフラッシュドライブ上のリモートコンピュータに保存されます。 スナップショットの場所に応じて、ネットワークまたはUSBフラッシュドライブ経由でシステムイメージを展開できます。

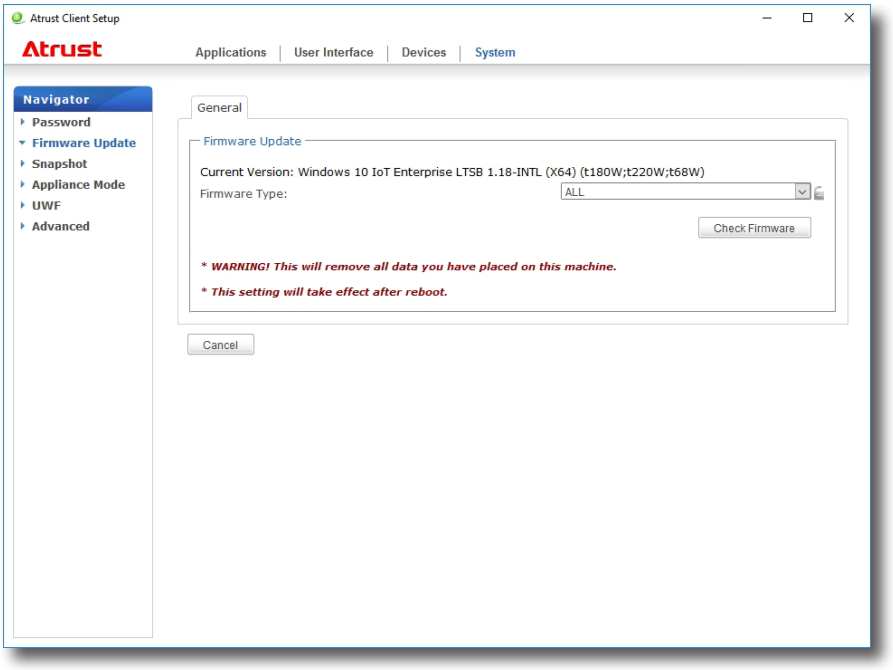
チェック

- スナップショットの取得方法の詳細は、「4.2.6 一括展開またはシステム復旧のためのスナップショットの作成」（42ページ）を参照してください。

リモートコンピュータ上のスナップショットを使用

リモートコンピュータ上のスナップショットを使用してt68Wにシステムイメージを展開するには、以下を実行してください。

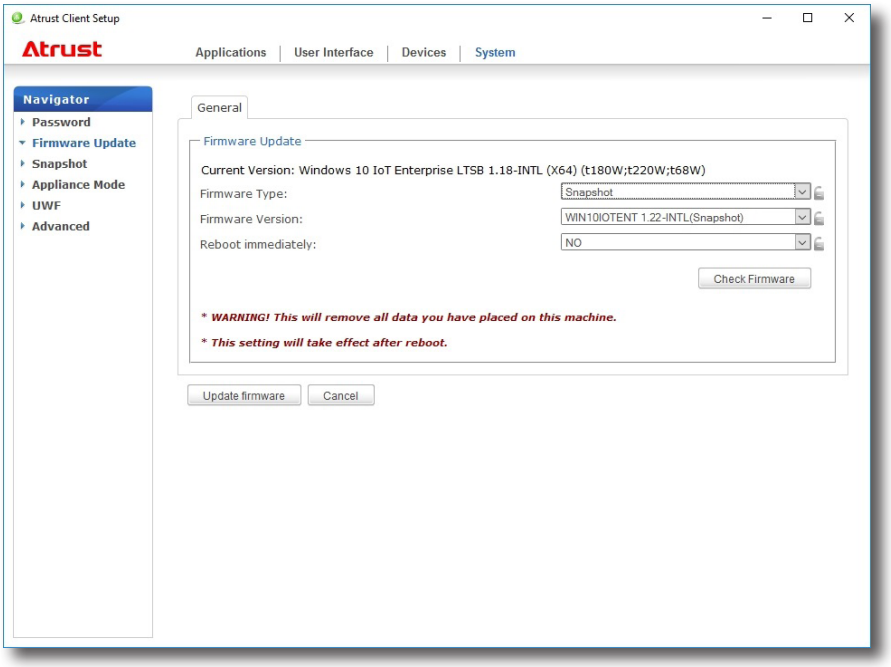
1. Atrust Client Setupで、[**System**] > [**Firmware Update**] の順にクリックします。



2. [Firmware Update] セクションで、[Firmware Type] ドロップダウンメニューをクリックして[スナップショット]を選択します。 システムは自動的にリモートコンピュータから [**Snapshot**] リストをダウンロードします。
3. 完了すると、スナップショットリストがロードされたことを知らせるメッセージが表示されます。

> **チェック**
>
> - リモートコンピュータに格納されたクライアントスナップショットは、Atrust Device Managerによって管理されます。 Atrust Device Managerを使用してクライアントスナップショットを管理する方法の詳細については、Atrust Device Managerのユーザーズマニュアルを参照してください。

4. [**OK**] をクリックして続行します。
5. ドロップダウンメニューをクリックして、目的のスナップショットとその他のオプションを選択します。



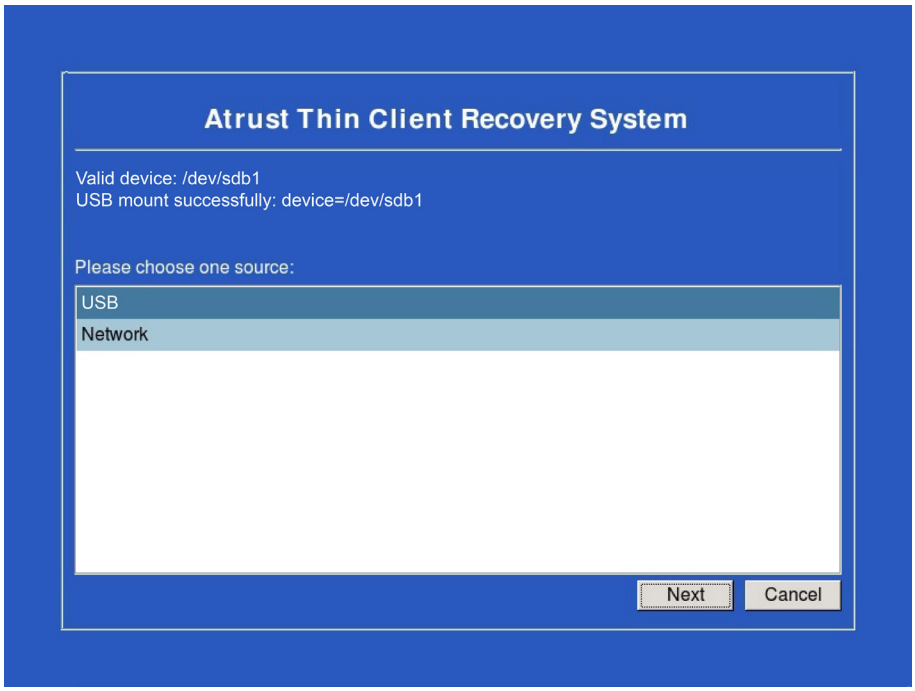
スナップショットを展開するためのオプション	
項目	**説明**
ファームウェアのバージョン	クリックして、スナップショットリストから目的のスナップショットを選択します。
すぐに再起動	ファームウェアを更新するためにすぐにシステムを再起動するか、後でシステムを手動で再起動するかを選択します。

6. [**Update firmware**] をクリックして選択を確定します。 再起動後、スナップショットの展開が開始されます。

*USB*フラッシュドライブ上のスナップショットで

USBフラッシュドライブにスナップショットを添付してt68Wにシステムイメージを展開するには、以下を実行してください。

1. USBフラッシュドライブをクライアントの空いているUSBポートに差し込みます。
2. クライアントを起動または再起動します。
3. 起動時に、[**F7**] キーを押してBoot Deviceメニューに入ります。
4. 接続されているUSBフラッシュドライブから起動する場合に選択します。
5. Atrustシンクライアントリカバリシステムが開始されました。
6. [**USB**] を選択し、[**Next**] をクリックして続行します。



7. 回復システムは、スナップショットをクライアントに展開する作業を開始します。
8. 完了後、[**Finish**] をクリックしてクライアントを再起動します。

4.2.8 作成されたスナップショットを使用したシステムの復元

スナップショットは、ネットワーク経由またはUSBフラッシュドライブ上のリモートコンピュータに保存されます。 スナップショットがどこにあるかによって、ネットワークまたはUSBフラッシュドライブからシステムイメージを復元できます。

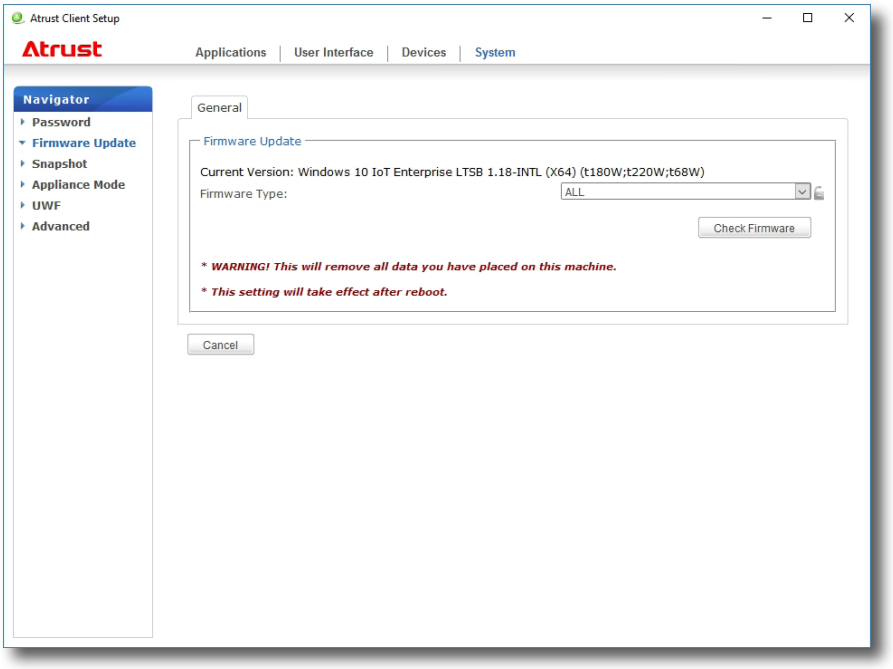
チェック

- スナップショットの取得方法の詳細は、「4.2.6 一括展開またはシステム復旧のためのスナップショットの作成」（42ページ）を参照してください。

リモートコンピュータ上のスナップショットを使用

リモートコンピュータ上のスナップショットを使用してt68Wにシステムイメージを復元するには、以下を実行してください。

1. Atrust Client Setupで、[**System**] > [**Firmware Update**] の順にクリックします。

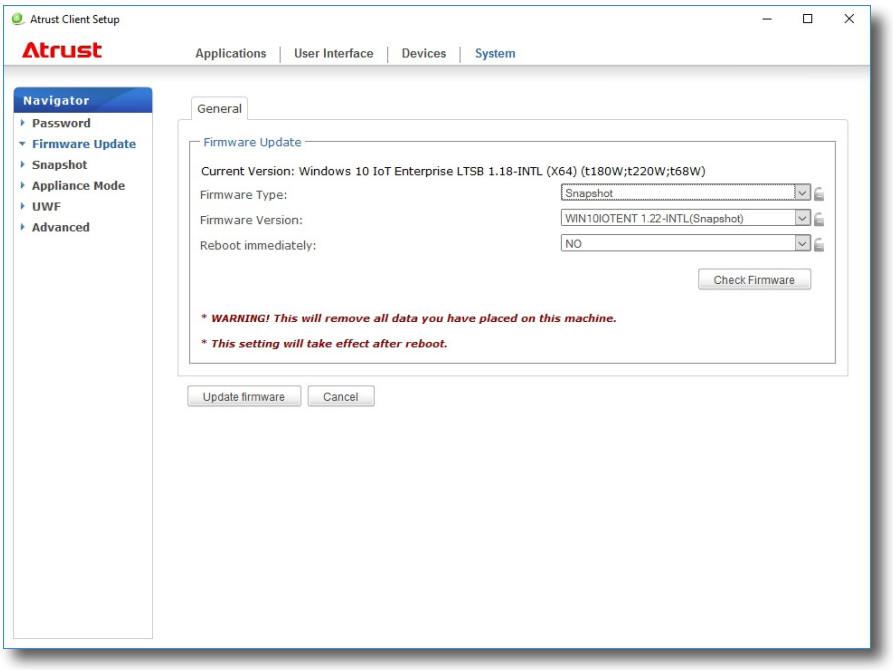


2. [Firmware Update] セクションで、[Firmware Type] ドロップダウンメニューをクリックして [**Snapshot**] を選択します。 システムは自動的にリモートコンピュータからスナップショットリストをダウンロードします。
3. 完了すると、スナップショットリストがロードされたことを知らせるメッセージが表示されます。

チェック

- リモートコンピュータに格納されたクライアントスナップショットは、Atrust Device Managerによって管理されます。 Atrust Device Managerでクライアントスナップショットを管理する方法の詳細については、Atrust Device Managerのユーザーズマニュアルを参照してください。

4. [**OK**] をクリックして続行します。
5. ドロップダウンメニューをクリックして、目的のスナップショットとその他のオプションを選択します。



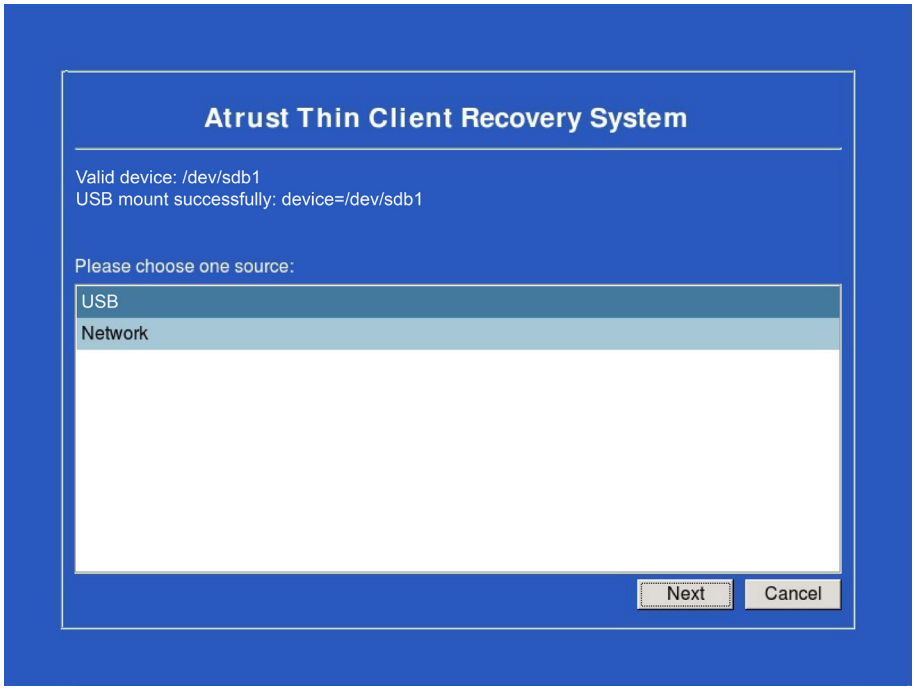
スナップショットを復元するためのオプション	
項目	**説明**
ファームウェアのバージョン	クリックして、スナップショットリストから目的のスナップショットを選択します。
すぐに再起動	ファームウェアを更新するためにすぐにシステムを再起動するか、後でシステムを手動で再起動するかを選択します。

6. [**Update firmware**] をクリックして選択を確定します。 再起動後、スナップショットの復元が開始されます。

*USB*フラッシュドライブ上のスナップショットで

USBフラッシュドライブにスナップショットを添付してt68Wにシステムイメージを展開するには、以下を実行してください。

1. USBフラッシュドライブをクライアントの空いているUSBポートに差し込みます。
2. クライアントを起動または再起動します。
3. 起動時に、[**F7**] キーを押してBoot Deviceメニューに入ります。
4. 接続されているUSBフラッシュドライブから起動する場合に選択します。
5. Atrustシンクライアントリカバリシステムが開始されました。
6. [**USB**] を選択し、[**Next**] をクリックして続行します。



7. 回復システムは、スナップショットをクライアントに復元することを開始します。
8. 完了後、[**Finish**] をクリックしてクライアントを再起動します。

4.2.9　アプライアンスモードの有効化または無効化

アプライアンスモードでは、Thin Clientを目的のMicrosoftリモートデスクトップ、Citrix ICA、VMware ViewまたはHorizon Viewセッションで直接起動できます。 セッションを終了すると、クライアントは設定された処理を実行します。

チェック

- シンクライアントには似ていますが異なるモードが2つあります。

番号	モード	説明
1	Appliance	クライアントは、目的のRDP / ICA / Viewセッションで直接起動し、セッションを終了した後に設定されたアクションを実行します。 使用可能なアクションは次のとおりです。 • 新しいセッションを再起動する • シンクライアントを再起動する • シンクライアントをオフにする
2	Autostart	クライアントは、目的のRDP / ICA / Viewセッションで直接起動し、セッションを終了した後に設定されたアクションを実行します。 使用可能なアクションは次のとおりです。 • ローカルのデスクトップに戻る • 新しいセッションを再起動する • シンクライアントを再起動する • シンクライアントをオフにする

- 上記のモードの詳細については、以下のセクションを参照してください。
  - ✧ 4.2.9（49ページ）　（アプライアンスモード）
  - ✧ 4.5.5（74ページ）　（RDPセッションの自動起動モード）
  - ✧ 4.5.8（99ページ）　（ICAセッションの自動起動モード）
  - ✧ 4.5.11（114ページ）　（ビューセッションの自動起動モード）

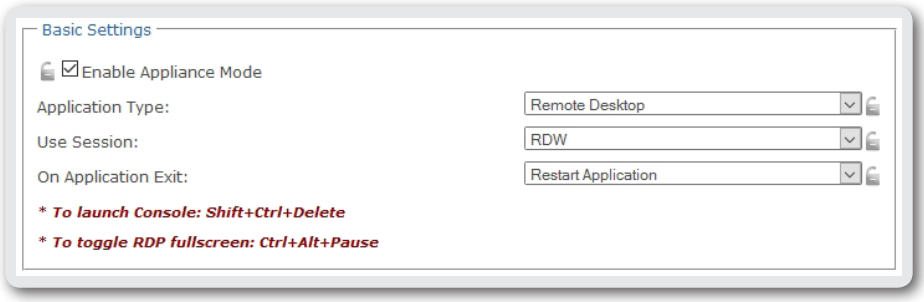
アプライアンスモードの有効化

アプライアンスモードを有効にするには、以下を実行してください。

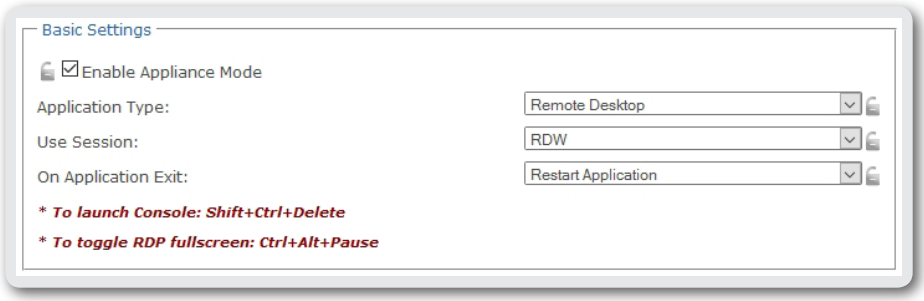
チェック

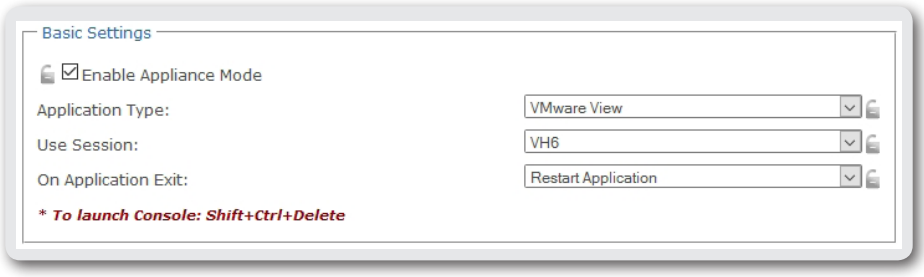
- アプリケーションタブの目的のMicrosoftリモートデスクトップ、Citrix ICA、VMware ViewまたはHorizon Viewセッションの接続設定を構成したことを確認します。 アプライアンスモードで使用するサービスタイプと接続設定エントリを指定する必要があります。 詳細な手順については、セクションを参照してください：
  - ✧ 「4.5.3 基本的なRDP接続設定の構成」（62ページ）
  - ✧ 「4.5.6 基本的なICA接続設定の設定」（87ページ）
  - ✧ 「4.5.9 VMware Viewの基本的な接続設定の構成」（110ページ）

1. Atrust Client Setupで、[**System**] > [**Appliance Mode**] をクリックします。
2. [**Enable Appliance Mode**] をクリックしてチェックします。
3. アプライアンスモードのその他の設定が表示されます。



4. ドロップダウンメニューをクリックして、**Citrix ICA**、**Remote Desktop**、または**VMware View**、およびそのタイプで利用可能な特定のサービスを選択します。





5. [**Save**] をクリックして選択内容を確定します。
6. 再起動後、アプライアンスモードになります。

チェック

- アプライアンスモードを無効にするか、アプライアンスモードでAtrust Client Setupにアクセスするには、「アプライアンスモードの無効化」（51ページ）を参照してください。

アプライアンスモードの無効化

アプライアンスモードを無効にするには、以下を実行してください。

1. アプライアンスモードでは、RDP / ICAセッションの全画面モードを終了するか、Viewセッション（仮想デスクトップ）からキーボードとマウスを離します。

   - RDPセッションの全画面モードを終了するには、**Ctrl** + **Alt** + **Pause** を押します。
   - ICAセッションのフルスクリーンモードを終了するには、上部にあるXenDesktopツールバーを使用します（フルスクリーンモードではない場合があります）。
   - Viewセッション（仮想デスクトップ）からキーボードとマウスを離すには、**Ctrl** + **Alt** を押します。

   チェック

   - Viewセッション（仮想デスクトップ）は、Viewセッション（仮想デスクトップ）からキーボードとマウスを離した後も、バックグラウンドで保持されます。

2. **Ctrl** + **Shift** + **Del** をクリックしてAtrust Client Setupを起動します。

   チェック

   - アプライアンスモードでは、ローカルデスクトップにアクセスできません。

3. Atrust Client Setupで、[**System**] > [**Appliance Mode**] をクリックします。
4. [**Enable Appliance Mode**] をオフにしてから、[**Save**] をクリックして変更を適用します。
5. 現在のRDP / ICA / Viewセッションに戻る：

   - 現在のRDP / ICAセッションに戻るには、現在のRDP / ICAセッションを選択して復元するために **Alt** + **Tab**キー（**Alt** キーを押しながらTabキーを押し、異なるアイテム間で切り替える）を使用します。
   - 現在のViewセッションに戻るには、バックグラウンドでViewセッション（仮想デスクトップ）の任意の場所をクリックします。

6. 現在のRDP / ICA / Viewセッションからログオフします。
7. クライアントがシャットダウンする可能性があります。 クライアントを手動で再起動します。

4.2.10 UWFの設定（Unified Write Filter）

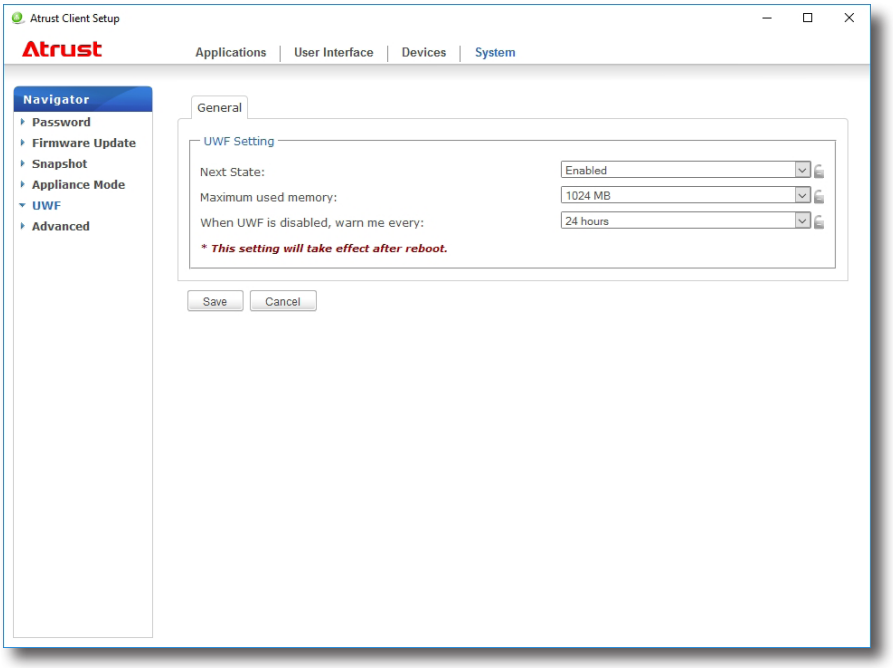
t68WはデフォルトでUWF対応です。 ユニファイド書き込みフィルタ（UWF）は、セクタベースの書き込みフィルタで、保護されたボリュームへのすべての書き込み試行をインターセプトし、それらの書き込み試行をRAMキャッシュにリダイレクトします。 UWFでは、すべてのシステム変更は変更が行われたセッションにのみ影響します。 再起動後、すべての変更は破棄されます。

