Wyse Thin Client の RAS 接続セットアップガイド

19

Parallels International GmbH
Vordergasse 59
8200 Schaffhausen
スイス
Tel: + 41 52 672 20 30
www.parallels.com/jp

© 2024 Parallels International GmbH. All rights reserved. Parallels および Parallels ロゴは、カナダ、米国またはその他の国における、Parallels International GmbH の商標または登録商標です。

Apple、Safari、iPad、iPhone、Mac、macOS、iPadOS は、Apple Inc.の登録商標です。Google、Chrome、Chrome OS、Chromebook は、Google LLC の登録商標です。

その他のすべての社名、製品名、サービス名、ロゴ、ブランド、またすべての登録商標または未登録商標は、識別の目的でのみ使用されているものであり、それぞれの所有者の独占的な財産となります。サードパーティに関わるブランド、名称、ロゴ、その他の情報、画像、資料の使用は、それらを推奨することを意味するものではありません。当社は、これらサードパーティに関わる情報、画像、素材、マーク、および他社の名称について所有権を主張するものではありません。特許に関するすべての通知と情報については、https://www.parallels.com/jp/about/legal/をご覧ください。

目次

はじめに....4
本ガイドの目的....4
注意事項....4
適用範囲....4
表記規則....4
概要....5
注意事項....5
RAS 接続設定....6
Wyse ブローカーの構成....6
DHCP サーバーの設定....6
RAS Secure Gateway の構成....9
証明書のインポート....12
証明書のエクスポート....12
WTOS ポリシー設定....13
証明書のインストール....13
AVD アプリケーション パッケージのインストール....14
セキュリティの設定....15
接続ブローカーの設定....16
接続確認....18

はじめに

本ガイドの目的

本ガイドは、Parallels® Remote Application Server (以降 RAS) の評価を目的に、初めて環境を構築されようとしているお客様や、販売店のエンジニア様に、シンプルなシステム構成で構築を完了し、RAS のリモート アクセスをお試しいただき体験いただくことを目的としております。

RAS 管理者ガイド (日本語) を、弊社 Web サイトに公開しておりますが、公開資料を補足する内容となっております。ぜひ、RAS 製品のシンプルで、かつ操作性の良いリモート アクセスを評価いただければ幸いです。

RAS 管理者ガイドを含むマニュアルの公開ページ
https://www.parallels.com/jp/products/ras/resources/

注意事項

- 本ガイドで紹介した仮想ネットワークおよび仮想サーバー等の導入に関しては自己責任での利用をお願いいたします。
- 本ガイドで示す環境構築および運用手順の実行に関しては、所属する組織等のセキュリティポリシーに必ず従ってください。
- 本ガイドに記載されている画面例、URL 等はガイド記載時のものとなるため、画面仕様が実際の画面とは異なることがありますのでご注意ください。
- 本ガイドに記載されている内容は、改善のため予告なしに変更される場合があります。あらかじめご了承下さい。
- 評価の際は、是非、インストール メディアのバージョンを含め、本ガイドの最新バージョンをご使用されることを推奨いたします。

適用範囲

本ガイドは、以下バージョンを対象としています。

- RAS Ver. 19

表記規則

本ガイド内の表記は、以下の規則に沿って行われています。

- RAS の画面に表示されるメニュー名/タブ名/プロパティ項目名/値/ボタン名は、[ ] で囲んで表記しています。
- 可変の値は < > で囲んで表記しています。

概要

本ドキュメントでは、Parallels RAS を Dell Wyse ThinOS™ (WTOS) / Thin Client で使用するための設定方法について説明します。

注意事項

- WTOS から RDS 環境へ接続するためには、商用の認証局 (CA) が必要です。
- RAS にてサポートされている OS バージョンにつきましては、管理者ガイドの「ソフトウェア要件」を参照してください。

RAS 接続設定

この章では、WTOS から RAS サーバーに接続する設定方法について説明します。

> 注 : WTOS から RDS 環境へ接続するためには、商用の認証局 (CA) が必要です。

この章の内容

Wyse ブローカーの構成 6
証明書のインポート 12
証明書のエクスポート 12

Wyse ブローカーの構成

公開デスクトップ/アプリケーションを RAS から WTOS に公開するために、Parallels Secure Gateway を Wyse ブローカーとして構成します。

DHCP サーバーの設定

Wyse を利用する際は、デフォルト以外の DHCP オプション (スコープ オプション) を新規に追加定義し、パラメーターを設定する必要があります。

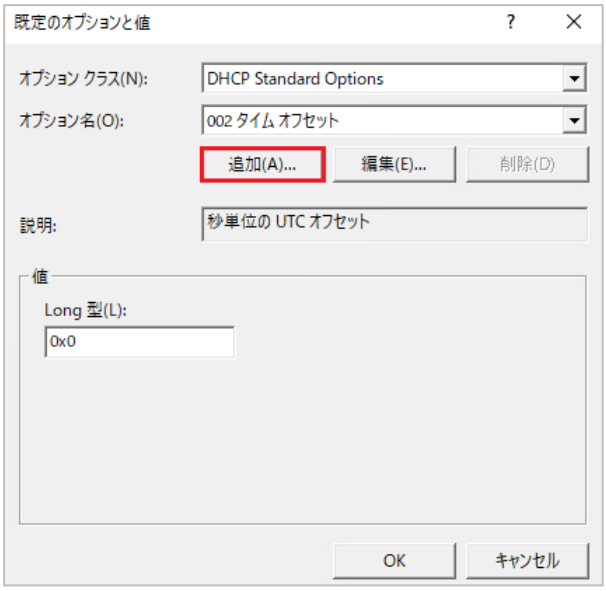
DHCP オプションを追加定義する手順は以下の通りです。

1 DHCP マシンにて、DHCP 管理ツール (dhcpmgnt.msc) を起動します。