重要

- UWF機能は工場出荷時のデフォルトで有効になっています。 ACS設定の変更を除いて、セッションで行われたすべての変更は、システムの再起動後も保持されません。 システムを変更する前に、ここで目的の設定を選択してください。
- タスクバーの通知領域にあるアイコンは、システムの現在のUWF状態を示します。 詳細は、このセクションの最後の説明を参照してください。

UWF設定を構成するには、以下を実行してください。

1. Atrust Client Setupで、[**System**] > [**UWF**] をクリックします。
2. [State] ドロップダウンメニューをクリックして、UWF機能を有効/無効にします。



3. 必要に応じて他のオプションをクリックして選択します。

UWFオプション	
項目	**説明**
次の状態	UWFを有効/無効にする場合にクリックします。 切り替えには再起動が必要です。
最大使用メモリ	UWFに使用される最大メモリをクリックして選択します。
UWFが無効になっている場合は、毎週警告してください	UWFが無効になっているときに、システムが警告する頻度を選択するためにクリックします。

4. [**Save**] をクリックして選択内容を確定します。
5. 変更を有効にするには、システムを再起動する必要があります。

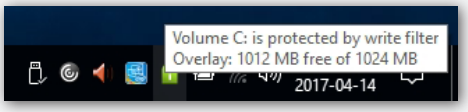
重要

- UWFを有効または無効にするには、システムを再起動する必要があります。 タスクバーの通知領域には、システムの現在のUWF状態を示すアイコンが表示されます。 次の表に、各アイコンの説明を示します。

アイコン	名称	説明
	グリーンロック	UWFは現在有効です。 ACS設定の変更を除いて、現在のセッションでシステムに加えられた他のすべての変更は、システムの再起動後は保持されません。
	オレンジロック	UWF状態が変更され、システムの再起動後に有効になります。
	赤いロック	UWFは現在無効になっています。

ヒント

- UWFを有効にすると、UWFアイコンの上にマウスポインタを移動できます。現在UWFの空きメモリ（オーバーレイ）を確認してください。 以下のようなツールチップが表示されます。



チェック

- シンクライアントデバイスとして、t68Wは主にサーバー上のリモートまたは仮想デスクトップへのアクセス用です。 制限付きで保護された（UWF対応）ハード・ディスク・スペースでは、t68Wにデータを保管することは推奨されません。 代わりに、リモート/仮想デスクトップ、リムーバブルストレージデバイス、またはネットワーク上のストレージスペースを使用できます。
- 保護されたボリュームにファイルをコピーする必要がある場合は、そのサイズが空きメモリ（オーバーレイ）の容量よりも小さいことを確認してください。 そうしないと、システムが予期しない結果になるか、応答しなくなる可能性があります。

4.2.11 自動登録を有効または無効

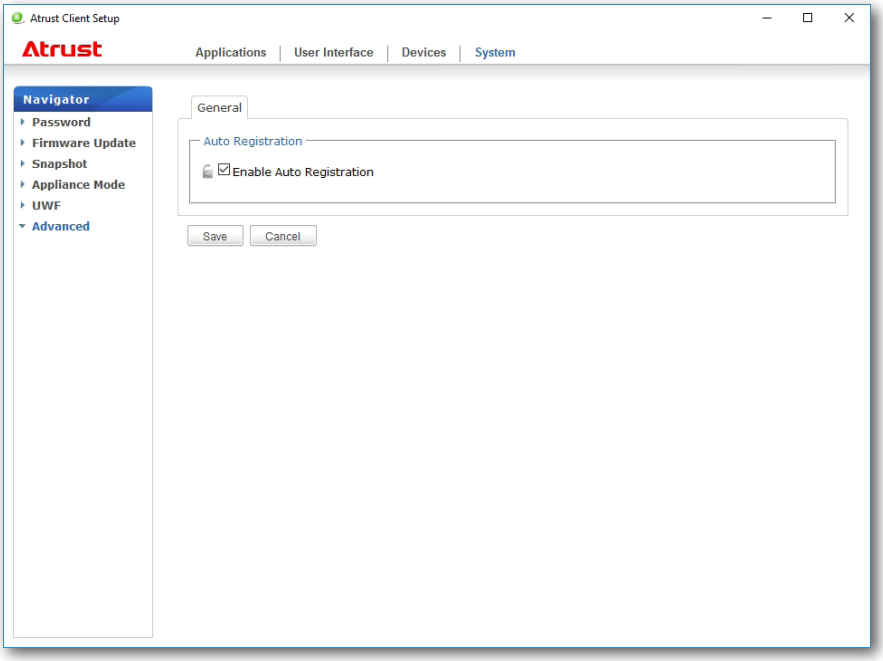
自動登録を使用すると、シンクライアントは、オンラインのときにAtrust Device Managerに自動的に登録してから、Atrust Device Managerで管理することができます。

チェック

- この機能を有効にするには、シンクライアントとターゲットのAtrust Device Managerの両方で自動登録を有効にする必要があります。 さらに、ネットワーク上のDHCPまたはDNSサーバーの一部の構成が必要です。 詳細は、Atrust Device Managerのユーザーズマニュアルを参照してください。
- デフォルトでは、シンクライアント側で自動登録が有効になっており、Atrustデバイスマネージャ。

シン・クライアントの自動登録を有効または無効にするには、以下を実行してください。

1. Atrust Client Setupで、[**System**] > [**Advanced**] をクリックします。
2. 自動登録を有効/無効にするには、[**Enable Auto Registration**] をオンまたはオフにします。



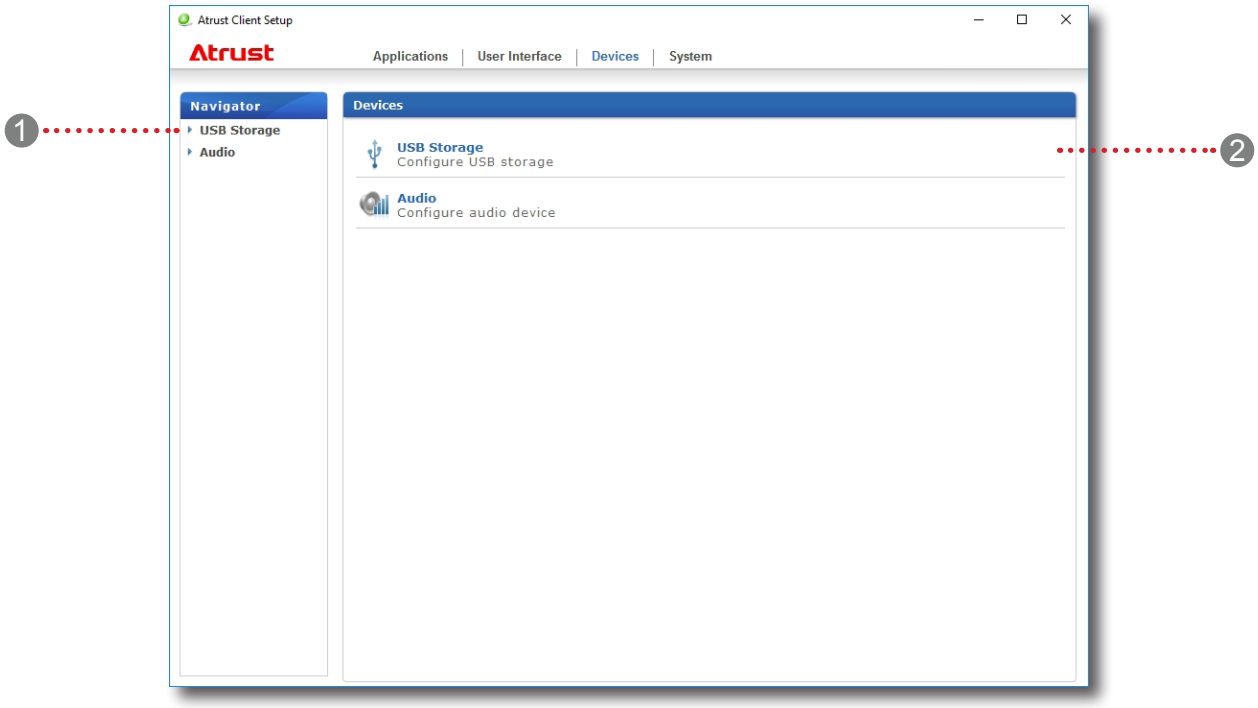
3. 適用するには [**Save**] をクリックします。

4.3 外部デバイス設定の構成

4.3.1 デバイスタブの概要

[**Devices**] タブでは、クライアントの外部デバイスの設定を構成できます。 [**Devices**] タブで使用可能な設定にアクセスするには、[Atrust Client Setup] のタブをクリックします。

デバイスタブの概要



インタフェース要素		
番号	**名称**	**説明**
1	ナビゲーション領域	[**Devices**] タブの設定項目をクリックして選択します。
2	構成領域	設定項目を選択したときの設定値を設定します。

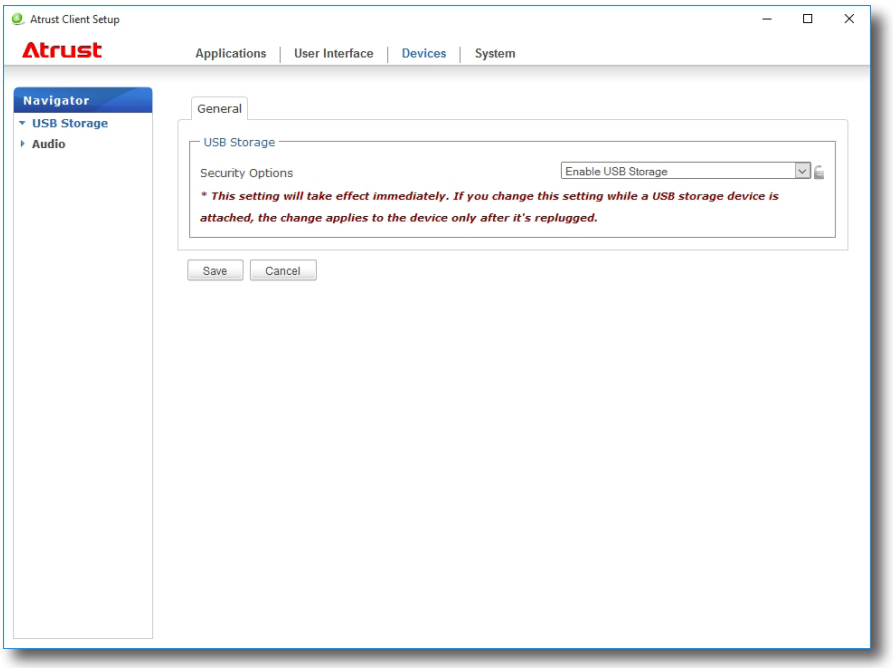
4.3.2 使用可能なタスク一覧

タブ	設定	アイコン	説明	参照先	ページ
デバイス	USBストレージ		USBストレージデバイスの設定を行う場合にクリックします。	4.3.3	56
	オーディオ		クリックすると、オーディオデバイスの設定を行います。	4.3.4	57

4.3.3 USBストレージデバイスの設定を構成

USBストレージデバイスの設定を行うには、以下を実行してください。

1. Atrust Client Setupで、[**Devices**] > [**USB Storage**] をクリックします。



2. ドロップダウンメニューをクリックして、希望する設定を選択します。 **Enable USB Storage**、**Read-Only Access**、および**Disable USB Storage**の3つのオプションを使用できます。

チェック

- [**Enable USB Storage**] を選択すると、リモート/仮想デスクトップセッションで**マップ**されたUSBストレージデバイスを使用できる場合、**Applications**タブのRDP / ICA接続エントリの設定が影響を受ける可能性があります。 詳細は、セクションを参照してください：
  - ✧ 「4.5.5 高度なRDP接続設定の構成」（74ページ）
  - ✧ 「4.5.8 高度なICA接続設定の構成」（99ページ）
- [**Disable USB Storage**] が選択されている場合、Citrix ICAおよびVMwareView / Horizon Viewのセッションでは、**リダイレクト**によってローカルに接続されたUSBストレージデバイスをユーザーが使用できるようになる場合があります。 仮想デスクトップセッションでUSBストレージデバイスの使用を実際に防止するには、CitrixとVMwareのサービス配信環境の一部の設定が必要です。

3. [**Save**] をクリックして変更を保存します。

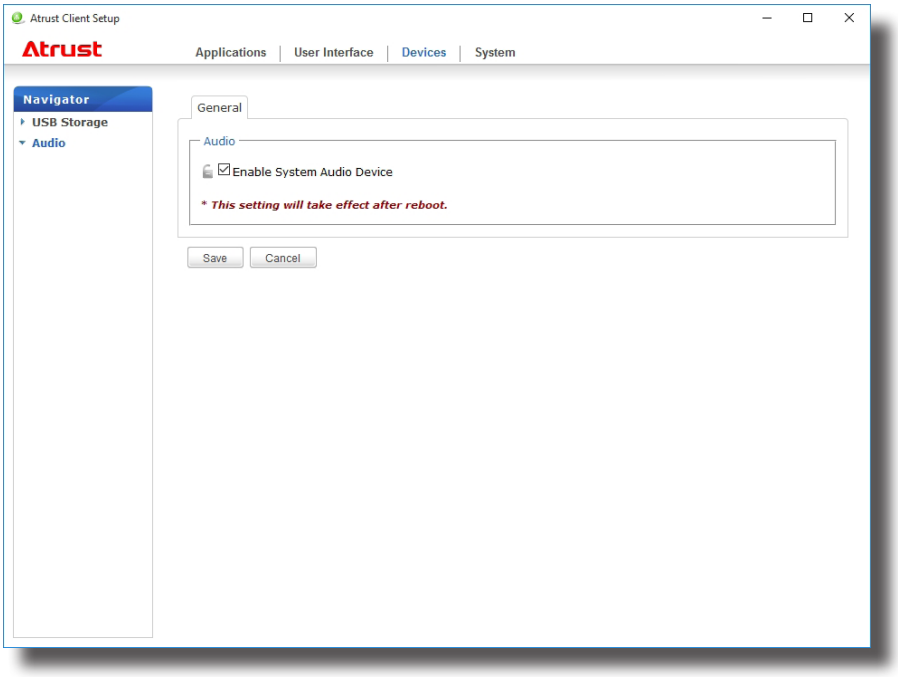
4.3.4　接続されたオーディオデバイスの無効化または有効化

付属のオーディオデバイスを無効/有効にするには、以下を実行してください。

チェック

- ローカルに接続されたオーディオデバイスを無効にすると、クライアントユーザーはRDP / ICA / Viewセッションでこれらのデバイスでオーディオ再生または録音を実行することはできません。
- RDP / ICA / Viewセッションでローカルオーディオデバイスでオーディオ再生または録音を実行するには、ここにローカルに接続されたオーディオデバイス（**デバイス**タブの**オーディオ設定**項目）を有効にし、RDP / ICA /接続設定を表示します。 詳細な手順については、セクションを参照してください。
  - ✧ 「4.5.5 高度なRDP接続設定の構成」（74ページ）
  - ✧ 「4.5.8 高度なICA接続設定の構成」（99ページ）
  - ✧ 「4.5.11 詳細ビュー接続設定の構成」（114ページ）

1. Atrust Client Setupで、[**Devices**] > [**Audio**] の順にクリックします。



2. [**Enable System Audio Device**] にするチェックボックスをオンまたはオフにします。
3. [**Save**] をクリックして選択を確定します。

チェック

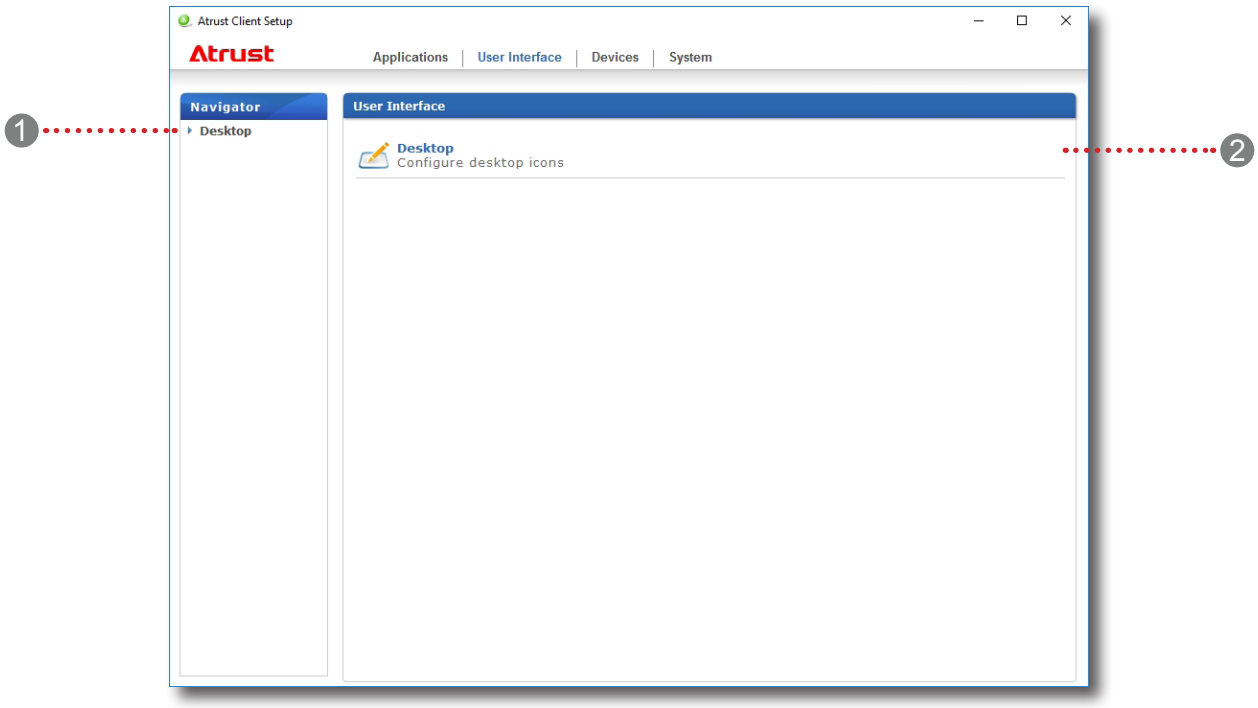
- この変更は、クライアントが再起動されるまで有効になりません。

4.4 ユーザーインターフェイス設定の構成

4.4.1 ユーザーインターフェイスタブの概要

[**User Interface**] タブでは、クライアントのユーザーインターフェイスの設定を構成できます。 [**User Interface**] タブの使用可能な設定にアクセスするには、[Atrust Client Setup] タブをクリックします。

ユーザーインターフェイスタブの概要



インタフェース要素		
番号	**名称**	**説明**
1	ナビゲーション領域	[**User Interface**] タブの設定項目をクリックして選択します。
2	構成領域	設定項目を選択したときの設定値を設定します。

4.4.2 使用可能なタスク一覧

タブ	設定	アイコン	説明	参照先	ページ
ユーザーインターフェース	デスクトップ		クリックすると、クイックサービスアクセス用の標準デスクトップショートカットの表示を設定します。	4.4.3	59

4.4.3 クイックアクセスの標準デスクトップショートカットの表示の設定

[**Desktop**] 設定を使用すると、サービスのクイックアクセス用の標準デスクトップショートカットを表示または非表示にすることができます。 Citrix XenApp / XenDesktop / VDI-in-a-Box、Microsoft Remote Desktop / Remote Application (RemoteApp)、およびリモートデスクトップ/リモートアプリケーションの迅速なサービスアクセスのために、**Citrix Receiver**、**Remote Desktop Connection**、および**VMware Horizon View Client**の3つの標準デスクトップショートカットを利用できます。 VMware View / VMwareのホライゾンビューー。


Remote Desktop Connection


Citrix Receiver


VMware Horizon View Client

ヒント

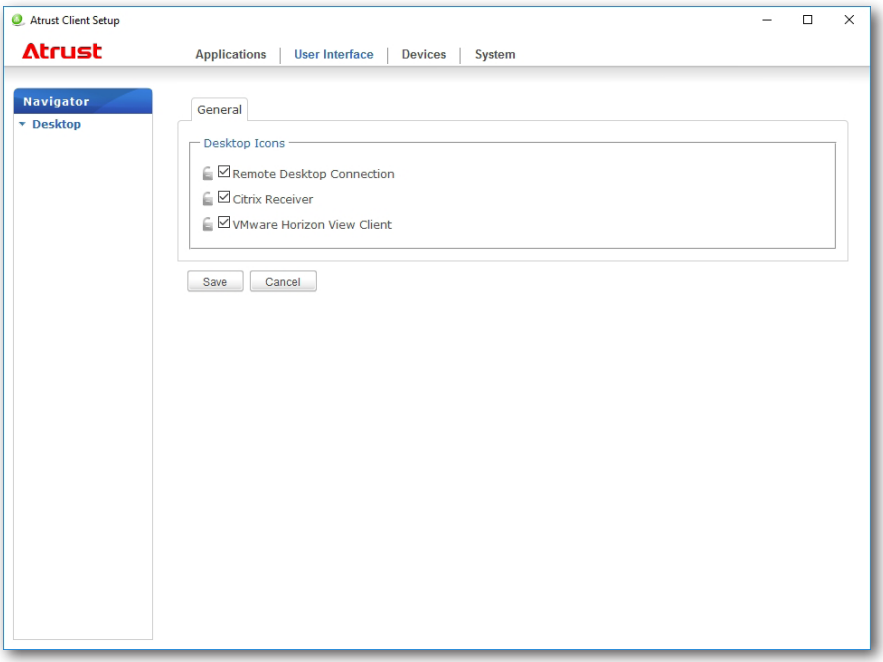
- これらの標準のデスクトップショートカットを使用すると、サービスにすばやくアクセスできます。 詳しい説明は第3章 「入門」（17ページ）を参照してください。

チェック

- デスクトップショートカットをカスタマイズして、迅速なサービスアクセスを実現することもできます。 デスクトップショートカットの作成方法とカスタマイズ方法については、「4.5 サービスアクセス設定の構成」（60ページ）を参照してください。

クイックサービスへのアクセスのための標準のデスクトップショートカットを表示または非表示にするには、以下を実行してください：

1. Atrust Client Setupで、[**User Interface**] > [**Desktop**] の順にクリックします。



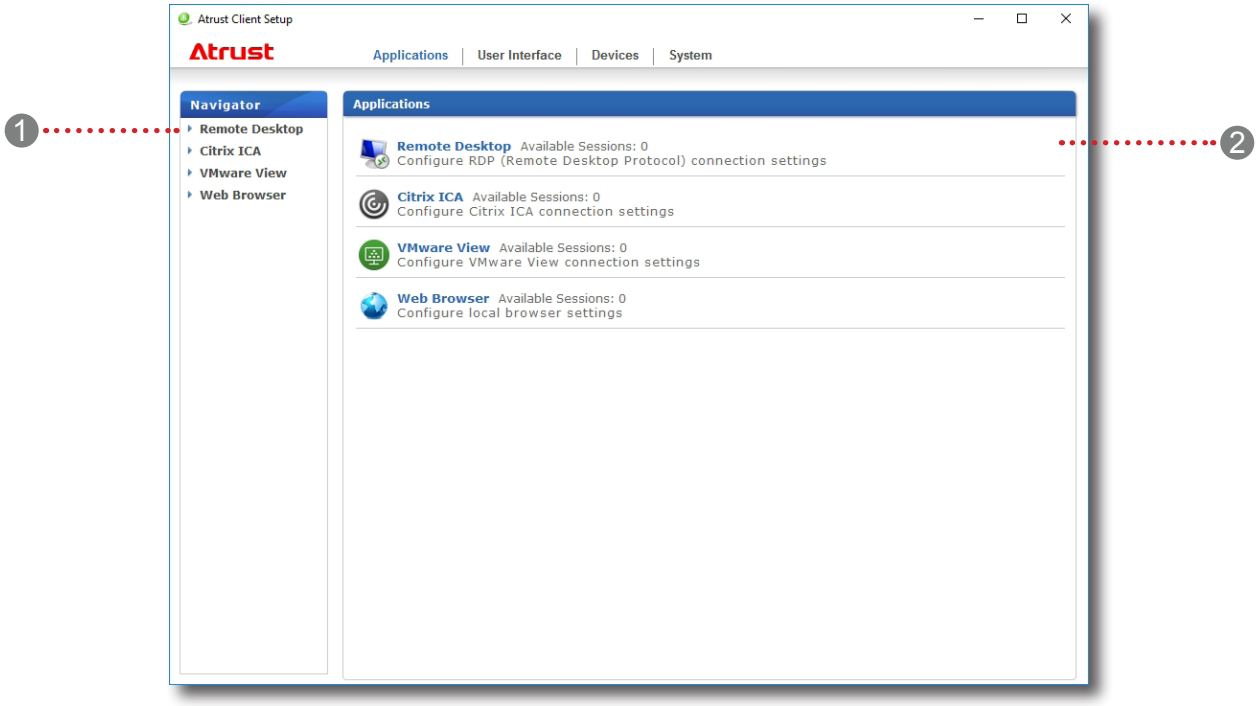
2. クリックして、**Remote Desktop Connection**、**Citrix Receiver**、または**VMware Horizon View Client**をオンまたはオフにします。
3. 適用するには [**Save**] をクリックします。

4.5 サービスアクセス設定の構成

4.5.1 アプリケーションタブの概要

[**Applications**] タブでは、クライアントのサービスアクセスの設定を構成できます。 [**Applications**] タブの使用可能な設定にアクセスするには、[Atrust Client Setup] タブをクリックします。

アプリケーションタブの概要



インタフェース要素		
番号	**名称**	**説明**
1	ナビゲーション領域	[**Applications**] タブの設定項目をクリックして選択するか、選択した設定項目の設定項目を選択します。
2	構成領域	設定項目または項目が選択されたときに設定値を設定します。

4.5.2　使用可能なタスク一覧

タブ	設定	アイコン	説明	参照先	ページ
アプリケーション	Remote Desktop		クリックすると、RDP（リモートデスクトッププロトコル）接続設定が構成され、RDPセッションのデスクトップにアクセスショートカットが作成されます。	4.5.3 4.5.4 4.5.5	62 69 74
	Citrix ICA		Citrix ICA（Independent Computing Architecture）接続設定を構成し、ICAセッションのデスクトップにアクセスショートカットを作成する場合にクリックします。	4.5.6 4.5.7 4.5.8	87 95 99
	VMware View		VMware Viewの接続設定を構成する場合はクリックし、Viewセッションの場合はデスクトップにアクセスのショートカットを作成します。	4.5.9 4.5.10 4.5.11	110 112 114
	ウェブブラウザ		クリックすると、ブラウザセッションの設定を行い、ブラウザセッションのデスクトップにアクセスショートカットを作成します。	4.5.12	116

4.5.3 基本的なRDP接続設定の構成

リモートデスクトップ設定では、RDP（リモートデスクトッププロトコル）接続設定を構成し、デスクトップ上にショートカットを作成したり、リモートデスクトップサービスの開始画面を作成したりすることができます。これらのショートカットを使用するだけで、仕事のためのサービスにアクセスできます。

チェック

- Microsoftリモートデスクトップサービスの詳細については、MicrosoftのWebサイト www.microsoft.com を参照してください。

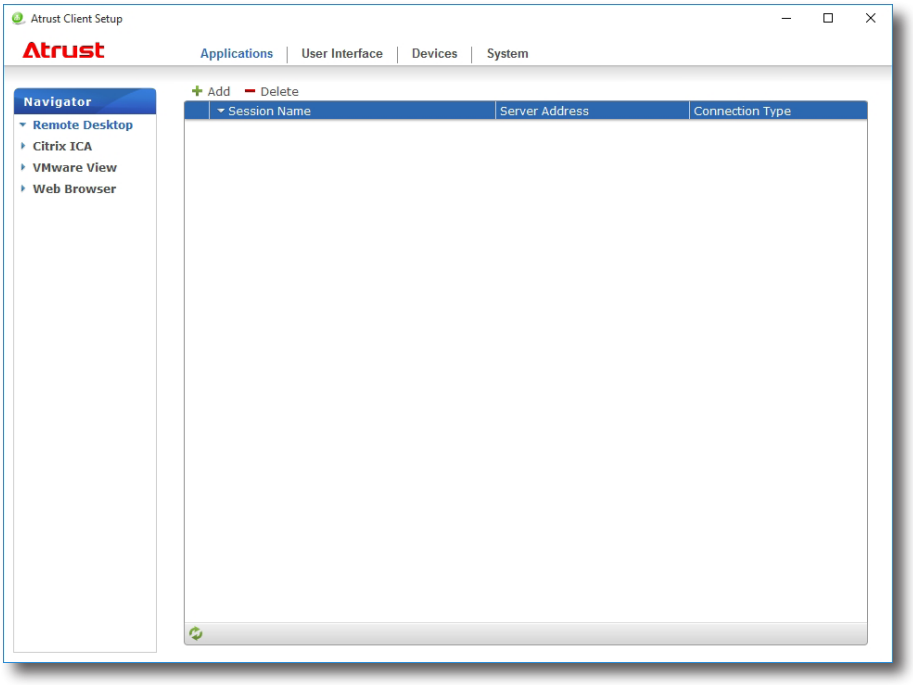
次の3つの接続タイプを使用できます。

接続タイプ	説明	ページ
リモートデスクトップ	リモートデスクトップ/アプリケーションにアクセスする場合に選択します。	63
リモートWebアクセス	Webブラウザを使用してリモートデスクトップ/アプリケーションにアクセスする場合に選択します。	65
Webフィード	公開された開始画面タイルを使用してリモートアプリケーションにアクセスする場合に選択します。	67

接続の種類：リモートデスクトップ

リモートデスクトップ接続タイプのRDP接続設定をすばやく設定するには、以下を実行してください。

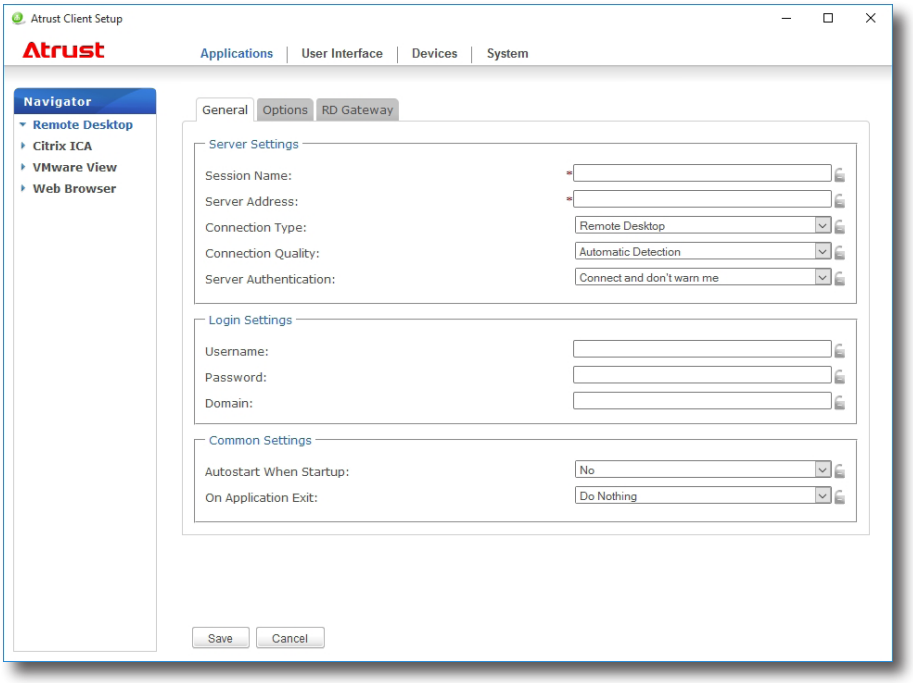
1. Atrust Client Setupで、[**Applications**] > [**Remote Desktop**] をクリックします。



2. RDP ConnectionリストがConfigurationエリアに表示されます。

> **チェック**
>
> - エントリを作成していない場合、RDP接続リストは空になります。

3. RDP接続リストの上部にある [**Add**] をクリックして、RDP接続の新しいエントリを作成します。



4. [**General**] サブタブで、[Server Settings] セクションの下にセッション名とサーバー/仮想マシンのアドレスを入力します。

チェック

- 赤いアスタリスクは必須フィールドを示します。
- リモートコンピュータは、物理サーバーまたは仮想マシンにすることができます。 詳細については、MicrosoftのWebサイト（www.microsoft.com または support.microsoft.com）を参照してください。

5. [**Save**] をクリックして、このRDP接続エントリを追加します。
6. リモートデスクトップ接続のショートカットは、デスクトップ上に自動的に作成されます。

チェック

- サービスの提供計画とサーバーの構成によっては、サービスアクセスのためのその他の高度なRDP接続設定を構成する必要があります。 その他の設定については、「4.5.5 高度なRDP接続設定の構成」（74ページ）を参照してください。

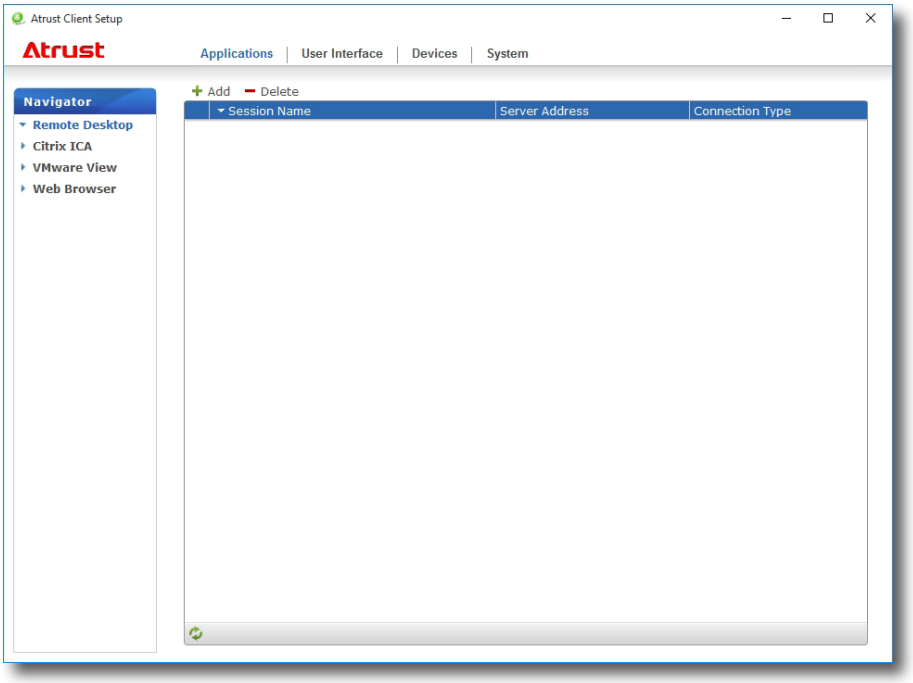
接続タイプ：リモート*Web*アクセス

リモートWebアクセス接続タイプのRDP接続設定をすばやく構成するには、次の操作を行います。

チェック

- t68WはWindows Server 2012 R2に基づくRD Webアクセスのみをサポートします。 Windows Server 2008 R2ベースはサポートされていません。

1. Atrust Client Setupで、[**Applications**] > [**Remote Desktop**] をクリックします。

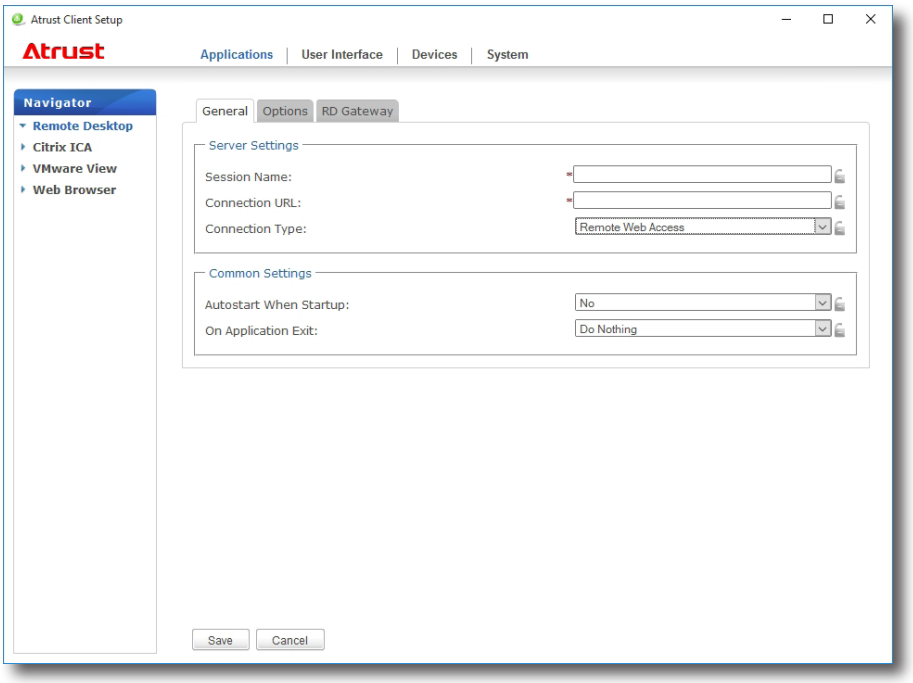


2. RDP ConnectionリストがConfigurationエリアに表示されます。

チェック

- エントリを作成していない場合、RDP接続リストは空になります。

3. RDP接続リストの上部にある [**Add**] をクリックして、RDP接続の新しいエントリを作成します。



4. [**General**] サブタブで、[Connection Type] ドロップダウン・メニューをクリックして [**Remote Web Access**] を選択します。
5. Webベースのリモートアプリケーション/デスクトップにアクセスできるセッション名と接続URLを入力します。

チェック

- 赤いアスタリスクは必須フィールドを示します。
- 適切な接続URLについては、IT管理者に相談してください。

6. [**Save**] をクリックして、このRDP接続エントリを追加します。
7. リモートWebアクセス接続のショートカットは、デスクトップ上に自動的に作成されます。

チェック

- サービスの提供計画とサーバーの構成によっては、サービスアクセスのためのその他の高度なRDP接続設定を構成する必要があります。 その他の設定については、「4.5.5 高度なRDP接続設定の構成」（74ページ）を参照してください。

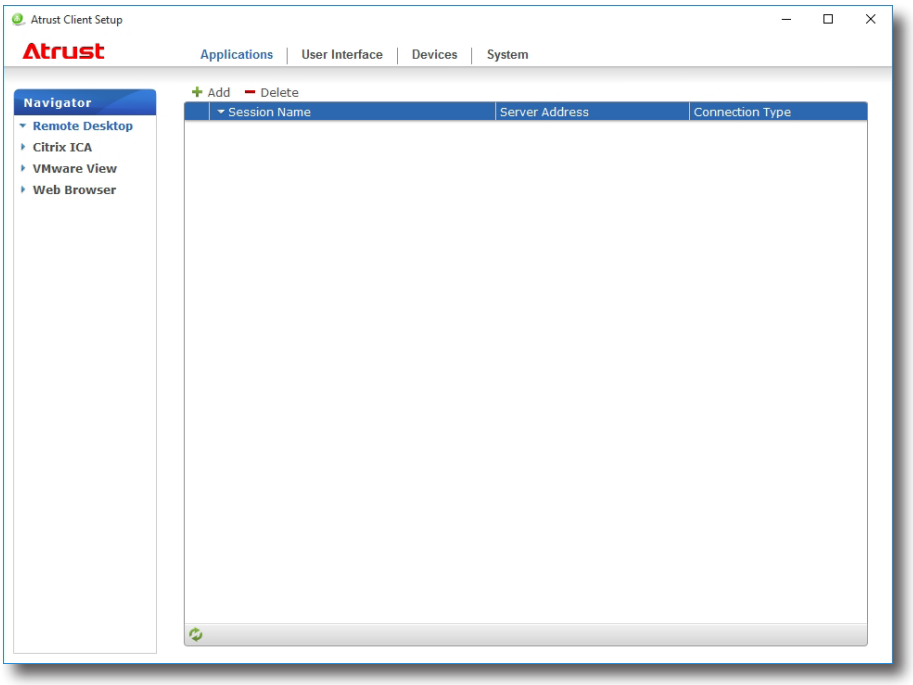
接続の種類：ウェブフィード

Webフィード接続タイプのRDP接続設定をすばやく設定するには、以下を実行してください。

チェック

- t68Wは、Windows Server 2012 R2に基づくRD Webフィードのみをサポートします。Windows Server 2008 R2ベースはサポートされていません。

1. Atrust Client Setupで、[**Applications**] > [**Remote Desktop**] をクリックします。

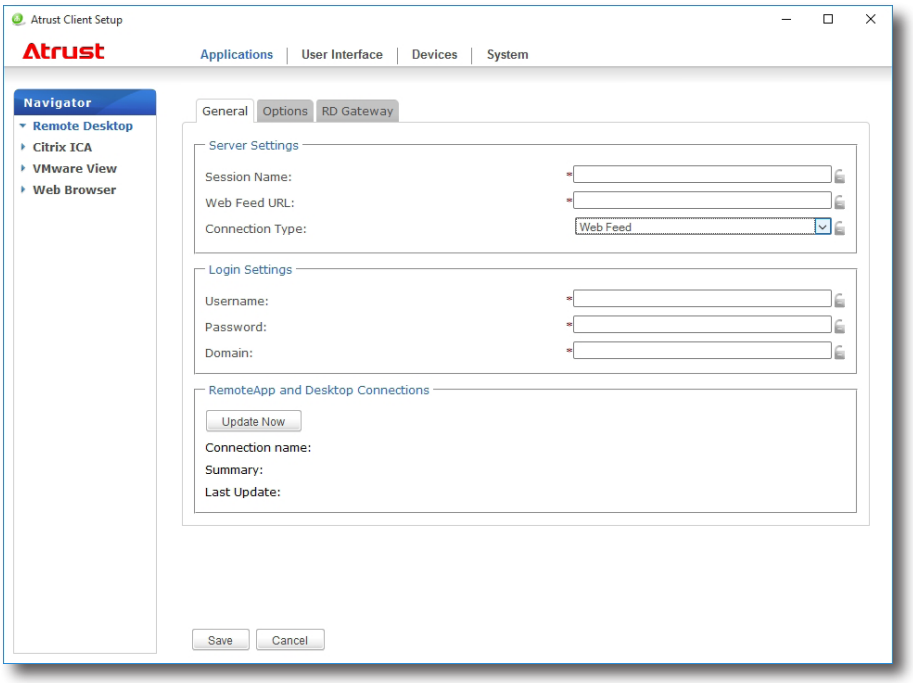


2. RDP ConnectionリストがConfigurationエリアに表示されます。

チェック

- エントリを作成していない場合、RDP接続リストは空になります。

3. RDP接続リストの上部にある [**Add**] をクリックして、RDP接続の新しいエントリを作成します。



4. [**General**] サブタブで、[Connection Type] ドロップダウンメニューをクリックして [**Web Feed**] を選択します。
5. セッション名、リモートアプリケーションがアクセスできるWebフィードURL、およびWebフィードの資格情報を入力します。

> **チェック**
> - 赤いアスタリスクは必須フィールドを示します。
> - 適切なWebフィードURLについては、IT管理者に相談してください。

6. [RemoteAppとDesktop Connections] セクションで [**Update Now**] をクリックします。 完了後、そのセクションに結果が表示されます。

7. [**Save**] をクリックして、このRDP接続エントリを追加します。
8. Webフィードのアプリケーションタイルは、[Start] 画面で自動的に作成されます。

> **チェック**
> - サービスの提供計画とサーバーの構成によっては、サービスアクセスのためのその他の高度なRDP接続設定を構成する必要があります。 その他の設定については、「4.5.5 高度なRDP接続設定の構成」（74ページ）を参照してください。

4.5.4　リモートデスクトップサービスへのアクセス

接続の種類：リモートデスクトップ

リモートデスクトップサービスにアクセスするには、以下を実行してください。

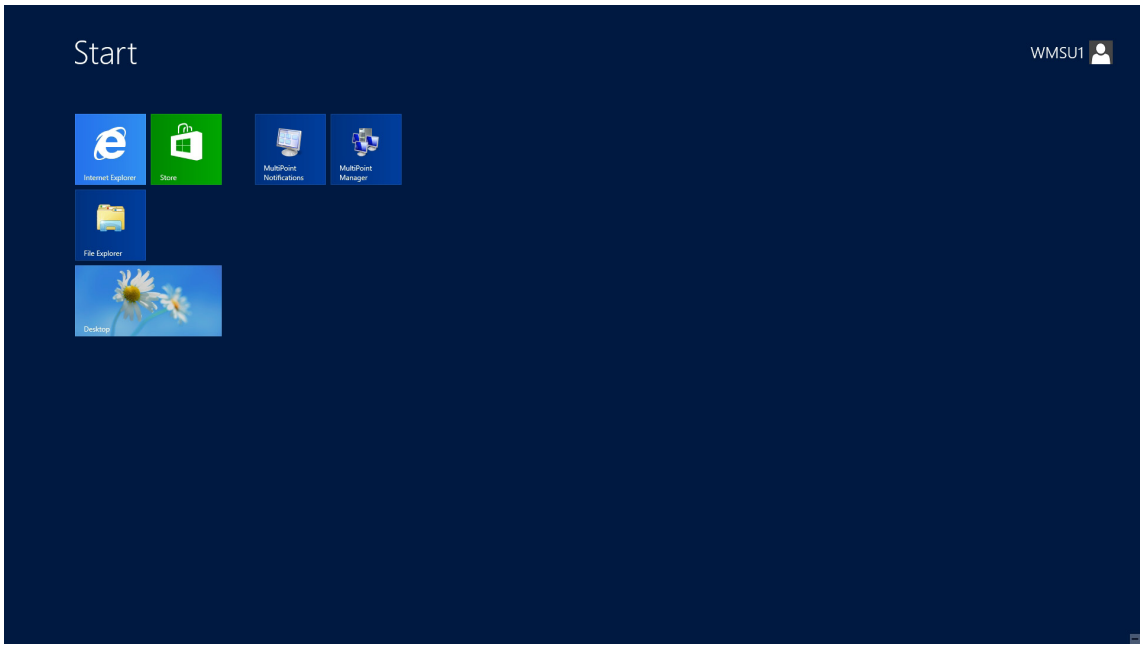
1. 作成された（カスタマイズされた）ショートカットをデスクトップ上でダブルクリックします。

> **チェック**
>
> - 標準のデスクトップショートカット「リモートデスクトップ接続」を使用して、リモートデスクトップサービスにアクセスすることもできます。 この標準ショートカットを使用してサービスにアクセスする方法の詳細については、 「3.3 Microsoftリモートデスクトップサービスへのアクセス」（26ページ）のセクションを参照してください。

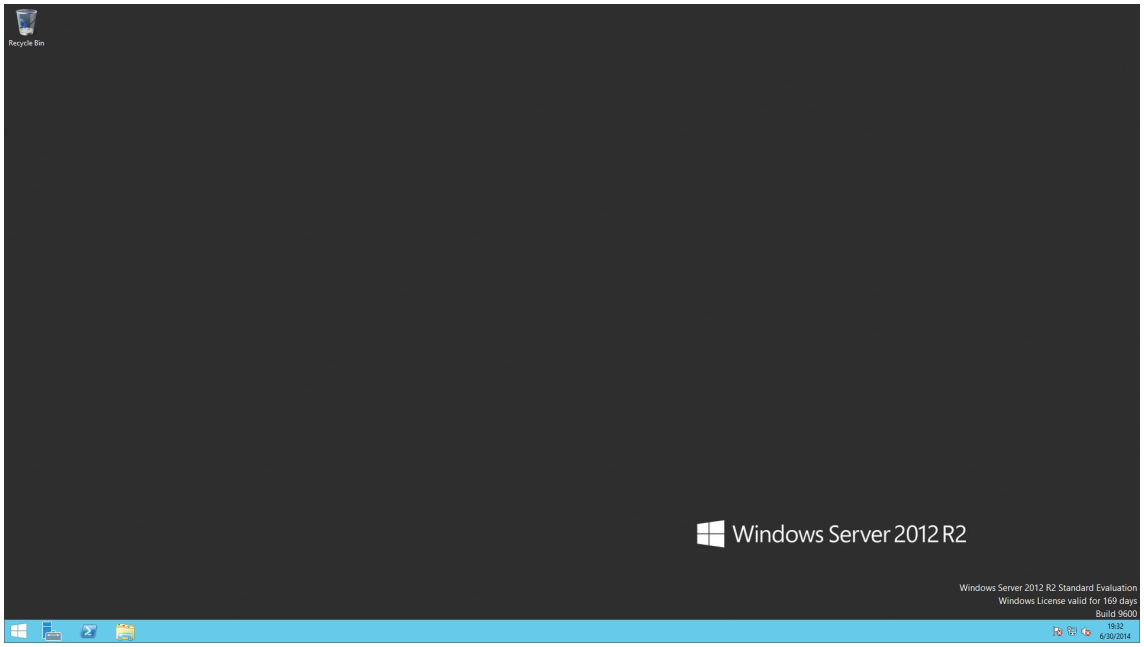
2. 画面の指示に従って、必要に応じて必要な資格情報を入力します。
3. 目的のリモートデスクトップがデスクトップにフルスクリーンで表示されます（デフォルト）。

> **チェック**
>
> - リモートデスクトップの接続タイプを使用すると、**アプリケーションのみ**のセッションを起動することもできます。 フルデスクトップではなく、特定のアプリケーションのみが起動されます。 詳細は「4.5.5 高度なRDP接続設定の構成」（74ページ）を参照してください。