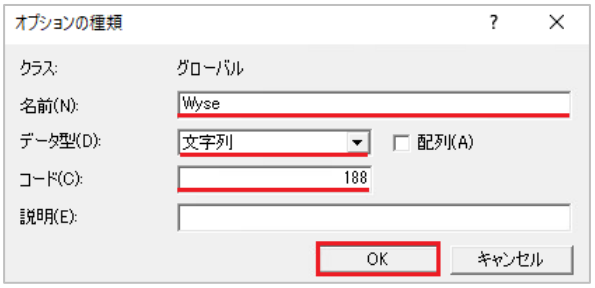
2 [IPv4] を右クリックし、[既定のオプションの設定] を選択します。



3 「既定のオプションと値」ウィンドウが表示されます。[追加] をクリックします。

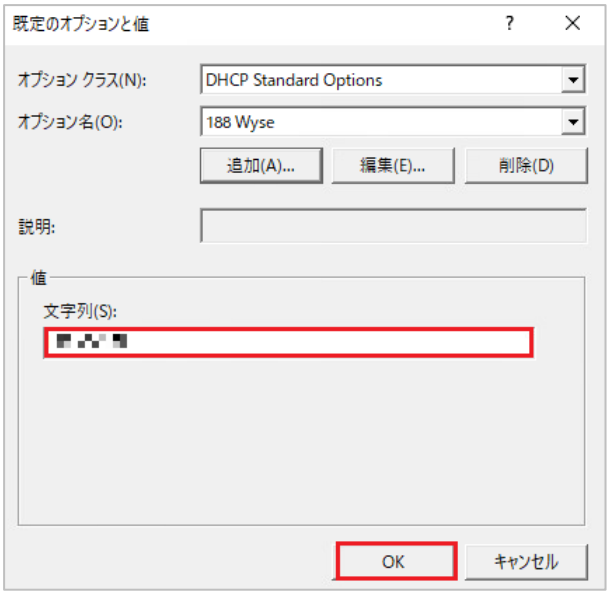


4 「オプションの種類」ウィンドウが表示されます。以下の値を設定し、[OK] をクリックします。

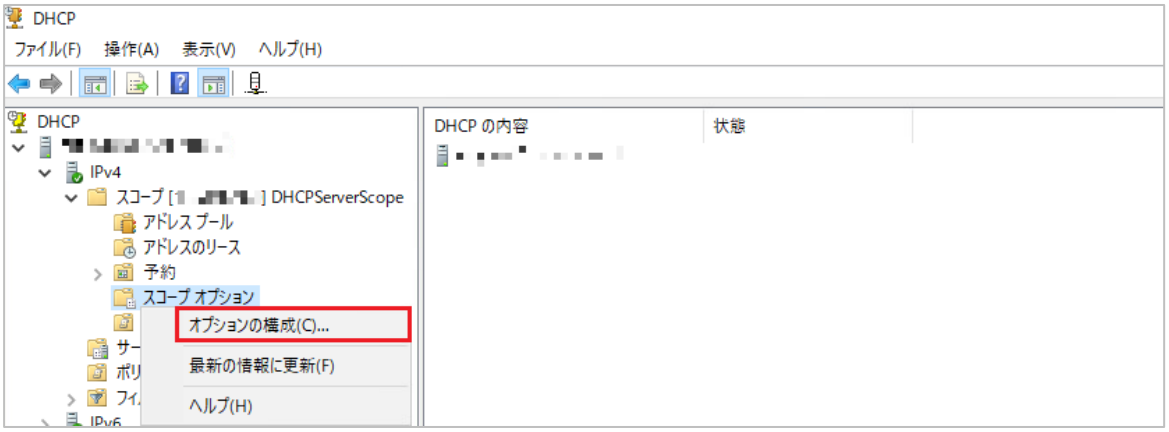


項目	説明	設定値
名前	DHCP のオプション名。	任意の値
データ型	オプションの型。	文字列
配列	複数の IP アドレスを渡す場合は、有効にします。	空欄
コード	DHCP のオプション番号。	188
説明	オプションの説明。	任意の値

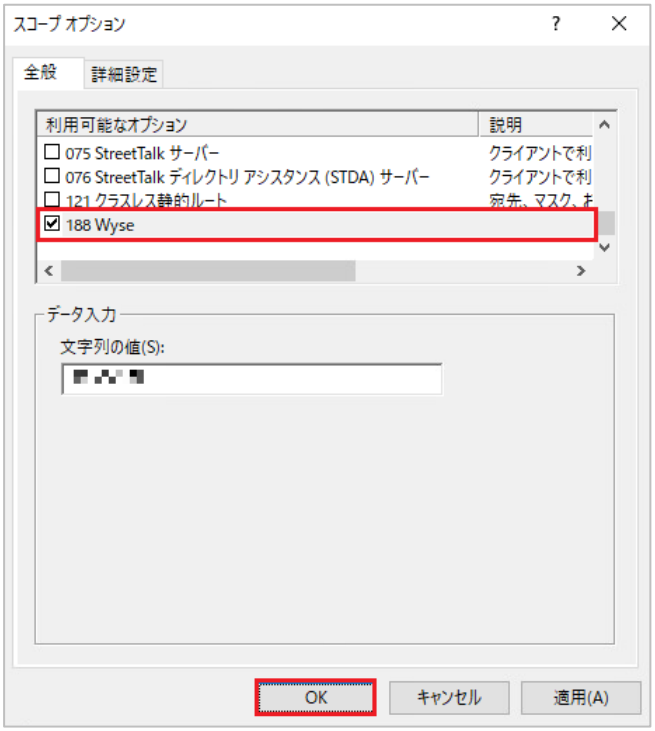
5 [値] フィールドに、Secure Gateway の IP またはホスト名を入力し、[OK] をクリックします。