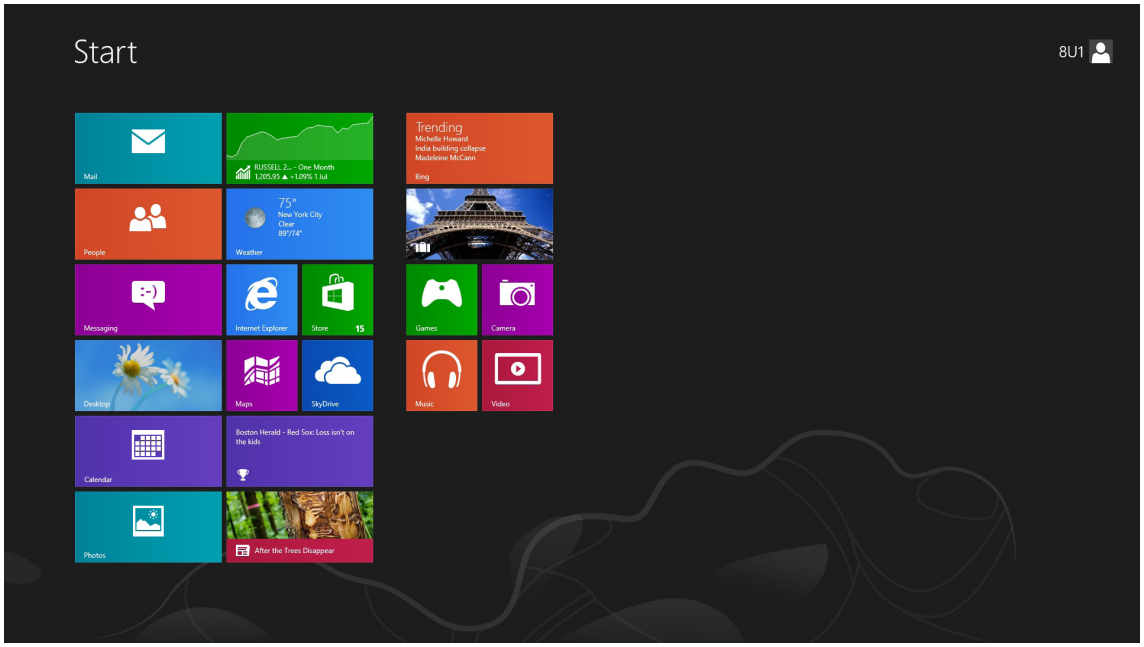
例：Windows MultiPoint Server 2012



例：Windows Server 2012



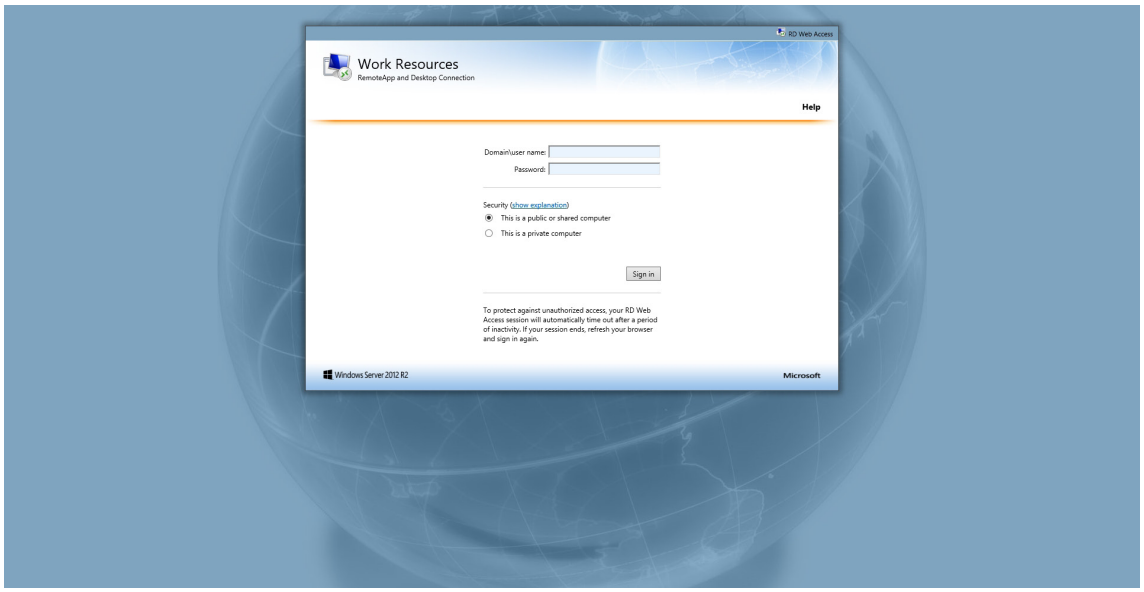
例：Windows 8 Enterprise



接続タイプ：リモート*Web*アクセス

リモートアプリケーション/デスクトップにアクセスするには、以下を実行してください。

1. 作成したショートカットをデスクトップ上でダブルクリックします。
2. 資格情報の入力を求めるウィンドウが表示されます。

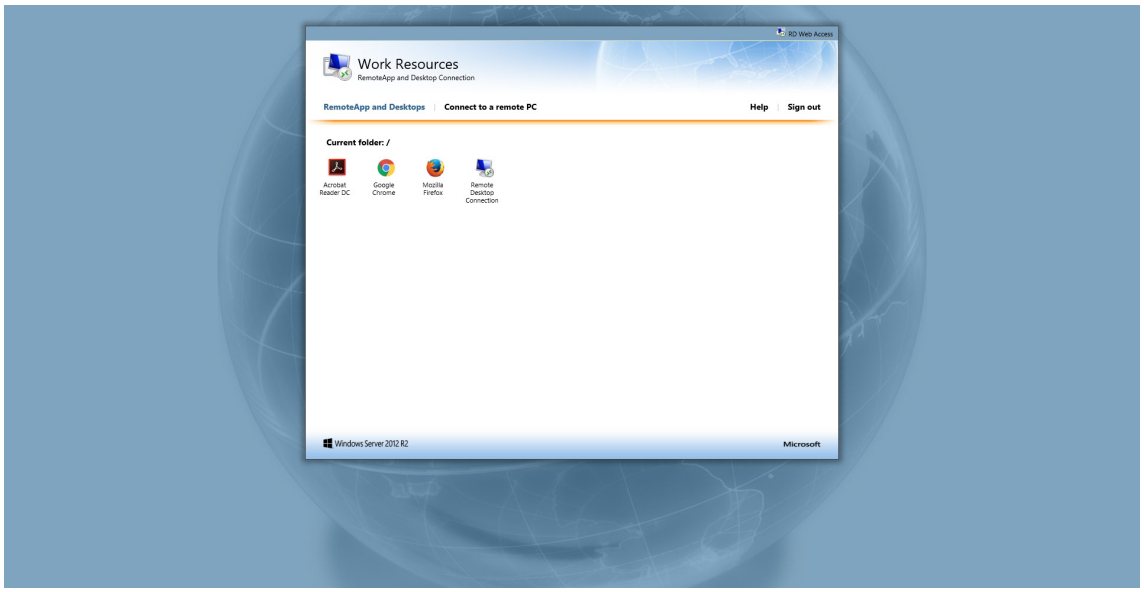


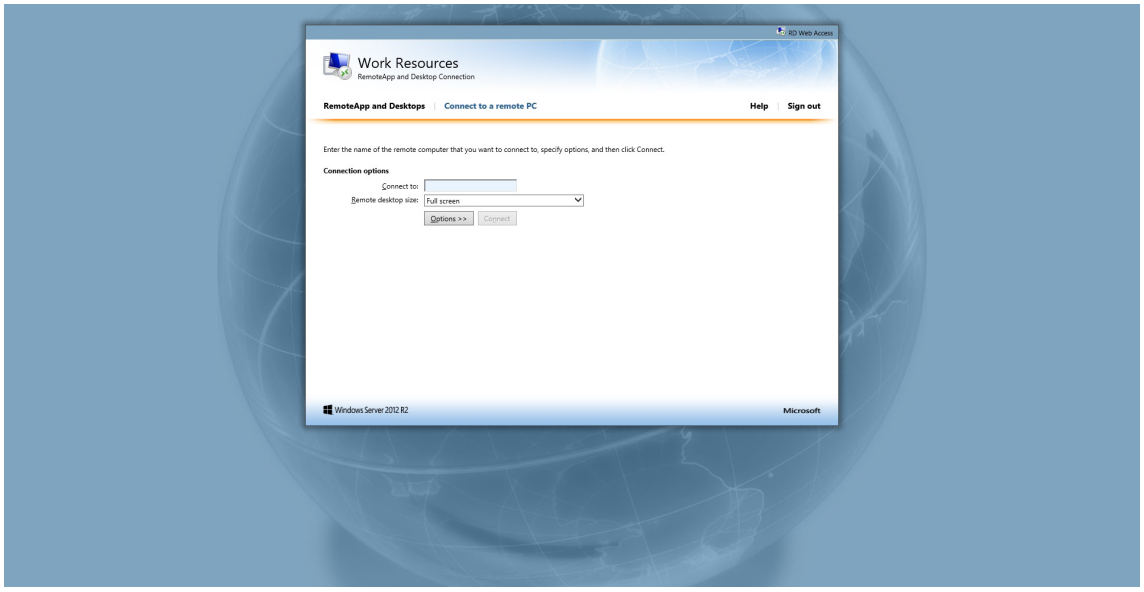
チェック

- セキュリティに関する警告メッセージが表示されることがあります。 詳細についてはIT管理者に相談し、最初に接続が安全であることを確認してください。 合格するには、このウェブサイトに進むをクリックしてください。
- ページの下部にポップアップメッセージが表示されたら、[**Allow**] をクリックしてActiveXコントロールを有効にします。

3. 資格情報を入力し、[**Sign in**] をクリックします。

4. [**RemoteApp**と**Desktops**] または [**Connect to a remote PC**] をクリックして選択します。





5. アイコンをクリックするか、画面上の指示に従ってアプリケーションやデスクトップを起動します。

接続の種類：ウェブフィード

リモートアプリケーションにアクセスするには、以下を実行してください。

1. デスクトップの左下にある  をクリックします。
2. クリックすると、開始時に目的のアプリケーションが起動します。

4.5.5 高度なRDP接続設定の構成

以下の表は、RDP接続の各設定項目の説明です。 この表を参照して、高度な設定を行い、サービスアクセスのためのデスクトップショートカットまたはスタートスクリーンタイルをカスタマイズしてください。

チェック

- 使用可能な設定は、選択した接続タイプによって異なります。

リモートデスクトップの接続タイプの設定

チェック

- リモートWebアクセスの接続タイプの設定については、「リモートWebアクセスの接続タイプの設定」（81ページ）を参照してください。
- Webフィードの接続タイプの設定については、「Webフィードの接続タイプの設定」（83ページ）を参照してください。

[**General**] サブタブ

<table>
<tr><th colspan="2">サーバー設定</th></tr>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>セッション名</td><td>リモートデスクトップセッションの名前を入力します。</td></tr>
<tr><td>サーバーアドレス</td><td>リモートデスクトップセッションを配信するサーバー/仮想マシンのコンピュータ名またはIPアドレスを入力します。</td></tr>
<tr><td>接続タイプ</td><td>この表は、リモートデスクトップが選択されている場合に使用可能な設定の説明のみを提供します。

次の3つの接続タイプを使用できます。
<table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>リモートデスクトップ</td><td>リモートデスクトップ/アプリケーションへのアクセスを提供します。</td></tr>
<tr><td>リモートWebアクセス</td><td>Webブラウザ（Internet Explorer）を介してリモートデスクトップ/アプリケーションへのアクセスを提供します。</td></tr>
<tr><td>Webフィード</td><td>公開された開始画面タイルを使用してリモートアプリケーションにアクセスできます。</td></tr>
</table></td></tr>
<tr><td>接続品質</td><td>ネットワーク接続の品質を最もよく表す設定を選択します：非常に高速（LAN）、高速（広帯域）、低速（モデム）、および自動検出の3つのオプションが利用できます。</td></tr>
</table>

<table>
<tr><td>サーバー認証</td><td>クライアントがリモートコンピュータのIDを確認できない場合は、次に行う処理を選択します。 3つのオプションがあります：接続して警告しないでください、私に警告し、接続しないでください。

<table><tr><th>オプション</th><th>説明</th></tr><tr><td>接続して、
私に警告しない</td><td>とにかく警告なしで接続します。</td></tr><tr><td>私に警告</td><td>接続するかどうかを警告し、ユーザーが選択できるようにします。</td></tr><tr><td>接続しない</td><td>接続を許可しません。</td></tr></table></td></tr>
<tr><td colspan="2">ログイン設定</td></tr>
<tr><td>項目</td><td>説明</td></tr>
<tr><td>ユーザー名</td><td>認証に使用されるユーザー/アカウント名を入力します。</td></tr>
<tr><td>パスワード</td><td>認証に使用するユーザーアカウントのパスワードを入力します。</td></tr>
<tr><td>ドメイン</td><td>サーバーのドメインを入力します。

注意: サーバーがどのドメインにも属していない場合は、このフィールドを空白のままにします。</td></tr>
<tr><td colspan="2">共通設定</td></tr>
<tr><td>項目</td><td>説明</td></tr>
<tr><td>起動時の自動起動</td><td>Windows 10のIoT Enterpriseが起動したときにリモートデスクトップセッションを自動的に開くかどうかを選択します。

[Yes] を選択すると、システムにログインするたびにリモートデスクトップセッションが自動的に開かれます。</td></tr>
<tr><td>アプリケーション終了時</td><td>リモートデスクトップセッションが終了したら何をするかを選択します。[何もしない]、[アプリケーションを再起動する]、[リブートする]、[シャットダウンする] の4つのオプションがあります。

<table><tr><th>オプション</th><th>説明</th></tr><tr><td>何もしない</td><td>Windows 10のIoT Enterpriseデスクトップに戻ります。</td></tr><tr><td>アプリケーションを再起動する</td><td>リモートデスクトップセッションを再度開きます。</td></tr><tr><td>リブートする</td><td>シンクライアントを再起動します。</td></tr><tr><td>シャットダウンする</td><td>シンクライアントを無効にします。</td></tr></table></td></tr>
</table>

[**Options**] サブタブ

プログラム	
項目	**説明**
接続時に次のプログラムを起動	ドロップダウンメニューをクリックして、アプリケーションモードを有効または無効にします。 このオプションを使用してセッションタイプを選択できます。 2つのリモートセッションタイプを使用できます。 • リモートデスクトップ（アプリケーションモードが無効の場合） • リモートアプリケーション（アプリケーションモードが有効な場合） **注意:** リモートアプリケーションセッションは、フルデスクトップではなく特定のアプリケーションのみにアクセスするために使用されるリモートセッションです。 **注意:** リモートアプリケーションセッションを開く前に、アプリケーションホストサーバー上のRemoteAppマネージャを使用して、目的のアプリケーションをRemoteAppプログラムリストに追加する必要があります。 サーバー上のRemoteAppプログラムリストに目的のアプリケーションを追加する方法の詳細については、MicrosoftサポートWebサイト support.microsoft.com を参照してください。
次のフォルダから開始	必要なアプリケーションの場所（ホストサーバー上）を入力します。 接続が有効なときに次のプログラムを起動します。 **注意:** このフィールドに目的のアプリケーションの場所/パスを入力し、**プログラムパスとファイル名**（次のフィールド）にアプリケーションの名前のみを指定できます。 または、**プログラムパスとファイル名**にアプリケーションのフルパスと名前を入力し、このフィールドを空のままにします。
プログラムのパスとファイル名	[**Start the following program on connection**] が有効になっている場合は、目的のアプリケーションのパスと名前を入力します。 **注意:** ファイル拡張子を省略することができます。

リモートAPP	**書式の例**
Windows Media Player	C:\Programs Files (x86)\Windows Media Player\wmplayer.exe
Adobe Reader X	C:\Programs Files (x86)\Adobe\Reader 10.0\Reader\ArcoRd32.exe
Adobe Reader X	C:\Programs Files (x86)\Adobe\Reader 10.0\Reader\ArcoRd32

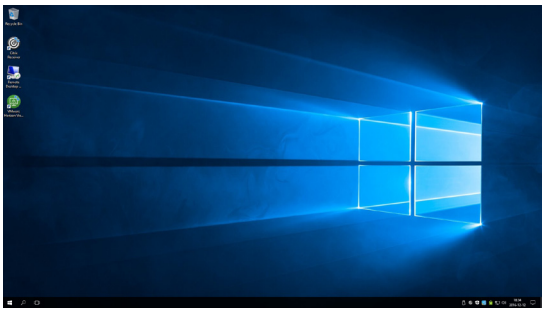
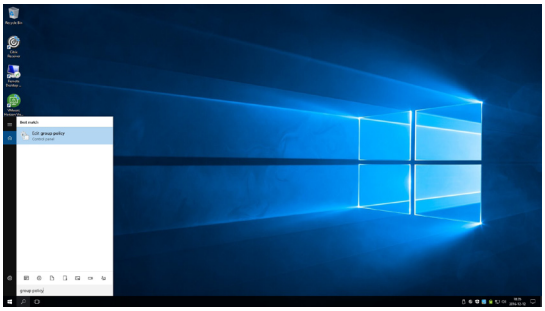
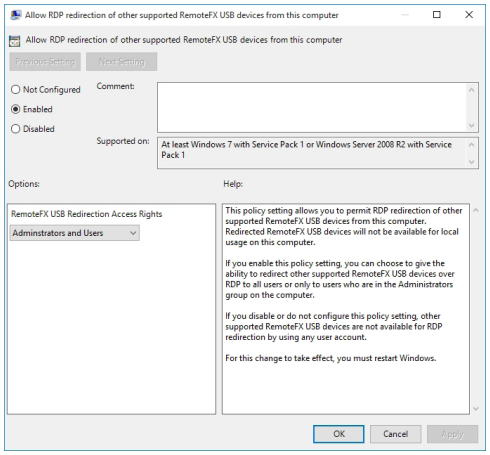
ウィンドウ設定	
項目	**説明**
色深度	ドロップダウンメニューをクリックして、リモートデスクトップセッションの色深度を選択します。 使用可能なオプションは、**15ビット**、**16ビット**、**24ビット**、および**32ビット**の4つです。 **注意:** RemoteFXを有効にすると、ここで選択した色の深度に関係なく、1ピクセルあたり32ビットが適用されます。 **注意:** ホストサーバー上のリモートデスクトップセッションの色深度の上限を設定できます。 この場合、ここで選択する色の深度に関係なく、値は定義された制限を超えることはできません。
解像度	ドロップダウンメニューをクリックして、リモートデスクトップセッションで目的のディスプレイ解像度を選択します。 **全画面**、**1920x1200**、**1920x1080**、**1680x1050**、**1400x1050**、**1440x900**、**1280x1024**、**1280x768**、**1280x720**、**1024x768**、**800x600**、および**640x480**の12種類のオプションが利用できます。

マルチモニタ	ドロップダウンメニューをクリックして、リモートデスクトップセッションで複数のディスプレイを有効または無効にします。
全画面使用時に接続バーを表示する	プルダウンメニューをクリックして、接続バーがフルスクリーンモードで表示されるかどうかを選択します。
接続設定	
項目	**説明**
プリンタマッピング	プルダウンメニューをクリックして、プリンタのマッピングを有効または無効にします。 [**Enable**] を選択すると、ユーザーはリモートデスクトップセッションでローカルプリンタまたはネットワークプリンタにアクセスできます。 **注意:** 最初にシンクライアント用のローカルまたはネットワークプリンタを追加してから、この機能を有効にして、リモートデスクトップセッションでそのプリンタを使用する必要があります。 **注意:** Windows 10のIoTエンタープライズベースのシンクライアントにローカルまたはネットワークプリンタを追加するには、コントロールパネルの [**Hardware and Sound**] > [**Devices and Printers**] > [**Add a printer**] をクリックし、画面の指示に従って、 ネットワークプリンタ。
クリップボードリダイレクト	ロップダウンメニューをクリックして、クリップボードのリダイレクトを有効または無効にします。 **注意:** [**Enable**] を選択すると、クリップボードはローカルおよびリモートデスクトップ（両方向）で使用できます。
スマートカードマッピング	スマートカードのマッピングを有効/無効にするには、ドロップダウンメニューをクリックします。 [**Enable**] を選択すると、ユーザーはリモートデスクトップセッションでスマートカードリーダーからスマートカードにアクセスできます。
ポートマッピング	ドロップダウンメニューをクリックして、ポートマッピングを有効または無効にします。 [**Enable**] を選択すると、ユーザーはリモートデスクトップセッションでローカルに使用可能なポートを使用して接続されているデバイスにアクセスできます。 **注意:** シンクライアント上のデバイスポートのタイプと可用性は、製品モデルによって異なります。

<table>
<tr><th colspan="2">ローカルリソースの設定</th></tr>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>リモートオーディオ再生</td><td>ドロップダウンメニューをクリックして、リモートデスクトップセッションでコンピュータサウンドとオーディオ再生設定を構成します。 このコンピュータに持ち込む、再生しない、およびリモートコンピュータに放置するという3つのオプションがあります。

<table><tr><th>オプション</th><th>説明</th></tr><tr><td>このコンピュータに持っていく</td><td>ローカルに接続されたオーディオデバイスを使用して、リモートデスクトップセッションでコンピュータサウンドとオーディオ再生を可能にします。</td></tr><tr><td>再生しない</td><td>リモートデスクトップセッションでコンピュータサウンドとオーディオ再生を無効にします。</td></tr><tr><td>リモートコンピュータに放置</td><td>コンピュータのサウンドとオーディオ再生をリモートコンピュータに任せてください。</td></tr></table></td></tr>
<tr><td>リモートオーディオ録音</td><td>ドロップダウンメニューをクリックして、リモートデスクトップセッションでオーディオ録画設定を構成します。 このコンピュータからの録音と録音しないという2つのオプションがあります。

<table><tr><th>オプション</th><th>説明</th></tr><tr><td>このコンピュータからの録音</td><td>ローカルに接続されたオーディオデバイスを使用して、リモートデスクトップセッションでオーディオ録音を可能にします。</td></tr><tr><td>録音しない</td><td>ローカルに接続されたオーディオデバイスを使用してリモートデスクトップセッションでオーディオ録音を無効にします。</td></tr></table>
注意: リモートオーディオ再生のドロップダウンメニューでリモートコンピュータに残すが選択されている場合、この設定項目はグレー表示されます。</td></tr>
<tr><td>Windowsキーの組み合わせを適用</td><td>ドロップダウンメニューをクリックして、Windowsのキーの組み合わせを適用する場所を選択します。 このコンピュータでは、リモートコンピュータ上で、フルスクリーンを使用している場合のみ、3つのオプションを使用できます。</td></tr>
<tr><td>駆動</td><td>リモートデスクトップセッションでローカルに接続されたドライブを有効または無効にするには、ドロップダウンメニューをクリックします。</td></tr>
<tr><td>サポートされているプラグアンドプレイデバイス</td><td>ドロップダウンメニューをクリックして、リモートデスクトップセッションでサポートされているプラグアンドプレイデバイスを有効/無効にします。</td></tr>
</table>

RemoteFX USBリダイレクト	ローカルに接続されたRemoteFX USBデバイスを有効/無効にする場合にクリックします。 **注意:** リモートデスクトップでRemoteFX USBデバイスを使用するには、RemoteFX USBデバイスリダイレクションを許可するように、デバイスリダイレクトに関するポリシー設定を構成する必要があります。 これを行うには、次の手順に従ってください： 1. 管理アカウントでt68Wにログインします。 2. Atrust Client Setupを使用してUWF（Unified Write Filter）を無効にする（「4.2.10 UWFの設定（Unified Write Filter）」（52ページ）を参照）。 3. デスクトップの左下にある  をクリックします。  4. 表示された検索ウィンドウで、[**group policy**] を入力し、[**Edit groupt policy**] をクリックします。  5. 開いているウィンドウで、 **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Connection Client** > **RemoteFX USB Device Redirection** > **Allow RDP redirection of other supported RemoteFX USB devices from this computer** 。 6. この設定が [**Enabled**] されるユーザーを [**Administrators Only**] または [**Administrators**] と [**Users**] に設定し、[**OK**] をクリックします。  7. Atrust Client SetupでUWFを有効 。

[**RD Gateway**] サブタブ

接続設定	
項目	**説明**
RDゲートウェイサーバーの設定	ドロップダウンメニューをクリックして、RDゲートウェイサーバーを使用するか、自動的に検出するか、手動で構成するかを選択します 。**Automatically detect RD Gateway server settings**、**Use these RD Gateway server settings**、**Do not use an RD Gateway server** の3つのオプションを使用できます。
サーバー名	RDゲートウェイサーバーのIPアドレス/ URL / FQDNを入力 。 **注意:** 詳細については、ネットワーク管理者に相談してください。
ログオン方法	ドロップダウンメニューをクリックして、ログオン方法を選択します。 **後で選択する**、**パスワードを要求する（NTLM）**、および**スマートカード**の3つのオプションを使用できます。 **オプション** / **説明** 後で選択 / ユーザーは、サーバーに接続中にログオン方法を選択できます。 パスワードを要求 (NTLM) / ユーザーは、サーバーに接続する際にパスワードの入力を求められます。 スマートカード / ユーザーは、サーバーに接続している間にスマートカードを要求されます。
ローカルアドレス用にRDゲートウェイサーバーをバイパス	ローカルネットワークアドレスとの間のトラフィックがRDゲートウェイサーバー経由でルーティングされないようにし、接続を高速化します。
ログオンの設定	
項目	**説明**
リモートコンピュータのRDゲートウェイ資格情報を使用	RDゲートウェイサーバーとリモートコンピューターの両方に対して同じ資格情報を使用して認証する場合は、このチェックボックスをオンにします。

リモート*Web*アクセスの接続タイプの設定

チェック

- リモートデスクトップの接続タイプの設定については、「リモートデスクトップの接続タイプの設定」（74ページ）を参照してください。
- Webフィードの接続タイプの設定については、「Webフィードの接続タイプの設定」（83ページ）を参照してください。

[**General**] サブタブ

サーバー設定	
項目	**説明**
セッション名	リモートWebアクセスセッションの名前を入力します。
接続URL	RD Webアクセスが使用できる接続URLを入力します。
接続タイプ	この表では、**リモートWebアクセス**が選択されている場合に使用可能な設定についてのみ説明しています。 次の3つの接続タイプを使用できます。 **オプション** / **説明** リモートデスクトップ / リモートデスクトップ/アプリケーションへのアクセスを提供します。 リモートWebアクセス / Webブラウザ（Internet Explorer）を介してリモートデスクトップ/アプリケーションへのアクセスを提供します。 Webフィード / 公開された開始画面タイルを使用してリモートアプリケーションにアクセスできます。
共通設定	
項目	**説明**
起動時の自動起動	Windows 10のIoT Enterpriseが起動したときにリモートデスクトップセッションを自動的に開くかどうかを選択します。 [**Yes**] を選択すると、システムにログインするたびにリモートデスクトップセッションが自動的に開かれます。
アプリケーション終了時	リモートデスクトップセッションが終了したら何をするか選択します。[**何もしない**]、[**アプリケーションを再起動する**]、[**リブートする**]、[**シャットダウンする**] の4つのオプションがあります。 **オプション** / **説明** 何もしない / Windows 10のIoT Enterpriseデスクトップに戻ります。 アプリケーションを再起動する / リモートデスクトップセッションを再度開きます。 リブートする / シンクライアントを再起動します。 シャットダウンする / シンクライアントを無効にします。

[**Options**] サブタブ

チェック

- [**Options**] のサブタブでは、リモートWebアクセスの接続タイプでは使用できません。

[**RD Gateway**] サブタブ

チェック

- リモートWebアクセスの接続タイプの [**RD Gateway**] サブタブで使用できるオプションはありません。

*Web*フィードの接続タイプの設定

チェック

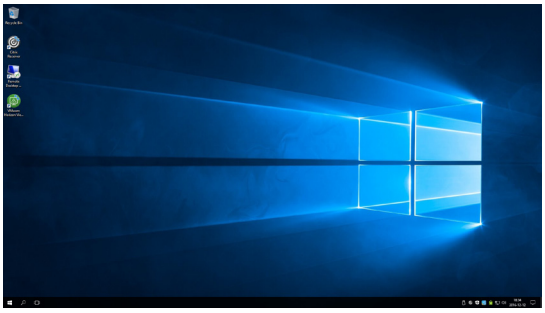
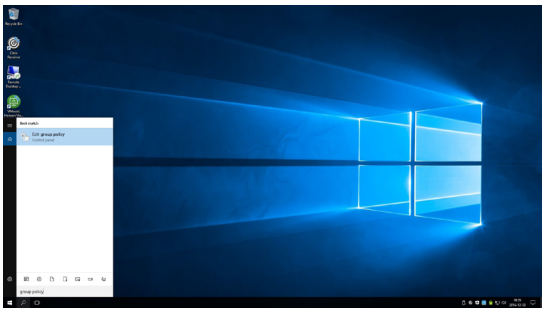
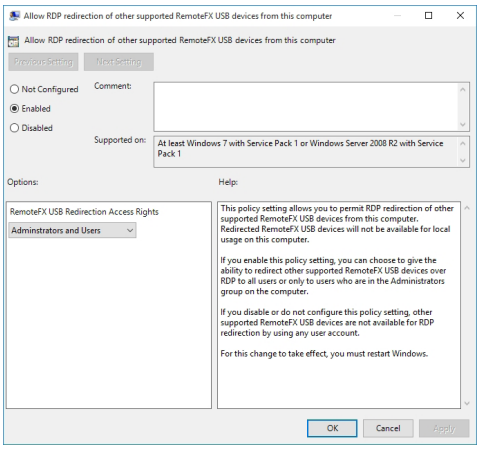
- リモートデスクトップの接続タイプの設定については、「リモートデスクトップの接続タイプの設定」（74ページ）を参照してください。
- リモートWebアクセスの接続タイプの設定については、「リモートWebアクセスの接続タイプの設定」（81ページ）を参照してください。

[**General**] サブタブ

サーバー設定	
項目	**説明**
セッション名	Webフィードセッションの名前を入力します。
WebフィードのURL	RD Webフィードにアクセスできるurlを入力します。
接続タイプ	この表では、**Web Feed**が選択されている場合にのみ使用可能な設定の説明が表示されます。 次の3つの接続タイプを使用できます。 **オプション** / **説明** リモートデスクトップ / リモートデスクトップ/アプリケーションへのアクセスを提供します。 リモートWebアクセス / Webブラウザ（Internet Explorer）を介してリモートデスクトップ/アプリケーションへのアクセスを提供します。 Webフィード / 公開された開始画面タイルを使用してリモートアプリケーションにアクセスできます。
ログイン設定	
項目	**説明**
ユーザー名	認証に使用されるユーザー/アカウント名を入力します。
パスワード	認証に使用するユーザーアカウントのパスワードを入力します。
ドメイン	サーバーのドメインを入力します。 **注意:** サーバーがどのドメインにも属していない場合は、このフィールドを空白のままにします。
RemoteAppとデスクトップ接続	
項目	**説明**
今すぐアップデート	サーバーから公開アプリケーションリストを取得して更新する場合にクリックします。

[**Options**] サブタブ

ウィンドウ設定	
項目	**説明**
色深度	ドロップダウンメニューをクリックして、リモートデスクトップセッションの色深度を選択します。 使用可能なオプションは、**15ビット**、**16ビット**、**24ビット**、および**32ビット**の4つです。 **注意:** RemoteFXを有効にすると、ここで選択した色の深度に関係なく、1ピクセルあたり32ビットが適用されます。 **注意:** ホストサーバー上のリモートデスクトップセッションの色深度の上限を設定できます。 この場合、ここで選択する色の深度に関係なく、値は定義された制限を超えることはできません。
解像度	ドロップダウンメニューをクリックして、リモートデスクトップセッションで目的のディスプレイ解像度を選択します。 **全画面**、**1920x1200**、**1920x1080**、**1680x1050**、**1400x1050**、**1440x900**、**1280x1024**、**1280x768**、**1280x720**、**1024x768**、**800x600**、および**640x480**の12種類のオプションが利用できます。
マルチモニタ	ドロップダウンメニューをクリックして、リモートデスクトップセッションで複数のディスプレイを有効または無効にします。
全画面使用時に接続バーを表示	プルダウンメニューをクリックして、接続バーがフルスクリーンモードで表示されるかどうかを選択します。
ローカルリソースの設定	
項目	**説明**
Windowsキーの組み合わせを適用	ドロップダウンメニューをクリックして、Windowsのキーの組み合わせを適用する場所を選択します。 **このコンピュータでは**、**リモートコンピュータ上で**、**フルスクリーンを使用している場合のみ**、3つのオプションを使用できます。

RemoteFX USBリダイレクト	ローカルに接続されたRemoteFX USBデバイスを有効/無効にする場合にクリックします。 **注意:** リモートデスクトップでRemoteFX USBデバイスを使用するには、RemoteFX USBデバイスリダイレクションを許可するように、デバイスリダイレクトに関するポリシー設定を構成する必要があります。 これを行うには、次の手順に従ってください： 1. 管理アカウントでt68Wにログインします。 2. Atrust Client Setupを使用してUWF（Unified Write Filter）を無効にする（「4.2.10 UWFの設定（Unified Write Filter）」（52ページ）を参照）。 3. デスクトップの左下にある  をクリックします。  4. 表示された検索ウィンドウで、[**group policy**] を入力し、[**Edit group policy**] をクリックします。  5. 開いているウィンドウで、**Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Connection Client** > **RemoteFX USB Device Redirection** > **Allow RDP redirection of other supported RemoteFX USB devices from this computer**。 6. この設定が [**Enabled**] されるユーザーを [**Administrators Only**] または [**Administrators**] と [**Users**] に設定し、[**OK**] をクリックします。  7. Atrust Client SetupでUWFを有効にします。

[**RD Gateway**] サブタブ

チェック

- リモートWebアクセスの接続タイプの [**RD Gateway**] サブタブで使用できるオプションはありません。

4.5.6 基本的なICA接続設定の設定

Citrix ICA設定では、CitrixサービスのICA接続を設定し、サービスアクセスのためにローカルデスクトップにショートカットを作成することができます。 これらのショートカットを使用するだけで、仮想デスクトップやアプリケーションにアクセスできます。

チェック

- Citrixデスクトップ仮想化ソリューションの詳細については、Citrix社のWebサイト（www.citrix.com）またはCitrix Knowledge Center（support.citrix.com）を参照してください。

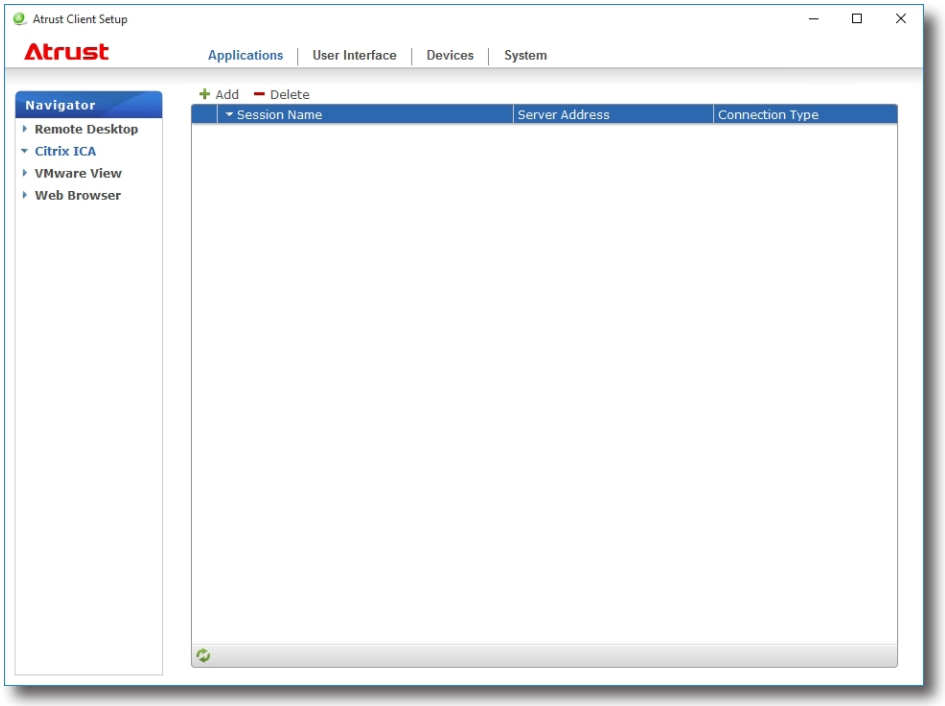
チェック

- また、Internet Explorerまたは標準のデスクトップショートカットCitrix Receiverを使用してCitrixサービスにアクセスすることもできます。 この標準デスクトップショートカットを使用してサービスにアクセスする方法の詳細については、 「3.2 Citrixサービスへのアクセス」（20ページ）を参照してください。
- このセクションの次のトピックでは、デスクトップとスタートメニューで独自のサービスアクセスショートカットを作成およびカスタマイズする手順を説明します。
- **Citrix VDI-in-a-Box**の接続設定を構成するには、**Web Logon**または**XenDesktop**接続タイプを選択します。

接続の種類：*Web*ログオン

Webログオンの接続タイプのICA接続設定をすばやく設定するには、以下を実行してください。

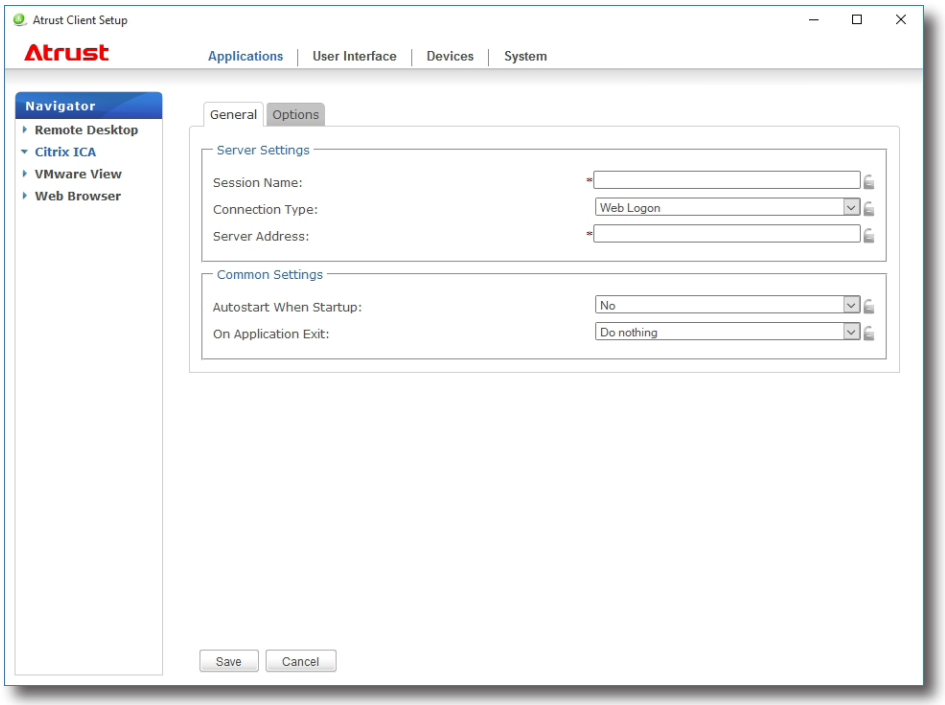
1. Atrust Client Setupで、[**Applications**] > [**Citrix ICA**] の順にクリックします。
2. 利用可能なICA ConnectionリストがConfigurationエリアに表示されます。



チェック

- エントリを作成していない場合、ICA接続リストは空になります。

3. ICA接続の新しいエントリを作成するには、ICA接続リストの上部にある [**Add**] をクリックします。
4. [**General**] サブタブで、接続タイプを [**Web Logon**] のままにしておき、[Server Settings] セクションでCitrixサービスにアクセスできるサーバーのIPアドレス/ URL / FQDNを希望するセッション名と入力します。



チェック

- Citrix環境によって、サーバー側の適切な情報タイプが異なる場合があります。 詳細については、IT管理者に相談してください。

5. [**Save**] をクリックして、このICA接続エントリを追加します。 アクセスショートカットはデスクトップ上に自動的に作成されます。

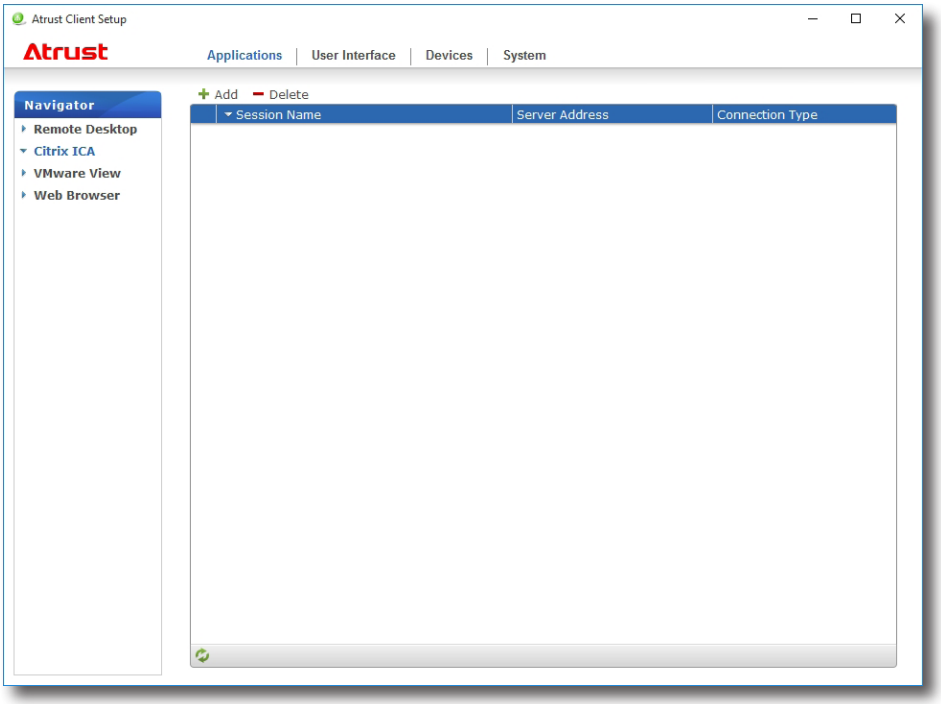
チェック

- サービスの提供計画とサーバーの構成に応じて、サービスアクセスのためのその他の高度なICA接続設定を構成する必要があります。 その他の設定については、「4.5.8 高度なICA接続設定の構成」（99ページ）を参照してください。

接続の種類：*XenDesktop*

XenDesktopの接続タイプのICA接続設定をすばやく設定するには、以下を実行してください。

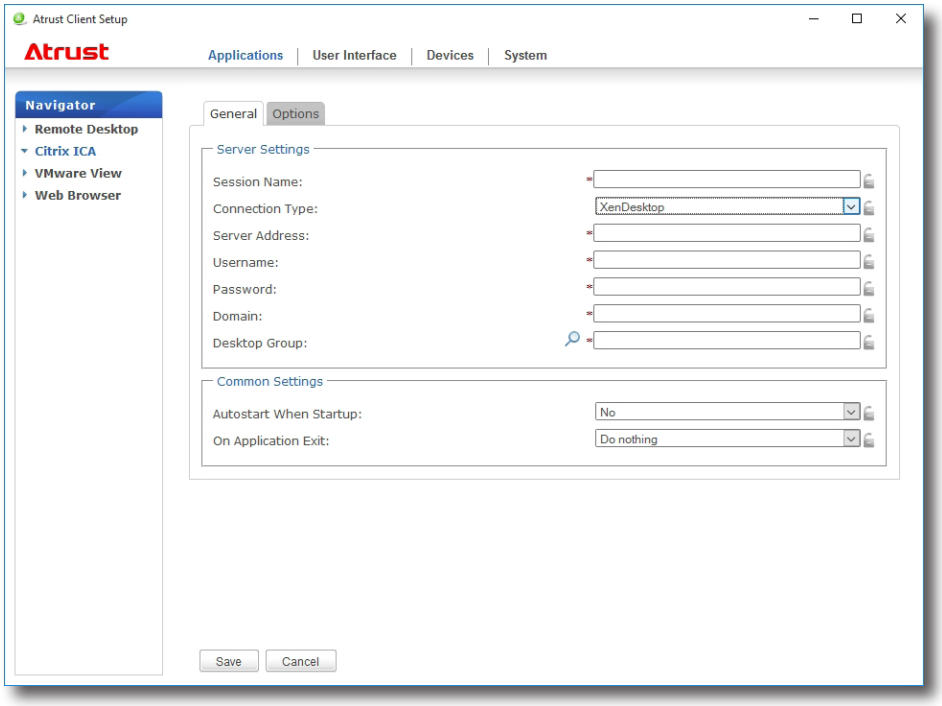
1. Atrust Client Setupで、[**Applications**] > [**Citrix ICA**] の順にクリックします。
2. 利用可能なICA Connectionリストが [Configuration] エリアに表示されます。



チェック

- エントリを作成していない場合、ICA接続リストは空になります。

3. ICA接続の新しいエントリを作成するには、ICA接続リストの上部にある [**Add**] をクリックします。
4. [**General**] サブタブで、[Connection Type] ドロップダウンメニューをクリックして [**XenDesktop**] を選択します。

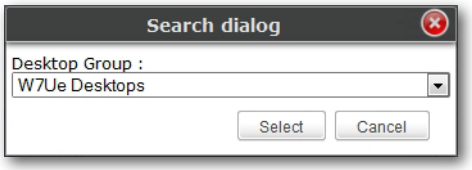


5. セッション名、XenDesktopにアクセスできるサーバーのIPアドレス/ FQDN、ユーザーの資格情報、サーバーのドメインを入力し、検索アイコン をクリックして使用可能なデスクトップグループを検出します。

チェック

- Citrix環境によって、サーバー側の適切な情報タイプが異なる場合があります。 詳細については、IT管理者に相談してください。
- 検索アイコンは、必要なデータ（赤いアスタリスクでマークされているフィールド）が提供されている場合にのみ機能します。

6. 完了すると、デスクトップグループを選択するための検索ダイアログウィンドウが表示されます。 ドロップダウンメニューをクリックして目的のデスクトップグループを選択し、[**Select**] をクリックして確定します。



7. 選択したデスクトップグループ名がデスクトップグループフィールドに自動的に表示されます。
8. [**Save**] をクリックして確認します。 アクセスショートカットはデスクトップ上に自動的に作成されます。

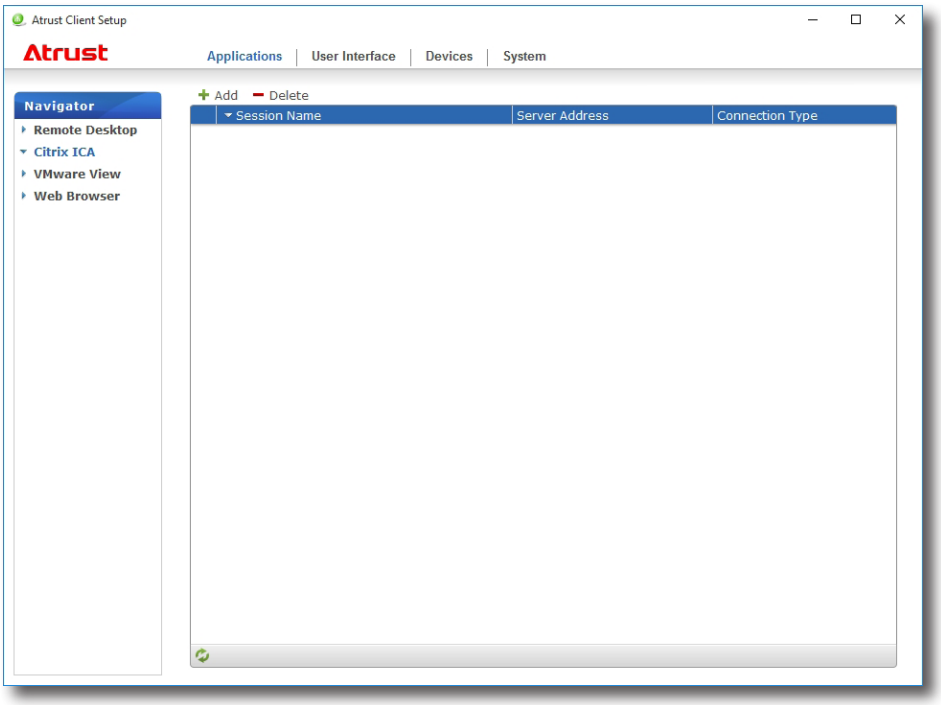
チェック

- サービスの提供計画とサーバーの構成に応じて、サービスアクセスのためのその他の高度なICA接続設定を構成する必要があります。 その他の設定については、「4.5.8 高度なICA接続設定の構成」（99ページ）を参照してください。

接続の種類：*XenApp*

XenAppの接続タイプのICA接続設定をすばやく設定するには、次の操作を行います。

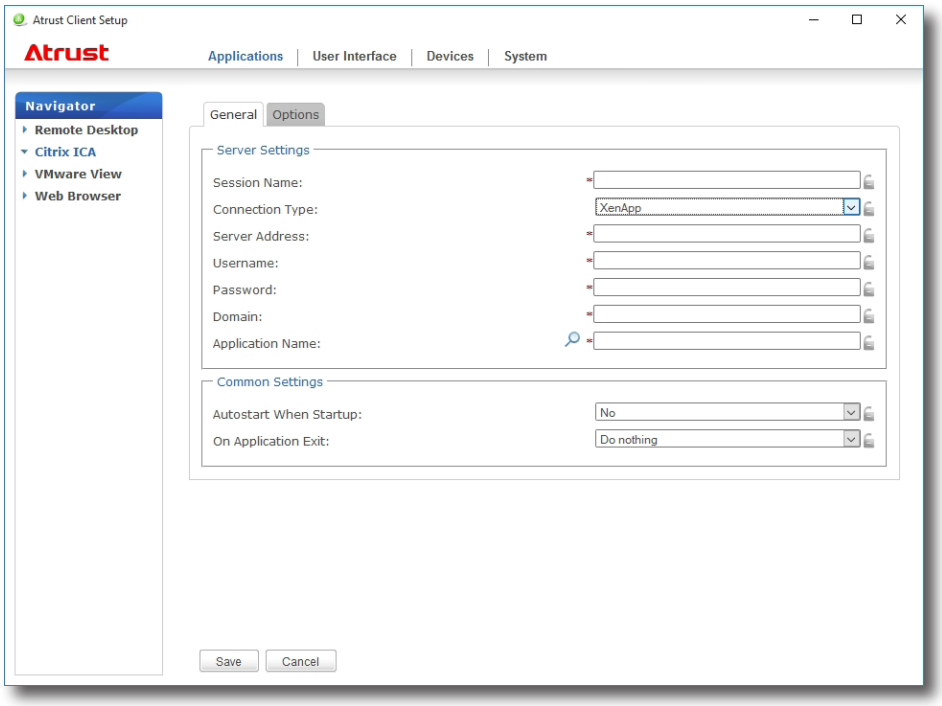
1. Atrust Client Setupで、[**Applications**] > [**Citrix ICA**] の順にクリックします。
2. 利用可能なICA Connectionリストが Configurationエリアに表示されます。



チェック

- エントリを作成していない場合、ICA接続リストは空になります。

3. ICA接続の新しいエントリを作成するには、ICA接続リストの上部にある [**Add**] をクリックします。
4. [**General**] サブタブで、[Connection Type] ドロップダウンメニューをクリックして [**XenApp**] を選択します。

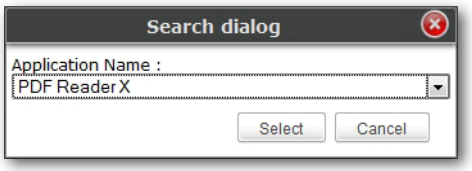


5. セッション名、XenAppにアクセスできるサーバーのIPアドレス/ FQDN、ユーザーの資格情報、サーバーのドメインを入力し、検索アイコン をクリックして使用可能なアプリケーションを検出します。

チェック

- Citrix環境によって、サーバー側の適切な情報タイプが異なる場合があります。 詳細については、IT管理者に相談してください。
- 検索アイコンは、必要なデータ（赤いアスタリスクでマークされているフィールド）が提供されている場合にのみ機能します。 XenAppサーバーがどのドメインにも属していない場合は、[Domain] フィールドにコンピュータ名を入力します。