6 [スコープ オプション] を右クリックし、[オプションの構成] を選択します。



7 「スコープオプション」ウィンドウが表示されます。[全般] タブにて、上記で追加した DHCP オプション [188] を選択し、[OK] をクリックします。



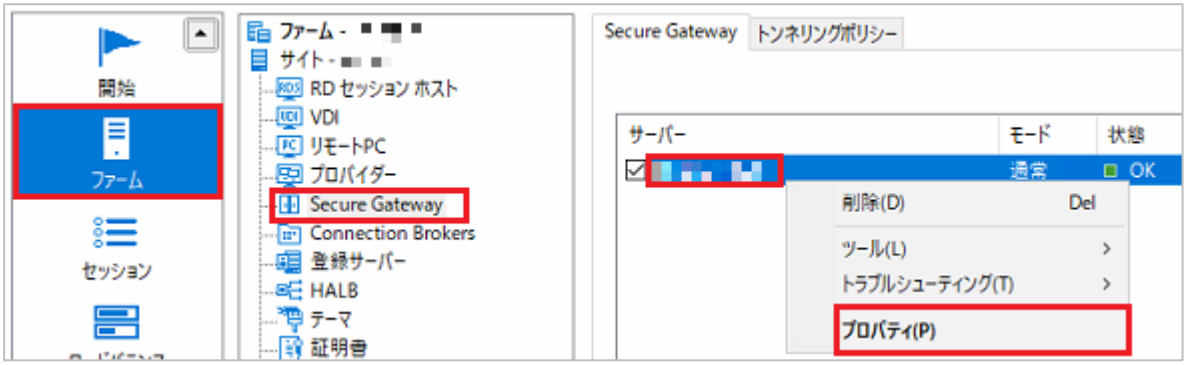
RAS Secure Gateway の構成

Wyse クライアントは、一般的な RAS 公開アプリケーションと互換性のない特定のブローカーを使用します。

Wyse ブローカーを有効化する手順は以下の通りです。

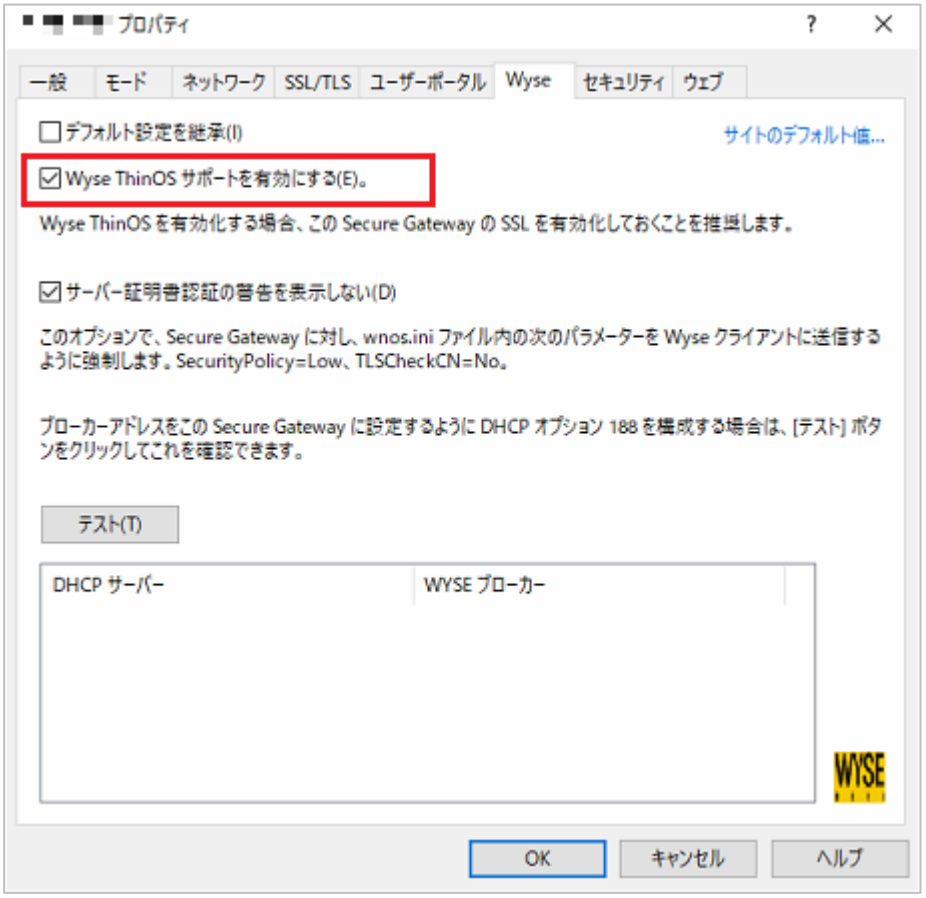
> 注 : 事前に、RAS Secure Gateway マシンで DHCP ポート UDP 67、68 を開く必要があります。

1 RAS Console を開き、[ファーム] > [Secure Gateway] にて、<Secure Gateway> を右クリックし、[プロパティ] を選択します。

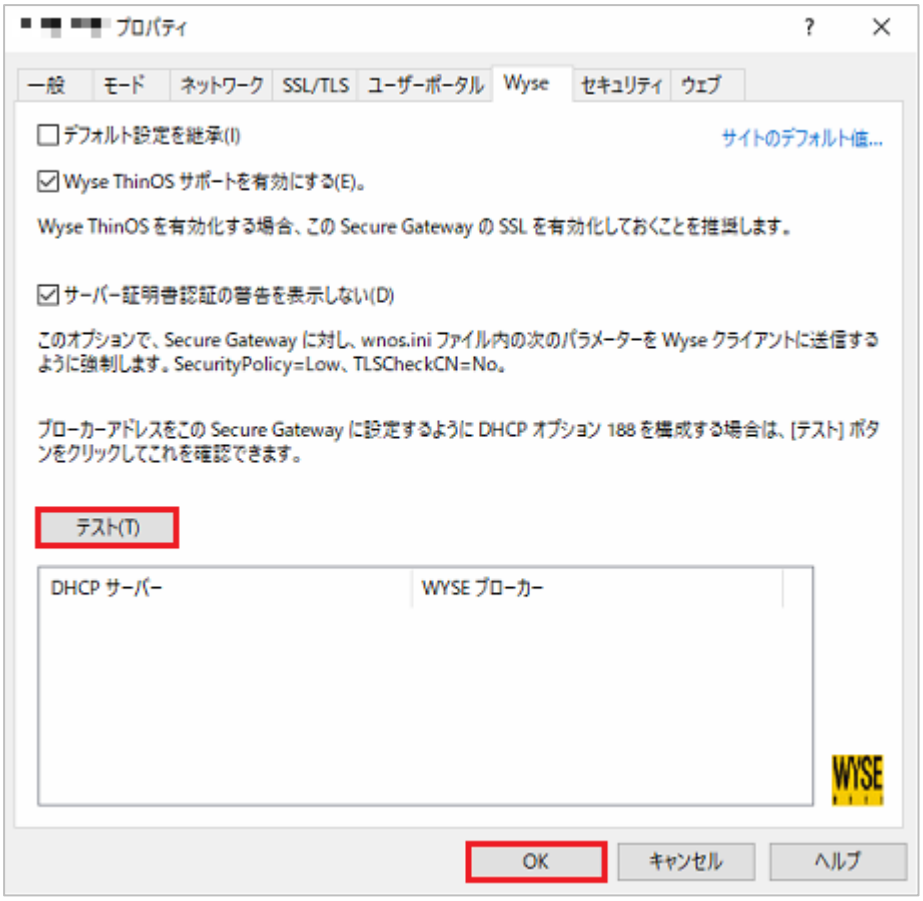


2 「プロパティ」ウィンドウが表示されます。[Wyse タブ] の [Wyse ThinOS サポートを有効にする] にチェックを付けます。

注 : [Wyse] タブは、ゲートウェイ モードが [通常] に設定されている場合にのみ使用できます。ゲートウェイ モードの詳細は、管理者ガイドの「ゲートウェイモードと転送設定」をご参照ください。



3 [テスト] を押して Wyse 設定を確認します。



注 : ホスト名が証明書と一致しないために、RAS Secure Gateway への接続時に Wyse デバイスで SSL 警告が表示される場合、[サーバー証明書認証の警告を表示しない] オプションを有効化してください。