6. 完了すると、アプリケーションを選択するための [Search Dialog] ウィンドウが表示されます。 ドロップダウンメニューをクリックして目的のアプリケーションを選択し、[**Select**] をクリックして確定します。



7. 選択したアプリケーション名が自動的に [Application Name] フィールドに表示されます。
8. [**Save**] をクリックして確認します。 アクセスショートカットはデスクトップ上に自動的に作成されます。

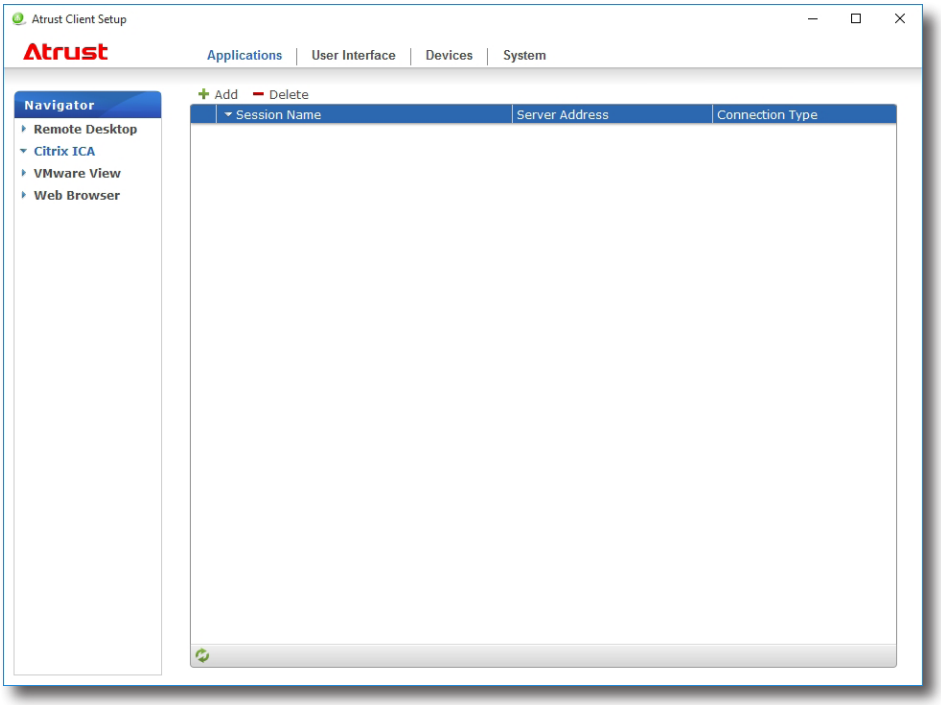
チェック

- サービスの提供計画とサーバーの構成に応じて、サービスアクセスのためのその他の高度なICA接続設定を構成する必要があります。 その他の設定については、「4.5.8 高度なICA接続設定の構成」（99ページ）を参照してください。

接続の種類：サーバー接続

サーバー接続の接続タイプのICA接続設定をすばやく設定するには、次の操作を行います。

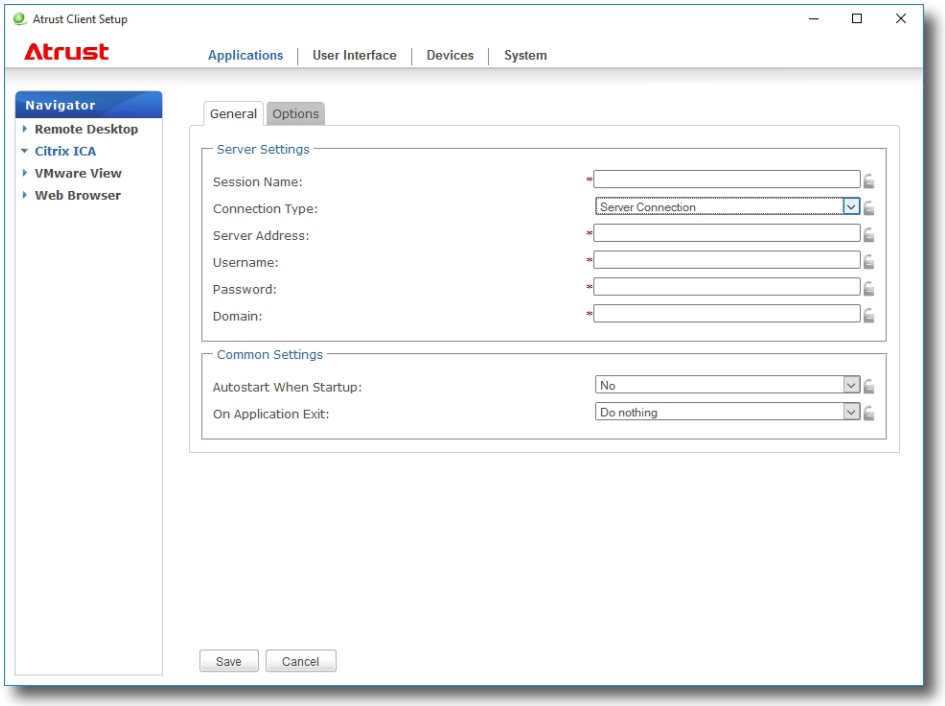
1. Atrust Client Setupで、[**Applications**] > [**Citrix ICA**] の順にクリックします。
2. 利用可能なICA Connectionリストが [Configuration] エリアに表示されます。



チェック

- エントリを作成していない場合、ICA接続リストは空になります。

3. ICA接続の新しいエントリを作成するには、ICA接続リストの上部にある [**Add**] をクリックします。
4. [**General**] サブタブで、[Connection Type] ドロップダウン・メニューをクリックして [**Server Connection**] を選択します。



5. セッション名、サーバーのIPアドレス/ FQDN、ユーザー資格情報、およびサーバーのドメインを入力します。

チェック

- Citrix環境によって、サーバー側の適切な情報タイプが異なる場合があります。 詳細については、IT管理者に相談してください。
- この接続タイプでは、XenAppサーバーへの接続のみがサポートされています。

6. [**Save**] をクリックして確認します。 アクセスショートカットはデスクトップ上に自動的に作成されます。

チェック

- サービスの提供計画とサーバーの構成に応じて、サービスアクセスのためのその他の高度なICA接続設定を構成する必要があります。 その他の設定については、「4.5.8 高度なICA接続設定の構成」（99ページ）を参照してください。

4.5.7 Citrixサービスへのアクセス

XenDesktop、*XenApp*、およびサーバー接続の接続タイプ

Citrixサービスにアクセスするには、以下を実行してください。

1. 作成された（カスタマイズされた）ショートカットをデスクトップ上でダブルクリックします。

> **チェック**
>
> - 標準のデスクトップショートカット「**Citrix Receiver**」を使用してCitrixサービスにアクセスすることもできます。 標準のデスクトップショートカットを使用してサービスにアクセスする方法の詳細については、「3.2 Citrixサービスへのアクセス」（20ページ）を参照してください。

2. 目的のアプリケーションまたはデスクトップが画面に表示されます。

*Web*ログオンの接続タイプ

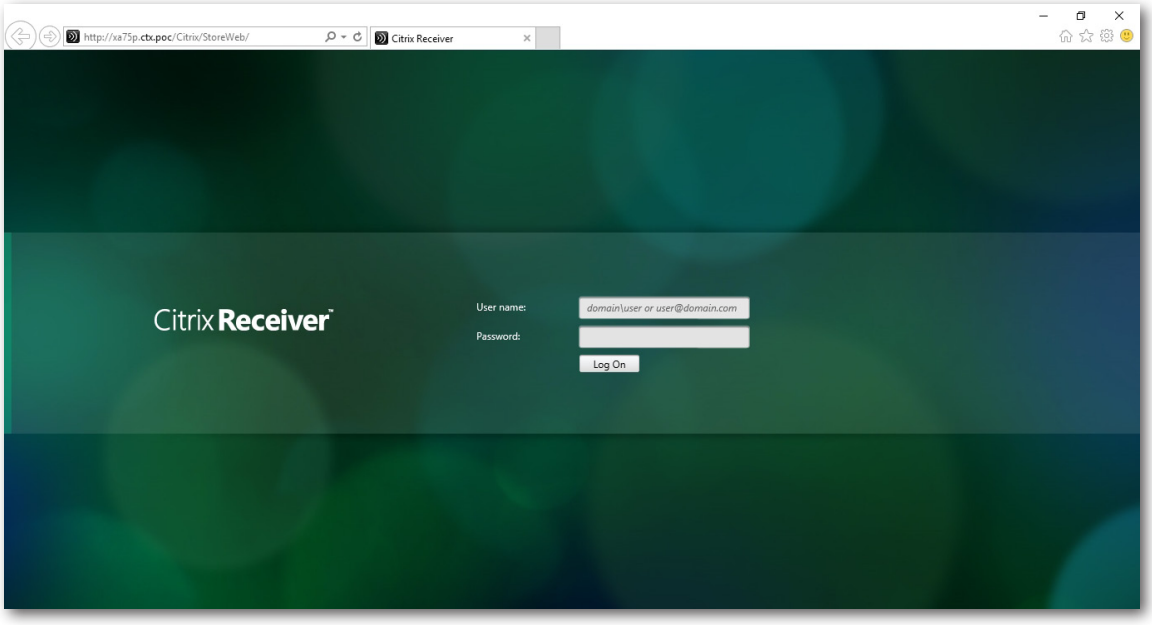
Citrixサービスにアクセスするには、以下を実行してください。

1. 作成された（カスタマイズされた）ショートカットをデスクトップ上でダブルクリックします。

> **チェック**
>
> - 標準のデスクトップショートカット「**Citrix Receiver**」を使用してCitrixサービスにアクセスすることもできます。 標準のデスクトップショートカットを使用してサービスにアクセスする方法の詳細については、「3.2 Citrixサービスへのアクセス」（20ページ）を参照してください。

2. WebブラウザはCitrixログオン画面で起動します。

ログオン画面の例：XenAppおよびXenDesktop 7.5 Platinum

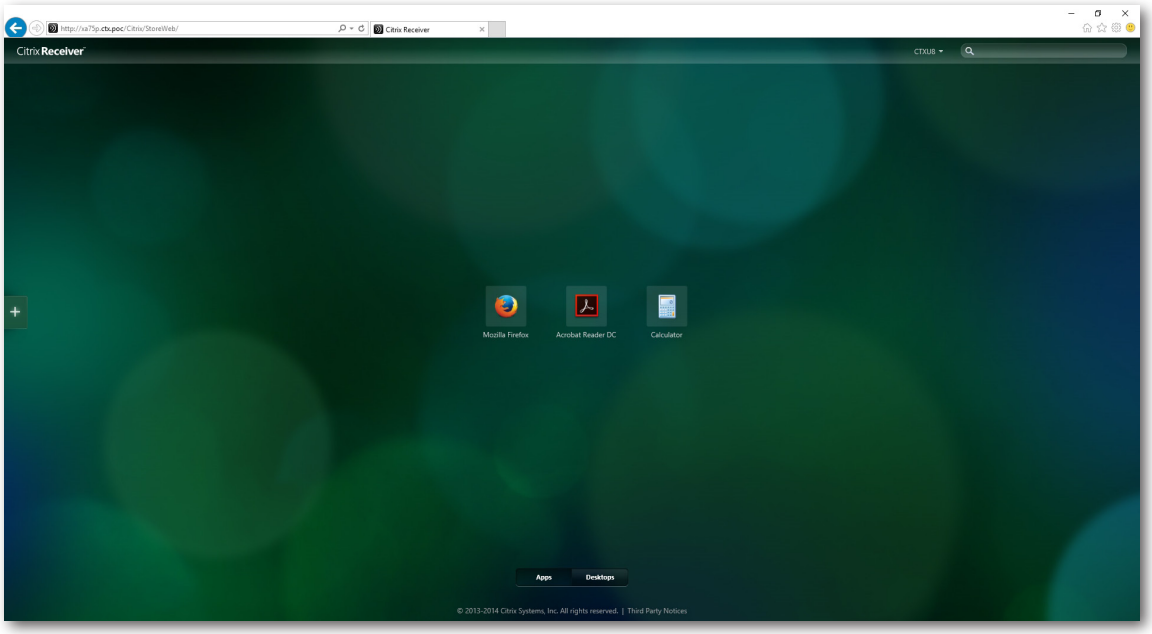


3. 必要な資格情報とドメイン名を入力し、[**Log On**] をクリックします。

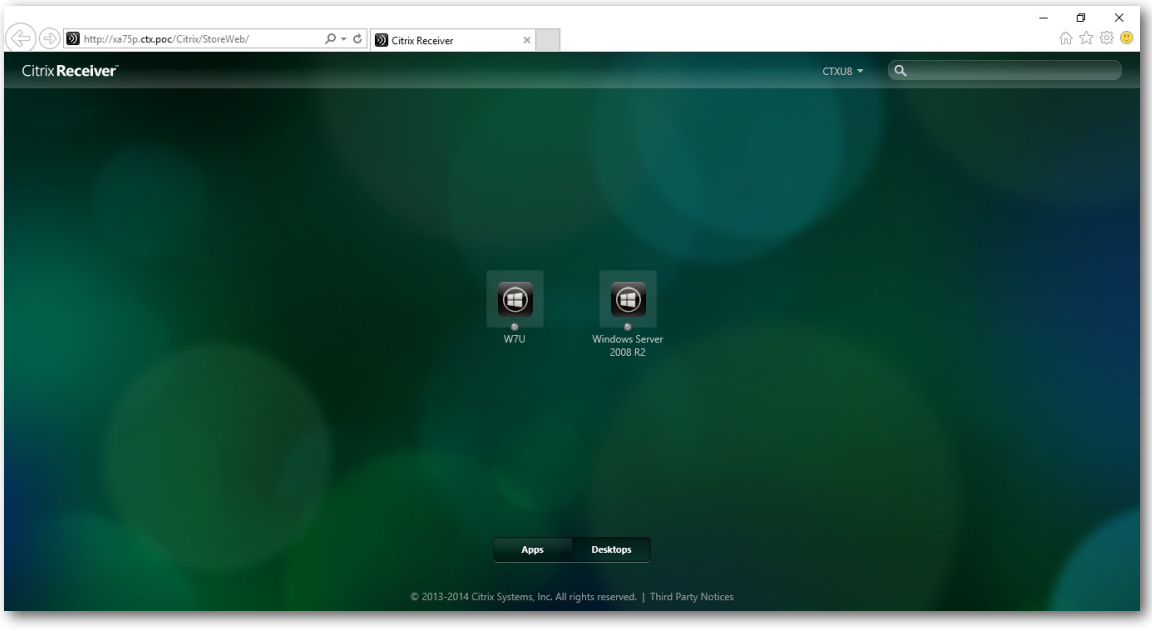
> **チェック**
>
> - サービスホストサーバーがどのドメインにも属していない場合は、必要に応じてサーバー名を入力します。

4. クリックして、目的のアプリケーションまたはデスクトップを選択します。

オンデマンドアプリケーションの画面：XenApp 7.5 Platinum

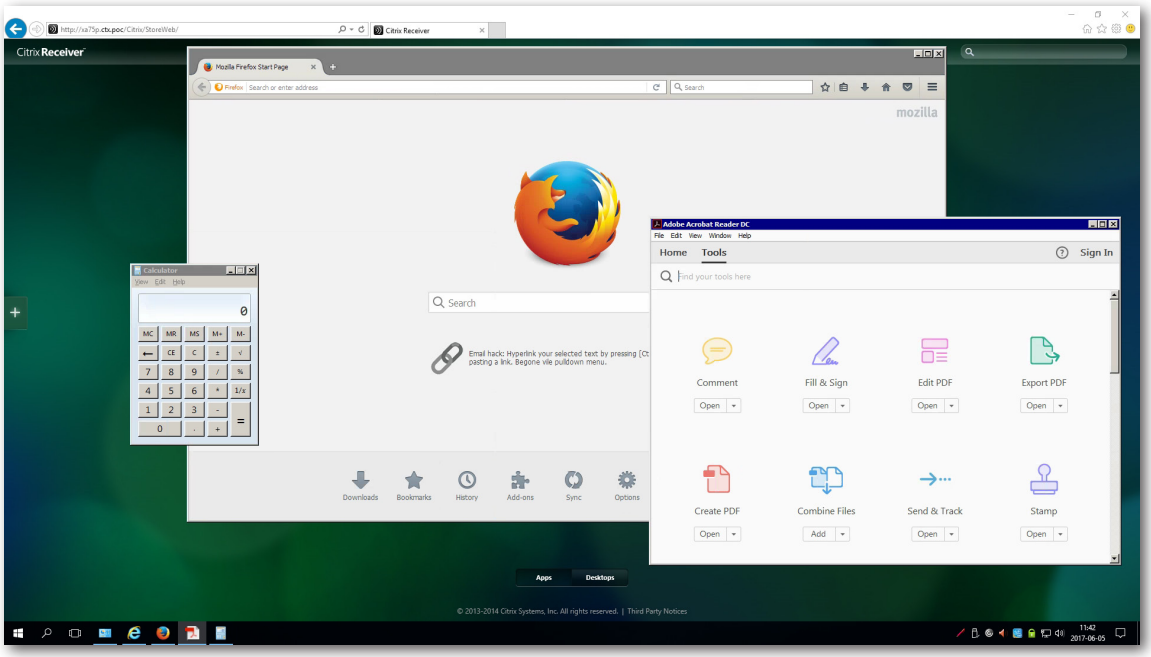


オンデマンドデスクトップの画面：XenDesktop 7.5 Platinum

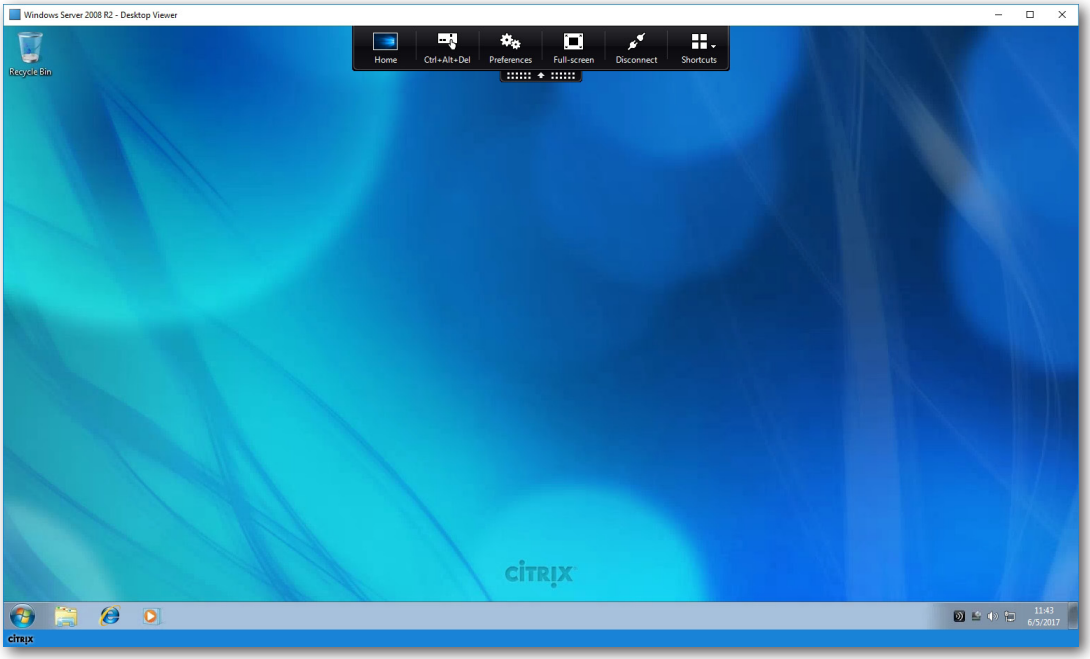


5. 選択したアプリケーションまたはデスクトップが画面に表示されます。

例：Applications Delivered by XenApp 7.5 Platinum
電卓、Mozilla Firefox、およびAdobe Reader



例：XenDesktop 7.5 Platinumが提供するデスクトップ
Windows Server 2008 R2



例：XenDesktop 7.5 Platinumが提供するデスクトップ
Windows 7 Ultimate

4.5.8 高度なICA接続設定の構成

以下の表は、ICA接続の各設定項目の説明です。 この表を参照して、デスクトップ上の詳細設定とショートカットをカスタマイズし、サービスアクセスのための [Start] メニューをカスタマイズしてください。

チェック

- 使用可能な設定は、選択した接続タイプによって異なります。

*Web*ログオンの接続タイプの設定

チェック

- XenDesktopの接続タイプの設定については、「XenDesktopの接続タイプの設定」（101ページ）を参照してください。
- XenAppの接続タイプの設定については、「XenAppの接続タイプの設定」（104ページ）を参照してください。
- サーバ接続の接続タイプの設定については、「サーバー接続の接続タイプの設定」（107ページ）を参照してください。

[**General**] サブタブ

<table>
<tr><th colspan="2">サーバー設定</th></tr>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>セッション名</td><td>Citrix ICAセッションの名前を入力します。</td></tr>
<tr><td>接続タイプ</td><td>この表では、[Web Logon] が選択されている場合に使用可能な設定についてのみ説明しています。

次の4つの接続タイプを使用できます。

<table><tr><th>オプション</th><th>説明</th></tr><tr><td>Webログオン</td><td>Webブラウザ（Internet Explorer）のインターフェイスを使用して、アプリケーション、デスクトップ、およびコンテンツアクセスサービスを提供します。</td></tr><tr><td>XenDesktop</td><td>デスクトップ配信サービスを提供します。</td></tr><tr><td>XenApp</td><td>アプリケーション配信サービスを提供します。</td></tr><tr><td>サーバー接続</td><td>管理者用の完全なサーバーアクセスサービスを提供します（XenAppサーバーのみ）。</td></tr></table>
注意: [Web Logon] を選択すると、t68WはWebブラウザを使用してサービスにアクセスします。 Internet Explorerは、他のブラウザをインストールしていても、デフォルトとして設定しているブラウザであれ、常に使用されます。 詳細は、「4.5.7 Citrixサービスへのアクセス」（95ページ）を参照してください。</td></tr>
<tr><td>サーバーアドレス</td><td>CitrixサービスにアクセスできるサーバーのIPアドレス/ URL / FQDNを入力します。</td></tr>
</table>

共通設定	
項目	**説明**
起動時の自動起動	Windows 10 IoT Enterpriseの起動時にCitrix ICAセッションを自動的に開くかどうかを選択します。 [**Yes**] を選択すると、システムにログインするたびにCitrix ICAセッションが自動的に開かれます。
アプリケーション終了時	Citrix ICAセッションが終了したときの対処方法を選択します。[**何もしない**]、[**アプリケーションを再起動する**]、[**リブートする**]、[**シャットダウンする**] の4つのオプションがあります。 **オプション** / **説明** 何もしない / Windows 10のIoT Enterpriseデスクトップに戻ります。 アプリケーションを再起動する / Citrix ICAセッションを再度開きます。 リブートする / シンクライアントを再起動します。 シャットダウンする / シンクライアントを無効にします。

[**Options**] サブタブ

Web設定	
項目	**説明**
モード設定	ドロップダウンメニューをクリックして、目的のブラウザウィンドウモードを選択します。**フルスクリーン**と**ノーマルモード**の2つのオプションがあります。 **オプション** / **説明** フルスクリーン / フルスクリーンモードでブラウザが開きます。 ノーマルモード / ブラウザは標準モードで開きます。 **注意:** この設定項目は、[Connection Type] フィールドで [**Web Logon**] が選択されている場合にのみ使用できます。 このタイプの接続により、Webブラウザーのインターフェースを介してサービスにアクセスできます。 **注意:** サービスアクセスのために使用されるWebブラウザは、デフォルトとして設定されているブラウザに関係なく、常にInternet Explorerです。

XenDesktopの接続タイプの設定

チェック

- Webログオンの接続タイプの設定については、「Webログオンの接続タイプの設定」（99ページ）を参照してください。
- XenAppの接続タイプの設定については、「XenAppの接続タイプの設定」（104ページ）を参照してください。
- サーバ接続の接続タイプの設定については、「サーバー接続の接続タイプの設定」（107ページ）を参照してください。

[**General**] サブタブ

<table>
<tr><th colspan="2">サーバー設定</th></tr>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>セッション名</td><td>Citrix ICAセッションの名前を入力します。</td></tr>
<tr><td>接続タイプ</td><td>この表では、XenDesktopが選択されている場合に使用可能な設定についてのみ説明しています。

4つの接続タイプが利用可能です。

<table><tr><th>オプション</th><th>説明</th></tr><tr><td>Webログオン</td><td>Webブラウザ（Internet Explorer）のインターフェイスを使用して、アプリケーション、デスクトップ、およびコンテンツアクセスサービスを提供します。</td></tr><tr><td>XenDesktop</td><td>デスクトップ配信サービスを提供します。</td></tr><tr><td>XenApp</td><td>アプリケーション配信サービスを提供します。</td></tr><tr><td>サーバー接続</td><td>管理者用の完全なサーバーアクセスサービスを提供します（XenAppサーバーのみ）。</td></tr></table></td></tr>
<tr><td>サーバーアドレス</td><td>XenDesktopを経由するサーバーのIPアドレス/ FQDNを入力しますアクセス可能です。</td></tr>
<tr><td>ユーザー名</td><td>認証に使用されるユーザー/アカウント名を入力します。</td></tr>
<tr><td>パスワード</td><td>認証に使用するユーザーアカウントのパスワードを入力します。</td></tr>
<tr><td>ドメイン</td><td>サーバーのドメインを入力します。</td></tr>
<tr><td>デスクトップグループ</td><td>デスクトップグループを入力します。