証明書に以下の項目がある場合、このオプションは必要ありません:

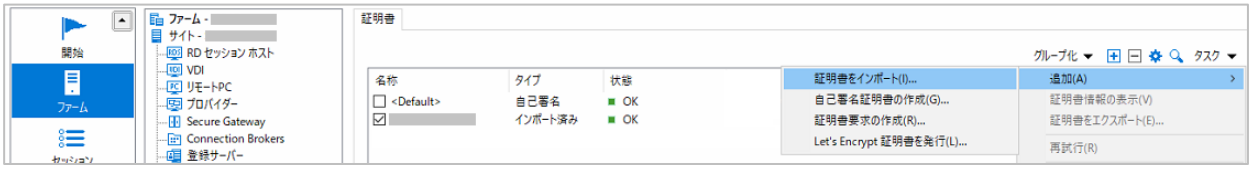
- CNAME が RAS Secure Gateway の FQDN に設定されている。
- SAN が RAS Secure Gateway の IP アドレスに設定されている。

証明書のインポート

WTOS の仕様上 RDS 環境へ接続するためには、商用の認証局 (CA) が必要です。

CA 証明書を RAS にインポートしてください。

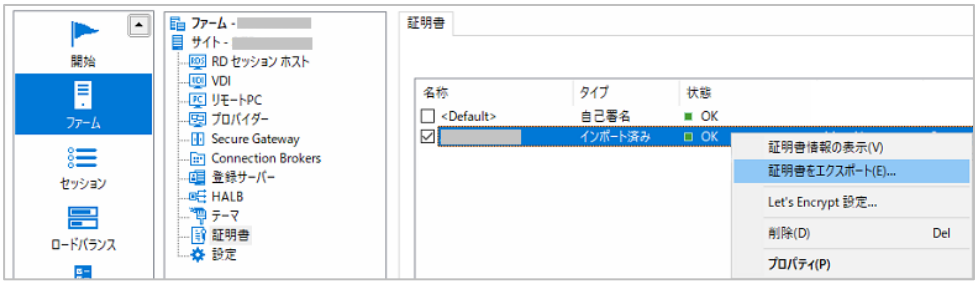
証明書インポートの詳細は、管理者ガイドの「証明書のインポート」をご参照ください。



証明書のエクスポート

サーバー証明書を WTOS にインポートするため、証明書をファイルにエクスポートします。

証明書エクスポートの詳細は、管理者ガイドの「証明書のエクスポート」をご参照ください。



WTOS ポリシー設定

「管理ポリシー ツール」または「Wyse Management Suite (WMS) 」を利用して Wyse シンクライアントのポリシーを構成します。WMS の詳細は、DELL の「Wyse Management Suite マニュアル」をご参照ください。

この章の内容

証明書のインストール....13
AVD アプリケーション パッケージのインストール....14
セキュリティの設定....15
接続ブローカーの設定....16
接続確認....18