注意: フィールドの前にある検索アイコン を使用して、使用可能なデスクトップグループを検出できます。 詳細な手順については、 「接続の種類：XenDesktop」（89ページ）を参照してください。</td></tr>
</table>

共通設定	
項目	**説明**
起動時の自動起動	Windows 10 IoT Enterpriseの起動時にCitrix ICAセッションを自動的に開くかどうかを選択します。 [**Yes**] を選択すると、システムにログインするたびにCitrix ICAセッションが自動的に開かれます。
アプリケーション終了時	Citrix ICAセッションが終了したときの対処方法を選択します。 [**何もしない**]、[**アプリケーションを再起動する**]、[**リブートする**]、[**シャットダウンする**] の4つのオプションがあります。 **オプション** / **説明** 何もしない / Windows 10のIoT Enterpriseデスクトップに戻ります。 アプリケーションを再起動する / Citrix ICAセッションを再度開きます。 リブートする / シンクライアントを再起動します。 シャットダウンする / シンクライアントを無効にします。

[**Options**] サブタブ

ウィンドウ設定	
項目	**説明**
要求された色品質	プルダウンメニューをクリックして、Citrix ICAセッションのカラー品質を選択します。 **優先度なし**、**ベタースピード（16ビット）**、**より良い外観（32ビット）**の3つのオプションがあります。 **オプション** / **説明** 優先度なし / 特定の色品質を優先しません。 ベタースピード（16ビット） / 16ビットのカラー品質は、表示速度を向上させるために使用されます。 より良い外観（32ビット） / デスクトップの外観を向上させるために、32ビットのカラー品質が使用されています。
ウィンドウサイズ	ドロップダウンメニューをクリックして、Citrix ICAセッションのウィンドウサイズを選択します。 **デフォルト**、**シームレス**、**全画面**、**640 x 480**、**800 x 600**、**1024 x 768**、**1280 x 1024**、および**1600 x 1200**の8つのオプションがあります。 **注意:** XenDesktopツールバーがサーバー側で有効になっていると、ウィンドウサイズを変更できない場合があります。 **注意:** XenDesktopツールバーを無効にする方法の詳細については、オンラインヘルプについては、CitrixのWebサイト（support.citrix.com または www.citrix.com）を参照してください。 **注意:** ツールバーを無効にしたくない場合は、ツールバーまたはマウスを使用して、必要に応じて起動したウィンドウのサイズを変更できます。

デバイスマッピング	
項目	**説明**
ローカルドライブのマッピング	ドロップダウンメニューをクリックして、Citrix ICAセッションでローカルドライブのマッピングを有効または無効にします。 [**Yes**] を選択すると、起動したCitrix ICAセッションでローカルに接続されているドライブが使用できるようになります。
ローカルシリアルポートのマッピング	ドロップダウンメニューをクリックして、Citrix ICAセッションでローカルシリアルデバイスのマッピングを有効または無効にします。 [**Yes**] を選択すると、起動したCitrix ICAセッションで、ローカルに接続されたシリアルデバイスが使用できるようになります。
ローカルプリンタのマッピング	ドロップダウンメニューをクリックして、Citrix ICAセッションでローカルプリンタのマッピングを有効または無効にします。 [**Yes**] を選択すると、起動したCitrix ICAセッションでローカルに接続されているプリンタが使用可能になります。
接続設定	
項目	**説明**
ネットワークプロトコル	プルダウンメニューをクリックして、接続に使用するプロトコルを選択します。**TCP/IP**、**TCP/IP + HTTP サーバーの場所**、**SSL/TLS + HTTPS サーバーの場所**の3つのオプションを使用できます。
オーディオ品質	ドロップダウンメニューをクリックして、オーディオ再生を無効にするか、Citrix ICAセッションで目的の音質を選択します。 ドロップダウンメニューをクリックして、オーディオの再生を無効にするか、Citrix ICAセッションでオーディオ再生の品質設定を構成します。 **高 - 高精細オーディオ**、**中 - スピーチ用に最適化**、**低速 - 低速接続用**、および**オフ**の4つのオプションがあります。

オプション	**説明**
高 - 高精細オーディオ	エンドポイントデバイスがネイティブデータ転送速度でサウンドファイルを再生できるようにします。 これは帯域幅が豊富で音質が重要な接続に適しています。
中 - スピーチ用に最適化	エンドポイントデバイスに送信されたすべてのサウンドを最大64Kbpsに圧縮するため、サウンドの品質が適度に低下します。 このオプションは、スピーチに適しており、ほとんどのLANベースの接続で推奨されます。
低速 - 低速接続用	エンドポイントデバイスに送信されたすべてのサウンドを最大16Kbpsに圧縮するため、サウンドの品質が大幅に低下します。 このオプションは、帯域幅の狭い接続に適しており、低速接続中に妥当なオーディオ性能を実現します。
オフ	開いているICAセッションでオーディオ再生を無効にします。

暗号化	プルダウンメニューをクリックして、目的の暗号化方式を選択します。 **基本設定**、**RC5 128ビット（ログインのみ）**、**RC5 40ビット**、**RC5 56ビット**、**RC5 128ビット**の5つのオプションを使用できます。
Windowsキーの組み合わせを適用	ドロップダウンメニューをクリックして、Windowsのキーの組み合わせを適用する場所を選択します。 次の3つのオプションを使用できます。**ローカルデスクトップ**、**リモートデスクトップ**、**フルスクリーンデスクトップのみ**。

XenAppの接続タイプの設定

チェック

- Webログオンの接続タイプの設定については、「XenAppの接続タイプの設定」（104ページ）を参照してください。
- XenDesktopの接続タイプの設定については、「XenDesktopの接続タイプの設定」（101ページ）を参照してください。
- サーバ接続の接続タイプの設定については、「サーバー接続の接続タイプの設定」（107ページ）を参照してください。

[**General**] サブタブ

サーバー設定	
項目	**説明**
セッション名	Citrix ICAセッションの名前を入力します。
接続タイプ	この表では、XenAppが選択されている場合に使用可能な設定についてのみ説明しています。 次の4つの接続タイプを使用できます。 **オプション** / **説明** Webログオン / Webブラウザ（Internet Explorer）のインターフェイスを使用して、アプリケーション、デスクトップ、およびコンテンツアクセスサービスを提供します。 XenDesktop / デスクトップ配信サービスを提供します。 XenApp / アプリケーション配信サービスを提供します。 サーバー接続 / 管理者用の完全なサーバーアクセスサービスを提供します（XenAppサーバーのみ）。
サーバーアドレス	XenAppがアクセスできるサーバーのIPアドレス/ FQDNを入力します。
ユーザー名	認証に使用されるユーザー/アカウント名を入力します。
パスワード	認証に使用するユーザーアカウントのパスワードを入力します。
ドメイン	サーバーのドメインを入力します。 **注意:** XenAppサーバーがどのドメインにも属していない場合は、完全なコンピュータ名またはサーバー名を入力します。
アプリケーション名	アプリケーション名を入力します。 **注意:** フィールドの前にある検索アイコン を使用して、使用可能なアプリケーションを検出できます。 詳細な手順については、「接続の種類：XenApp」（91ページ）を参照してください。

共通設定	
項目	**説明**
起動時の自動起動	Windows 10 IoT Enterpriseの起動時にCitrix ICAセッションを自動的に開くかどうかを選択します。 [**Yes**] を選択すると、システムにログインするたびにCitrix ICAセッションが自動的に開かれます。
アプリケーション終了時	Citrix ICAセッションが終了したときの対処方法を選択します。[**何もしない**]、[**アプリケーションを再起動する**]、[**リブートする**]、[**シャットダウンする**] の4つのオプションがあります。 **オプション** / **説明** 何もしない / Windows 10のIoT Enterpriseデスクトップに戻ります。 アプリケーションを再起動する / Citrix ICAセッションを再度開きます。 リブートする / シンクライアントを再起動します。 シャットダウンする / シンクライアントを無効にします。

[**Options**] サブタブ

ウィンドウ設定	
項目	**説明**
要求された色品質	プルダウンメニューをクリックして、Citrix ICAセッションのカラー品質を選択します。**優先度なし**、**ベタースピード（16ビット）**、**より良い外観（32ビット）**の3つのオプションがあります。 **オプション** / **説明** 優先度なし / 特定の色品質を優先しません。 ベタースピード（16ビット） / 16ビットのカラー品質は、表示速度を向上させるために使用されます。 より良い外観（32ビット） / デスクトップの外観を向上させるために、32ビットのカラー品質が使用されています。
ウィンドウサイズ	ドロップダウンメニューをクリックして、Citrix ICAセッションのウィンドウサイズを選択します。 **デフォルト**、**シームレス**、**全画面**、**640 x 480**、**800 x 600**、**1024 x 768**、**1280 x 1024**、および**1600 x 1200**の8つのオプションがあります。
デバイスマッピング	
項目	**説明**
ローカルドライブのマッピング	ドロップダウンメニューをクリックして、Citrix ICAセッションでローカルドライブのマッピングを有効または無効にします。 [**Yes**] を選択すると、この接続を介して起動したCitrix ICAセッションで、ローカルに接続されたドライブが使用可能になります。
ローカルシリアルポートのマッピング	ドロップダウンメニューをクリックして、Citrix ICAセッションでローカルシリアルデバイスのマッピングを有効または無効にします。 [**Yes**] を選択すると、起動したCitrix ICAセッションで、ローカルに接続されたシリアルデバイスが使用できるようになります。

ローカルプリンタのマッピング	ドロップダウンメニューをクリックして、Citrix ICAセッションでローカルプリンタのマッピングを有効または無効にします。 [**Yes**] を選択すると、この接続を介してローカルに接続されているプリンタが起動したCitrix ICAセッションで使用できるようになります。
接続設定	
項目	**説明**
ネットワークプロトコル	プルダウンメニューをクリックして、接続に使用するプロトコルを選択します。 3つのオプション、**TCP / IP**、**TCP / IP + HTTPサーバーの場所**、および **SSL / TLS + HTTPSサーバーの場所**。
オーディオ品質	ドロップダウンメニューをクリックして、オーディオ再生を無効にするか、Citrix ICAセッションで目的の音質を選択します。 ドロップダウンメニューをクリックして、オーディオの再生を無効にするか、Citrix ICAセッションでオーディオ再生の品質設定を構成します。**高 - 高精細オーディオ**、**中 - スピーチ用に最適化**、**低速 - 低速接続用**、および**オフ**の4つのオプションがあります。

オプション	**説明**
高 - 高精細オーディオ	エンドポイントデバイスがネイティブデータ転送速度でサウンドファイルを再生できるようにします。 これは帯域幅が豊富で音質が重要な接続に適しています。
中 - スピーチ用に最適化	エンドポイントデバイスに送信されたすべてのサウンドを最大64Kbpsに圧縮するため、サウンドの品質が適度に低下します。 このオプションは、スピーチに適しており、ほとんどのLANベースの接続で推奨されます。
低速 - 低速接続用	エンドポイントデバイスに送信されたすべてのサウンドを最大16Kbpsに圧縮するため、サウンドの品質が大幅に低下します。 このオプションは、帯域幅の狭い接続に適しており、低速接続中に妥当なオーディオ性能を実現します。
オフ	開いているICAセッションでオーディオ再生を無効にします。

暗号化	プルダウンメニューをクリックして、目的の暗号化方式を選択します。**基本設定**、**RC5 128ビット（ログインのみ）**、**RC5 40ビット**、**RC5 56ビット**、**RC5 128ビット**の5つのオプションを使用できます。
Windowsキーの組み合わせを適用	ドロップダウンメニューをクリックして、Windowsのキーの組み合わせを適用する場所を選択します。 次の3つのオプションを使用できます。**ローカルデスクトップ**、**リモートデスクトップ**、**フルスクリーンデスクトップのみ**。

サーバー接続の接続タイプの設定

チェック

- Webログオンの接続タイプの設定については、「Webログオンの接続タイプの設定」（99ページ）を参照してください。
- XenDesktopの接続タイプの設定については、「XenDesktopの接続タイプの設定」（101ページ）を参照してください。
- XenAppの接続タイプの設定については、「XenAppの接続タイプの設定」（104ページ）を参照してください。

[**General**] サブタブ

<table>
<tr><th colspan="2">サーバー設定</th></tr>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>セッション名</td><td>Citrix ICAセッションの名前を入力します。</td></tr>
<tr><td>接続タイプ</td><td>この表では、[Server Connection] が選択されている場合に使用可能な設定の説明のみが表示されます。

4つの接続タイプが利用可能です。
<table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>Webログオン</td><td>Webブラウザ（Internet Explorer）のインターフェイスを使用して、アプリケーション、デスクトップ、およびコンテンツアクセスサービスを提供します。</td></tr>
<tr><td>XenDesktop</td><td>デスクトップ配信サービスを提供します。</td></tr>
<tr><td>XenApp</td><td>アプリケーション配信サービスを提供します。</td></tr>
<tr><td>サーバー接続</td><td>管理者用の完全なサーバーアクセスサービスを提供します（XenAppサーバーのみ）。</td></tr>
</table></td></tr>
<tr><td>サーバーアドレス</td><td>XenAppサーバーのIPアドレス/ URL / FQDNを入力します。

注意: サーバー接続は、XenAppサーバーへの接続のみをサポートします。</td></tr>
<tr><td>ユーザー名</td><td>認証に使用されるユーザー/アカウント名を入力します。</td></tr>
<tr><td>パスワード</td><td>認証に使用するユーザーアカウントのパスワードを入力します。</td></tr>
<tr><td>ドメイン</td><td>サーバーのドメインを入力します。

注意: サーバーがどのドメインにも属していない場合は、完全なコンピューター/サーバー名を入力します。</td></tr>
</table>

共通設定	
項目	**説明**
起動時の自動起動	Windows 10 IoT Enterpriseの起動時にCitrix ICAセッションを自動的に開くかどうかを選択します。 [**Yes**] を選択すると、システムにログインするたびにCitrix ICAセッションが自動的に開かれます。
アプリケーション終了時	Citrix ICAセッションが終了したときの対処方法を選択します。[**何もしない**]、[**アプリケーションを再起動する**]、[**リブートする**]、[**シャットダウンする**] の4つのオプションがあります。

オプション	**説明**
何もしない	Windows 10のIoT Enterpriseデスクトップに戻ります。
アプリケーションを再起動する	Citrix ICAセッションを再度開きます。
リブートする	シンクライアントを再起動します。
シャットダウンする	シンクライアントを無効にします。

[**Options**] サブタブ

ウィンドウ設定	
項目	**説明**
要求された色品質	プルダウンメニューをクリックして、Citrix ICAセッションのカラー品質を選択します。**優先度なし**、**ベタースピード（16ビット）**、**より良い外観（32ビット）**の3つのオプションがあります。

オプション	**説明**
優先度なし	特定の色の品質の好みはありません。
ベタースピード（16ビット）	16ビットのカラー品質は、表示速度を向上させるために使用されます。
より良い外観（32ビット）	デスクトップの外観を向上させるために、32ビットのカラー品質が使用されています。

ウィンドウサイズ	ドロップダウンメニューをクリックして、Citrix ICAセッションのウィンドウサイズを選択します。**デフォルト**、**シームレス**、**全画面**、**640 x 480**、**800 x 600**、**1024 x 768**、**1280 x 1024**、および**1600 x 1200**の8つのオプションがあります。
デバイスマッピング	
項目	**説明**
ローカルドライブのマッピング	ドロップダウンメニューをクリックして、Citrix ICAセッションでローカルドライブのマッピングを有効または無効にします。 [**Yes**] を選択すると、この接続を介して起動したCitrix ICAセッションで、ローカルに接続されたドライブが使用可能になります。
ローカルシリアルポートのマッピング	ドロップダウンメニューをクリックして、Citrix ICAセッションでローカルシリアルデバイスのマッピングを有効または無効にします。 [**Yes**] を選択すると、起動したCitrix ICAセッションで、ローカルに接続されたシリアルデバイスが使用できるようになります。

ローカルプリンタのマッピング	ドロップダウンメニューをクリックして、Citrix ICAセッションでローカルプリンタのマッピングを有効または無効にします。 [**Yes**] を選択すると、この接続を介してローカルに接続されているプリンタが起動したCitrix ICAセッションで使用できるようになります。
接続設定	
項目	**説明**
ネットワークプロトコル	プルダウンメニューをクリックして、接続に使用するプロトコルを選択します。 3つのオプション、**TCP / IP**、**TCP / IP + HTTPサーバーの場所**、および **SSL / TLS + HTTPSサーバーの場所**。
オーディオ品質	ドロップダウンメニューをクリックして、オーディオ再生を無効にするか、Citrix ICAセッションで目的の音質を選択します。 ドロップダウンメニューをクリックして、オーディオの再生を無効にするか、Citrix ICAセッションでオーディオ再生の品質設定を構成します。 **高 - 高精細オーディオ**、**中 - スピーチ用に最適化**、**低速 - 低速接続用**、および**オフ**の4つのオプションがあります。
暗号化	プルダウンメニューをクリックして、目的の暗号化方式を選択します。 **基本設定**、**RC5 128ビット（ログインのみ）**、**RC5 40ビット**、**RC5 56ビット**、**RC5 128ビット**の5つのオプションを使用できます 。
Windowsキーの組み合わせを適用	ドロップダウンメニューをクリックして、Windowsのキーの組み合わせを適用する場所を選択します。 次の3つのオプションを使用できます。**ローカルデスクトップ**、**リモートデスクトップ**、**フルスクリーンデスクトップのみ**。

オプション	**説明**
高 - 高精細オーディオ	エンドポイントデバイスがネイティブデータ転送速度でサウンドファイルを再生できるようにします。 これは帯域幅が豊富で音質が重要な接続に適しています。
中 - スピーチ用に最適化	エンドポイントデバイスに送信されたすべてのサウンドを最大64Kbpsに圧縮するため、サウンドの品質が適度に低下します。 このオプションは、スピーチに適しており、ほとんどのLANベースの接続で推奨されます。
低速 - 低速接続用	エンドポイントデバイスに送信されたすべてのサウンドを最大16Kbpsに圧縮するため、サウンドの品質が大幅に低下します。 このオプションは、帯域幅の狭い接続に適しており、低速接続中に妥当なオーディオ性能を実現します。
オフ	開いているICAセッションでオーディオ再生を無効にします。

4.5.9 VMware Viewの基本的な接続設定の構成

VMware Viewの設定では、VMware ViewまたはHorizon Viewデスクトップサービスの View接続設定を構成し、デスクトップにショートカットを作成し、サービスアクセスのためにStartメニューを作成できます。 これらのショートカットを使用するだけで、オンデマンドデスクトップサービスにアクセスできます。

チェック

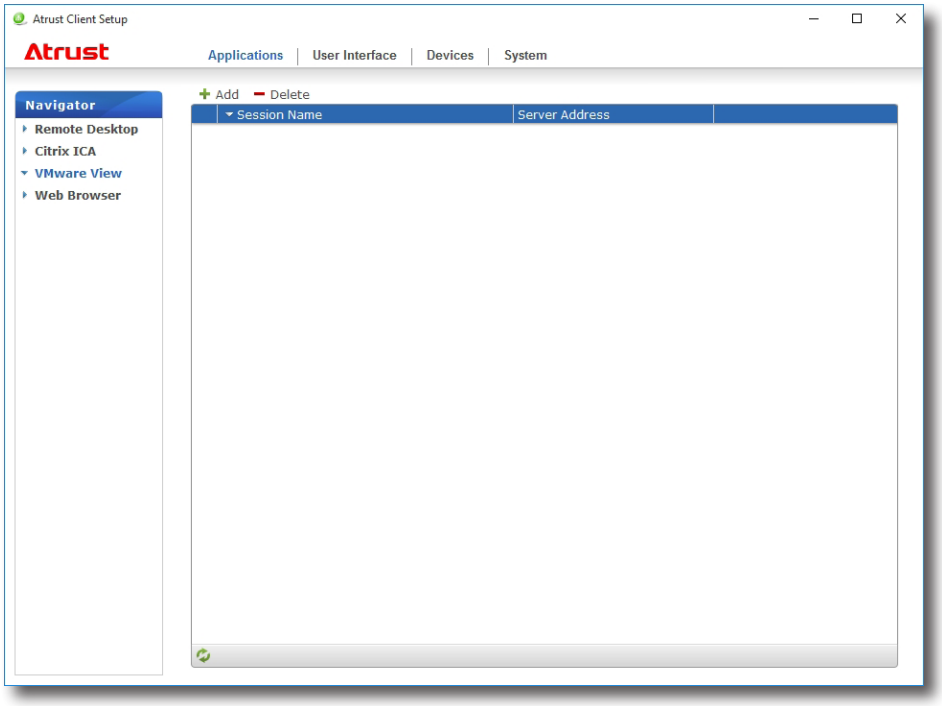
- VMwareデスクトップ仮想化ソリューションの詳細については、VMwareのWebサイト www.vmware.comを参照してください。

チェック

- 標準のデスクトップショートカットVMware Horizon View Clientを使用して、VMware ViewまたはHorizon Viewサービスにアクセスすることもできます。標準のデスクトップショートカットを使用してサービスにアクセスする方法の詳細については、第3章“入門” on page 17またはt68Wのクイックスタートガイドを参照してください。
- 以下のセクションでは、デスクトップに独自のサービスアクセスショートカットを作成する手順について説明します。

VMware Viewの接続設定をすばやく設定するには、以下を実行してください。

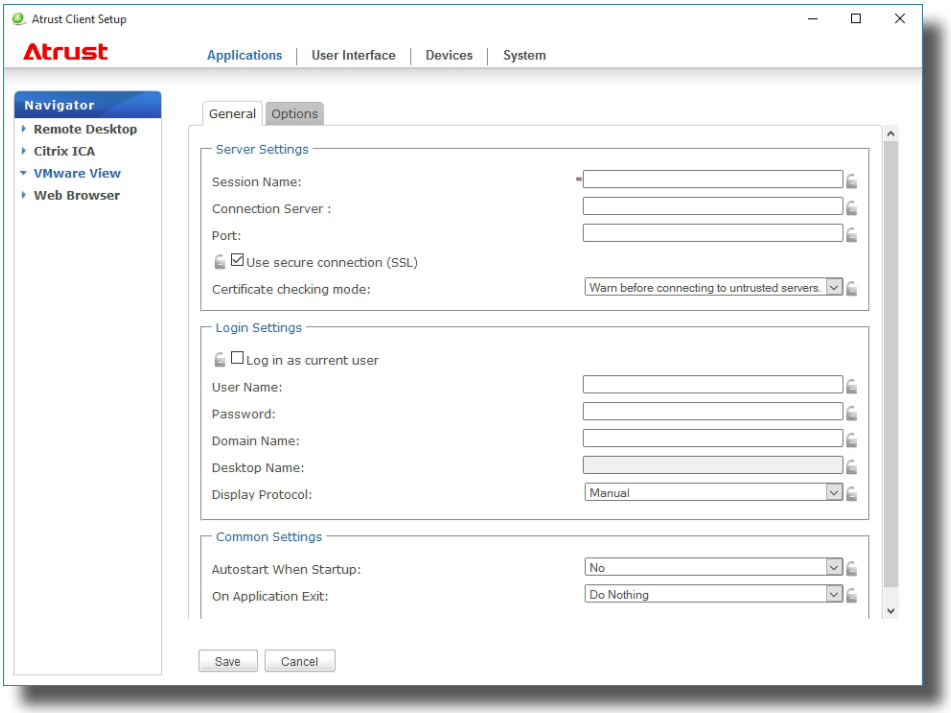
1. Atrust Client Setupで、[**Applications**] > [**VMware View**] をクリックします。
2. [View Connection] リストが [Configuration] 領域に表示されます。



チェック

- エントリを作成していない場合、View Connectionリストは空になります。

3. [View Connection] リストの上部にある [**Add**] をクリックして、View接続の新しいエントリを追加します。



4. 目的のセッション名を入力し、[**Save**] をクリックして確認します。

チェック

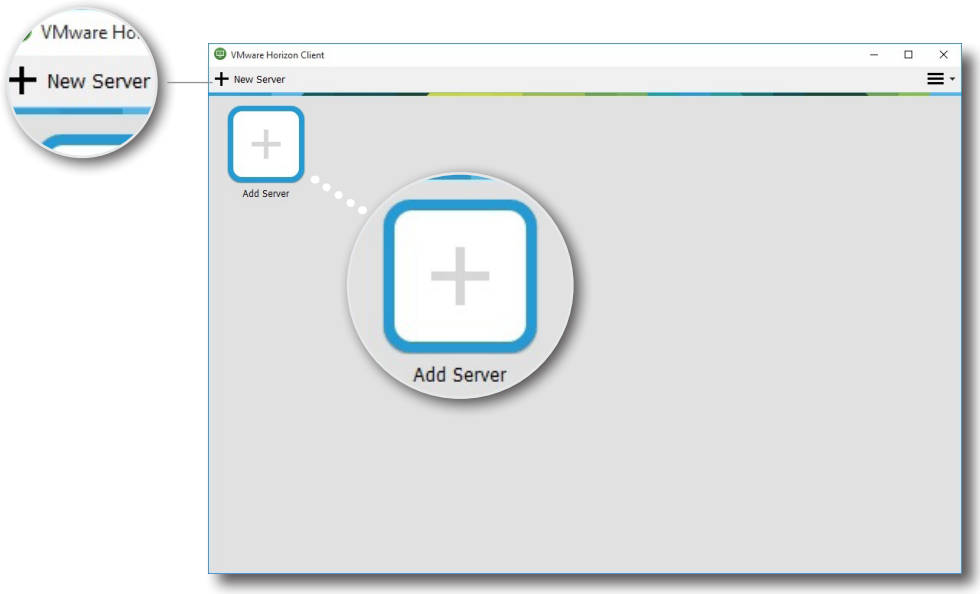
- これは、デスクトップ上にサービスアクセスショートカットを作成するために必要な唯一のフィールドです。 サービスアクセス期間中に他のデータを提供することができます。 必要に応じて、他のデータを入力することもできます。

5. 新しいエントリが [View Connection] リストに追加され、デスクトップにアクセスショートカットが自動的に作成されます。

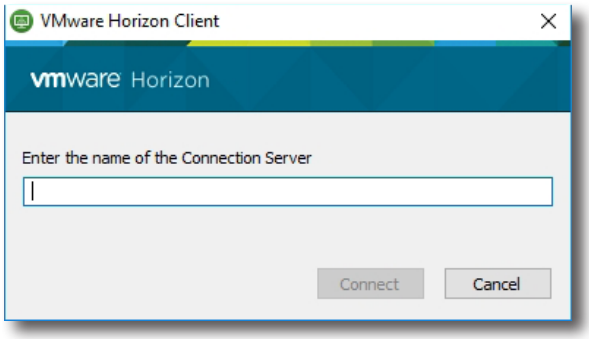
4.5.10 VMware ViewまたはHorizon Viewサービスへのアクセス

VMware ViewまたはHorizon Viewのサービスにアクセスするには、以下を実行してください。

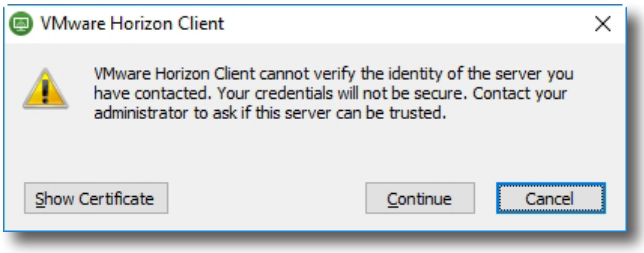
1. デスクトップ上に作成された（カスタマイズされた）アクセスショートカットをダブルクリックします。
2. View Connection Serverの名前またはIPアドレスを追加できるウィンドウが表示されます。
3. [**Add Server**] アイコンをダブルクリックするか、左上隅の [**New Server**] をクリックします。



4. View Connection Serverの名前またはIPアドレスの入力を求めるウィンドウが表示されます。 必要な情報を入力し、[**Connect**] をクリックします。

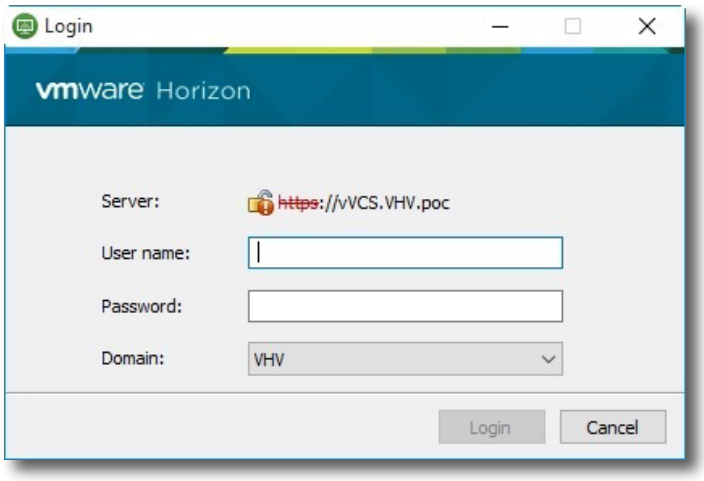


5. ウィンドウにリモートサーバーに関する証明書メッセージが表示されることがあります。 詳細についてはIT管理者に相談し、最初に接続が安全であることを確認してください。 バイパスするには、[**Continue**] をクリックします。

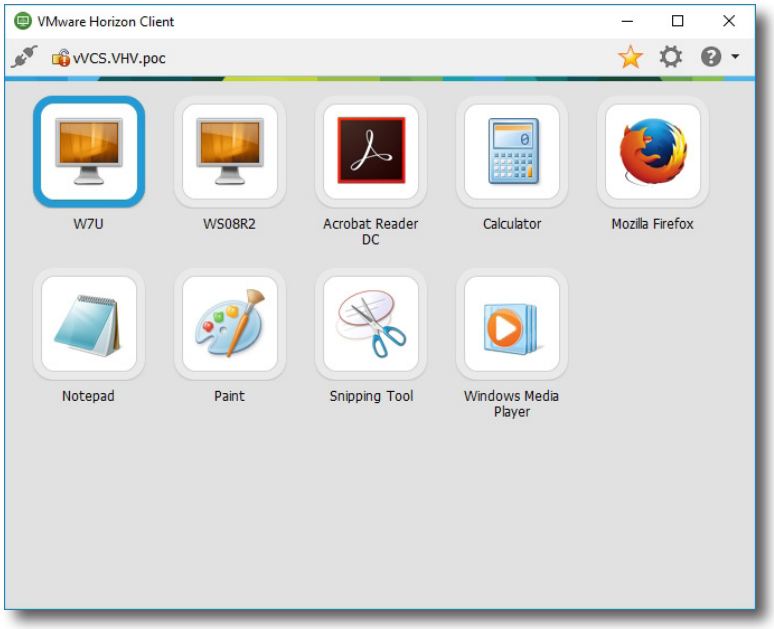


6. ウェルカムメッセージが表示されたウィンドウが表示されることがあります。 [**OK**] をクリックして続行します。

7. 開いたウィンドウにユーザー名とパスワードを入力し、[**Login**] をクリックします。



8. 使用可能なデスクトップまたはアプリケーションの資格情報のウィンドウが表示されます。 目的のデスクトップまたはアプリケーションをダブルクリックして選択します。



9. デスクトップまたはアプリケーションが画面に表示されます。

4.5.11 詳細ビュー接続設定の構成

下の表は、View接続の各設定項目の説明です。 この表を参照して、デスクトップ上の詳細設定とショートカットをカスタマイズし、サービスアクセスのための[スタート]メニューをカスタマイズしてください。

[**General**] サブタブ

サーバー設定	
項目	**説明**
セッション名	VMware ViewまたはHorizon Viewセッションの名前を入力します。
接続サーバー	View Connection Serverのコンピュータ名またはIPアドレスを入力します。 **注意:** View Connection Serverの詳細については、VMwareのWebサイト（www.vmware.com）を参照してください。
ポート	View Connection Serverとの通信に使用するポート番号を入力します。 デフォルト値を使用するには、単に空白のままにします。
セキュア接続（SSL）を使用	セキュア接続を有効/無効にするには、チェック/チェックを外します。
証明書検査モード	リモートサーバーのIDを確認するかどうか、および信頼されていないサーバーに接続するかどうかをクリックして選択します。[**サーバーID証明書を検証しない**]、[**信頼されていないサーバーに接続する前に警告する**]、[**信頼できないサーバーに接続しない**]、という3つのオプションがあります。

オプション	**説明**
サーバーID証明書を検証しない	リモートサーバーのIDを確認して、とにかく接続しないでください。
信頼されていないサーバーに接続する前に警告する	接続するかどうかを警告し、ユーザーが選択できるようにします。
信頼できないサーバーに接続しない	信頼できない接続を許可しません。

ログイン設定	
項目	**説明**
現在のユーザーとしてログインする	VMware ViewまたはHorizon Viewのサービスに現在のユーザー資格情報でログインする場合に選択します。 オンにすると、[User Name]、[Password]、および [Domain Name] フィールドはグレー表示されます。
ユーザー名	認証のためのユーザー名を入力します。
パスワード	認証のためにパスワードを入力します。
ドメイン名	View Connection Serverのドメイン名を入力します。
デスクトップ名	デスクトップ名を入力します。 または、ユーザーが空白のままにしておきます。 **注意:** 下の [Display Protocol] フィールドで [**Manual**] が選択されている場合、このフィールドはグレー表示されます。

表示プロトコル	プルダウンメニューをクリックして、表示プロトコルを選択します。 [**手動**]、[**Microsoft RDP**]、および [**PCoIP**] の3つのオプションが利用できます。 **オプション** / **説明** 手動 / 目的のディスプレイプロトコルを手動で選択します。 Microsoft RDP / ディスプレイプロトコルとしてMicrosoft RDPを使用します。 PCoIP / VMware PCoIPを表示プロトコルとして使用します。
共通設定	
項目	**説明**
起動時の自動起動	Windows 10 IoT Enterpriseの起動時に、VMware ViewまたはHorizon Viewのセッションを自動的に開くかどうかを選択します。 [**Yes**] を選択すると、システムにログインすると、VMware ViewまたはHorizon Viewセッションが自動的に開かれます。
アプリケーション終了時	VMware ViewまたはHorizon Viewセッションが終了したときの対処方法を選択します。 [**何もしない**]、[**アプリケーションを再起動する**]、[**リブートする**]、[**シャットダウンする**] の4つのオプションがあります。 **オプション** / **説明** 何もしない / Windows 10のIoT Enterpriseデスクトップに戻ります。 アプリケーションを再起動する / ViewまたはHorizon Viewセッションを再度開きます。 リブートする / シンクライアントを再起動します。 シャットダウンする / シンクライアントを無効にします。

[**Options**] サブタブ

ウィンドウ設定	
項目	**説明**
ディスプレー	ドロップダウンメニューをクリックして、Viewデスクトップの表示サイズを選択します。 [**フルスクリーン**]、[**マルチモニタ**]、[**ラージウィンドウ**]、[小さなウィンドウ]。 **オプション** / **説明** フルスクリーン / 選択したViewデスクトップをフルスクリーンで開きます。 マルチモニタ / 選択したViewデスクトップを複数のディスプレイで開きます。 ラージウィンドウ / 選択したViewデスクトップを大きなウィンドウで開きます。 小さなウィンドウ / 選択したViewデスクトップを小さなウィンドウで開きます。

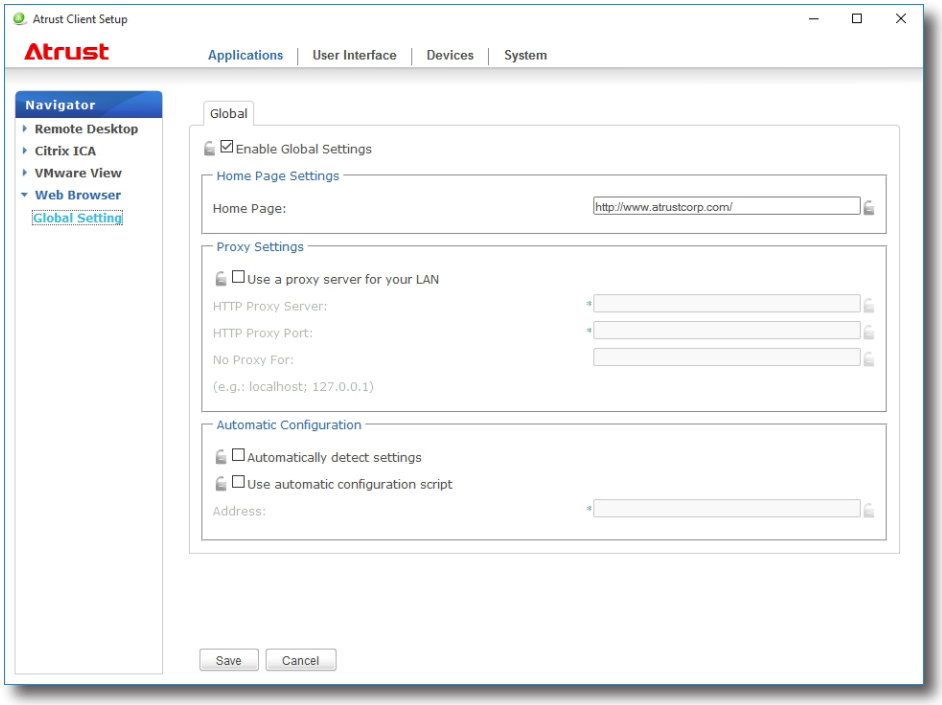
4.5.12 Webブラウザ設定の構成

[**Web Browser**] の設定項目では、ブラウザのセッション設定を構成し、デスクトップ上のショートカットやブラウザセッションの [Start] メニューを作成できます。

一般的なブラウザのセッション設定の構成

一般的なブラウザのセッション設定を行うには、以下を実行してください。

1. Atrust Client Setupで、[**Applications**] > [**Web Browser**] > [**Global Setting**] をクリックします。



2. 下の表を参照して、ホームページ、プロキシ、および自動構成設定を設定し、[**Save**] をクリックして適用します。

基本設定	
項目	**説明**
ホームページ	WebページのURLを入力すると、[Home] ボタンを使用して簡単にアクセスできます。
プロキシ設定	
項目	**説明**
LANにプロキシサーバーを使用する	ローカルエリアネットワークでプロキシサーバーを使用するかどうかをチェックします。
HTTPプロキシサーバー	プロキシサーバーのIPアドレスを入力します。
HTTPプロキシポート	プロキシサーバーの通信ポートを入力します。
プロキシなし	プロキシサーバーをバイパスするIPアドレスを入力します。

自動設定	
項目	**説明**
自動的に設定を検出する	ブラウザの設定を自動的に検出する場合にオンにします。
自動設定スクリプトを使用する	自動設定を許可し、設定ファイルが保存されているIPアドレスを指定します。
アドレス	[**Use automatic configuration script**] が選択されている場合は、IPアドレスを入力します。

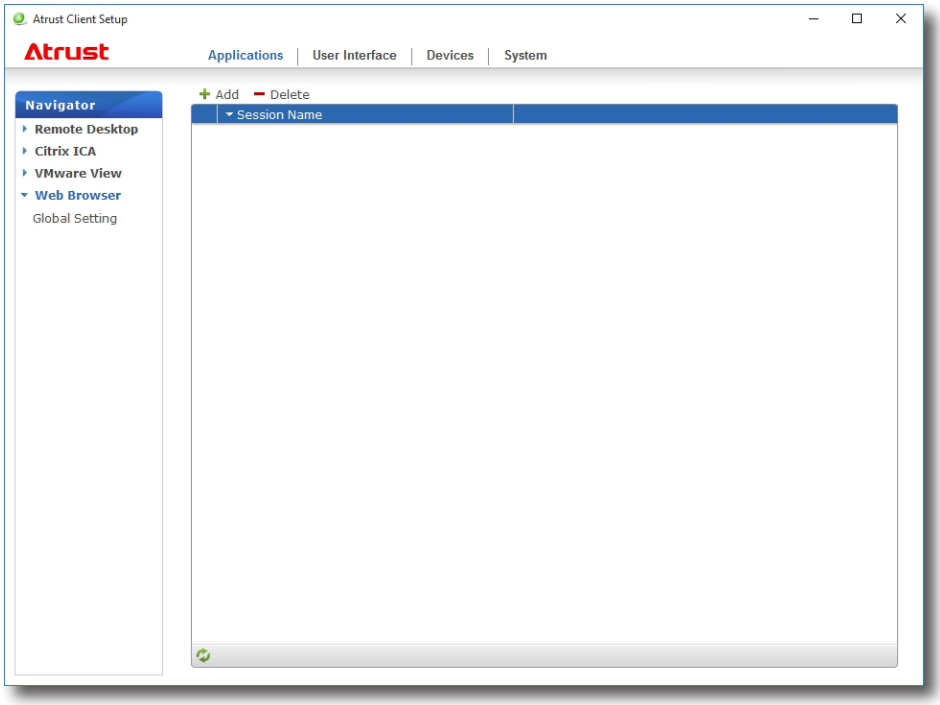
特定のブラウザセッション設定の構成

特定のブラウザーセッション設定を構成し、デスクトップと [Start] メニューにショートカットを作成するには、以下を実行してください。

ヒント

- この機能を使用して、特定のWebページ（イントラネットホームページなど）のデスクトップショートカットを作成できます。

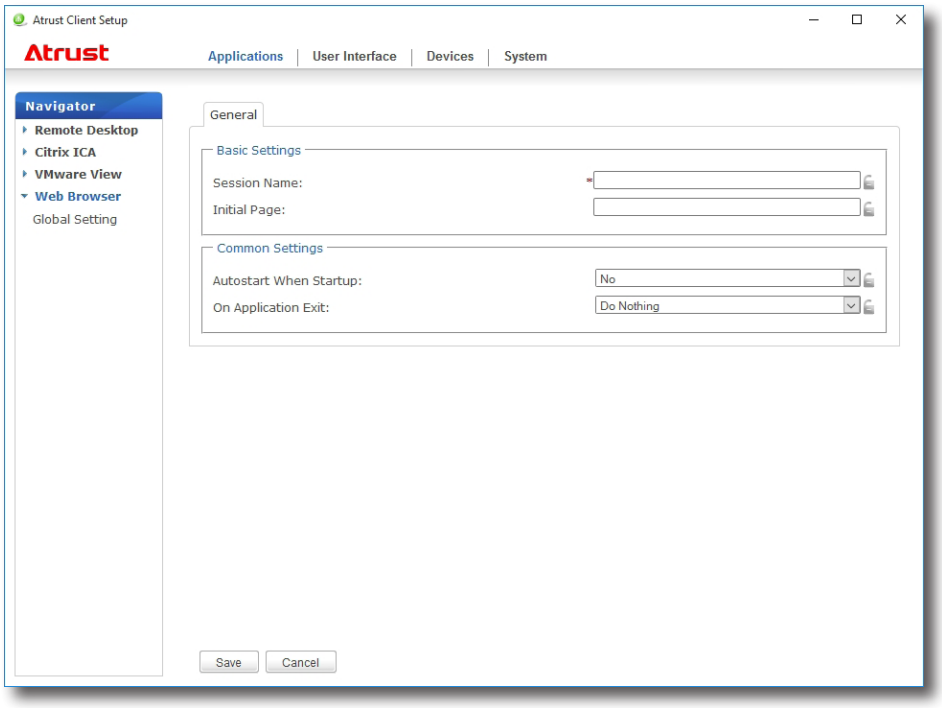
1. Atrust Client Setupで、[**Applications**] > [**Web Browser**] をクリックします。
2. ブラウザーセッションリストが構成領域に表示されます。



チェック

- エントリを作成していない場合、ブラウザセッションリストは空になります。

3. ブラウザセッションリストの上部にある [**Add**] をクリックします。
4. [**General**] サブタブで、目的のセッション名、初期WebページのURLを入力し、必要に応じてその他の設定を選択します（詳細は下の表を参照）。



共通設定	
項目	**説明**
起動時の自動起動	Windows 10 IoT Enterpriseの起動時にブラウザセッションを自動的に開くかどうかを選択します。 [**Yes**] を選択すると、システムにログインするたびにブラウザセッションが自動的に開かれます。
アプリケーション終了時	ブラウザセッションが終了したときに何をするかを選択します。 [**何もしない**]、[**アプリケーションを再起動する**]、[**リブートする**]、[**シャットダウンする**] の4つのオプションがあります。

オプション	**説明**
何もしない	Windows 10のIoT Enterpriseデスクトップに戻ります。
アプリケーションを再起動する	ブラウザセッションを再度開きます。
リブートする	シンクライアントを再起動します。
シャットダウンする	シンクライアントを無効にします。

5. [**Save**] をクリックして確認します。 アクセスショートカットはデスクトップ上に自動的に作成されます。

付録

この章では、t68Wシンクライアントのメンテナンスについて説明します。

A.1 t68Wのリセット

リセットモードでは、Atrust Client Setupの設定を工場出荷時のデフォルトに戻すことができます。 また、Atrustがリモートおよび大量クライアント管理用に開発した管理コンソールであるAtrust Device Managerの管理から、管理対象のt68Wをリリースします。

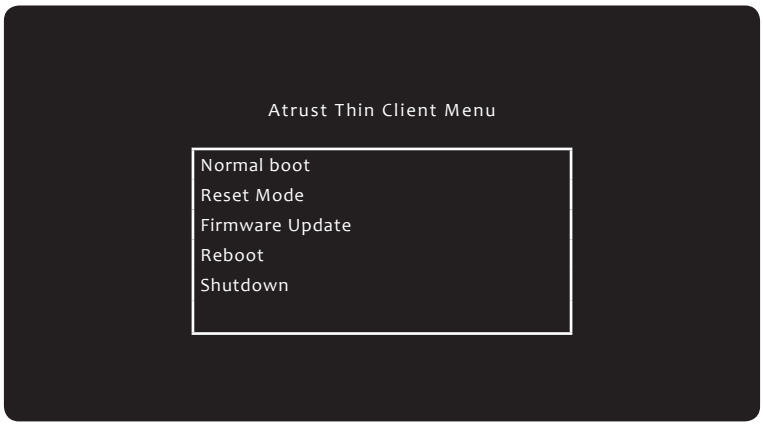
アトラストシンクライアントメニューからローカルに**リセットモード**を実行できます。

チェック

- また、管理対象のt68WをAtrust Device Managerから**リモート**で解放することもできます。 詳細は、Atrust Device Managerのユーザーズマニュアルを参照してください。

t68Wをリセットするには、以下を実行してください：

1. t68Wを再起動します。
2. 起動時に、キーボードの [**Esc**] キーを押してAtrust Thin Clientメニューに入ります。



チェック

- Atrustシンクライアントメニューには、**通常起動**、**リセットモード**、**ファームウェア更新**、**再起動**、**シャットダウン**の5つのオプションがあります。 各オプションの説明については、下の表を参照してください。

メニューオプション	説明
普通のブーツ	t68Wを通常の起動手順として起動します。
リセットモード	t68WのAtrust Client Setup設定とリモート管理ステータスをリセットします。
ファームウェアアップデート	t68Wのファームウェアをネットワーク経由でアップデートします。
リブート	t68Wを再起動します。
シャットダウン	t68Wをパワーオフします。

3. 矢印キーを使用して [**Reset Mode**] を選択し、[**Enter**] キーを押して続行します。
4. 確認のメッセージが表示されます。 確認するには、[**y**] と入力します。
5. 完了したら、[**Enter**] キーを押して再起動します。

A.2 t68Wのファームウェアのアップデート

t68Wのファームウェアをアップデートするには4つの方法があります：

方法	説明
Atrustシンクライアントメニュー	リモートコンピュータからファームウェアをダウンロードし、シンクライアント用のファームウェアを更新します。
USBフラッシュドライブ	Recovery USB Disk Creatorによって作成されたUSBフラッシュドライブでファームウェアを更新します。
Atrust Client Setup	Atrust Client Setupの助けを借りてシンクライアント上でローカルにファームウェアアップデートを開始します。
Atrust Device Manger	Atrust Device Managerを使用してリモートコンピュータ上でリモートからファームウェアのアップデートを開始します。

Atrustシンクライアントメニューの使用

アトラストシンクライアントメニューを使用してファームウェアをアップデートするには、以下を実行してください。

1. シンクライアントをネットワークに接続し、再起動します。
2. 起動時に、キーボードの [**Esc**] キーを押してAtrust Thin Clientメニューに入ります。
3. **ファームウェアアップデート**を選択し、画面の指示に従ってタスクを完了します。

> **チェック**
>
> - ネットワーク経由でファームウェアサーバのIPアドレスを指定する必要があります。 ファームウェアサーバは、Atrust Device Managerがインストールされ、クライアントファームウェアファイルがAtrust Device Managerを介してインポートされるサーバです。
> - Atrust Device Managerの詳細については、Atrust Device Managerのユーザーズマニュアルを参照してください。

USBフラッシュドライブの使用

Recovery USB Disk Creatorで作成されたUSBフラッシュドライブを使用してファームウェアを更新するには、次の手順を実行してください。

> **チェック**
>
> - Recovery USB Disk Creatorを使用してUSBフラッシュドライブを作成する方法については、クイックガイドfor USB Creatorを参照してください。

1. USBフラッシュドライブを接続し、シンクライアントを再起動します。
2. 起動時に、[**F7**] キーを押してBoot Deviceメニューに入ります。
3. そのメニューのUSBフラッシュドライブを選択し、Atrust Thin Client Recovery System画面に入ります。
4. 画面の指示に従ってタスクを完了します。

Atrust Client Setupの使用

Atrust Client Setupを使用してファームウェアをアップデートするには、40ページの「4.2.5 管理コンピュータからのファームウェアの更新」のセクションを参照してください。

Atrust Device Managerの使用

Atrust Device Managerを使用してファームウェアを更新するには、Atrust Device Managerのユーザーズ・マニュアルを参照してください。

仕様

Atrust t68W シン・クライアント

プロセッサー	Intel® Celeron® N2807, Dual-core, 1.58 GHz
ランダム・アクセス・メモリ	4 GB
フラッシュメモリー	mSATA DOM 16 GB (最大64 GB)
解像度	最大1920 x 1200
I/Oポート	フロント: 2 x USB 2.0 1 x マイク 1 x ヘッドホン リア: 2 x USB 2.0 1 x DVI-I 1 x RJ-45 1 x DC IN
ネットワーク	1 x 10/100/1000Mb Ethernet
電源	入力/出力：100-240Vac, 0.5A, 50-60Hz / DC +5Vdc, 3A
オペレーティングシステム	Windows 10 IoT Enterprise
プロトコル	Microsoft RDP with RemoteFX / Citrix ICA with HDX / VMware PCoIP
管理ツール	Atrust Client Setup / Atrust Device Manager
セキュリティ	1 x ケンジントンロック
マウント	VESAマウントキット (W)114 x (H)6 x (D)60 mm (オプション)
サイズ	(W)135 x (H)29 x (D)93 mm
重量	約 278 g、ACアダプタを除く
環境	動作温度環境: 0° C ~ 35° C 対応温度環境: -30° C ~ 60° C 動作湿度環境 (Rh): 10% ~ 90% (結露なきこと) 対応湿度環境 (Rh): 5% ~ 95%