証明書のインストール

RAS console から取得したサーバー証明書を WTOS にインストールします。

証明書をインストールする手順は以下の通りです。

1 「管理ポリシー ツール」または「Wyse Management Suite (WMS) 」の「設定制御」画面の左ペインの [詳細設定] を選択します。



2 [プライバシーおよびセキュリティ] > [証明書] の順に遷移し、[証明書の自動インストール] を [有効] にします。



3 [参照] をクリックし、アップロードする証明書を選択し、[開く] をクリックします。

注: WTOS は、.cer、.crt、.pfx、.der、.pem の証明書ファイル タイプをサポートしています。



4 [アップロードする証明書を選択] のドロップダウン リストから、アップロードした証明書を選択します。



5 [保存して公開] をクリックします。



AVD アプリケーション パッケージのインストール

OS バージョンに合わせた AVD アプリケーション パッケージを WTOS にインストールします。

AVD アプリケーション パッケージをインストールする手順は以下の通りです。

1 DELL Technologies から、Microsoft AVD パッケージをインストールします。

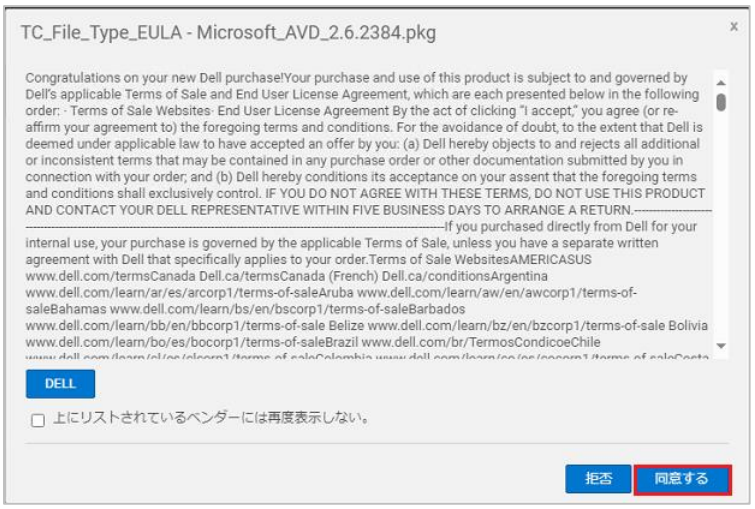
2 「管理ポリシー ツール」または「Wyse Management Suite (WMS) 」の「設定制御」画面の左ペインの [詳細設定] を選択します。

3 [ファームウェア] > [アプリケーション パッケージのアップデート] の順に遷移します。

4 [参照] をクリックし、アップロードする AVD アプリケーション パッケージを選択し、[開く] をクリックします。



5 [同意する] をクリックします。



6 [Microsoft AVD] 項目が「INSTALL」であることを確認します。



7 アプリケーション パッケージのリストをクリックして展開し、アップロードしたバージョンを選択します。



8 [保存して公開] をクリックします。



セキュリティの設定

ThinOS がサーバー証明書の共通名をチェックしないように設定します。

注 : このオプションを有効にすると、ThinOS クライアントは、フル セキュリティ モードで SSL 接続を設定するときに、サーバー証明書の共通名をチェックできます。

TLS チェッカーを無効化する手順は以下の通りです。

1 「管理ポリシー ツール」または「Wyse Management Suite (WMS) 」の「設定制御」画面の左ペインの [詳細設定] を選択します。

2 [プライバシーおよびセキュリティ] > [セキュリティ ポリシー] の順に遷移し、[TLS チェック CN] を [無効] にします。



3 [保存して公開] をクリックします。



接続ブローカーの設定

接続ブローカーの場所が認識されると、WTOS 起動後、自動的に接続ブローカーに接続してログインします。

接続ブローカーを設定する手順は以下の通りです。

1 「管理ポリシー ツール」または「Wyse Management Suite (WMS) 」の「設定制御」画面の左ペインの [詳細設定] を選択します。

2 [ブローカー設定] > [グローバル ブローカー設定] の順に遷移し、[デフォルトのブローカー タイプ] で [その他のブローカー] を選択します。



3 [その他のブローカー] に遷移し、[ブローカー サーバー] に [<RAS Secure Gateway の URL (FQDN 形式)>] を入力します。



4 [ログイン エクスペリエンス] > [ログイン設定] の順に遷移し、[ログイン エクスペリエンス] の [パスワード変数を有効にする] を [有効] にします。



5 [デフォルトの資格情報] の [デフォルトのユーザー名] [パスワード] [デフォルト ドメイン] に有効なログイン情報を入力します。



6 [保存して公開] をクリックします。



接続確認

ポリシー設定を適用し、ブローカー接続を確認します。

1. WTOS を再起動します。ツールバーから [シャットダウン] > [システムを再起動] の順に選択し、[OK] をクリックします。
2. WTOS の再起動後、自動でブローカー接続が実行されます。
3. 認証に成功すると、左側ツールバーの [VDI メニュー] に、RAS によって定義された公開済みリソースが表示されます。