Dell Wyse ThinOS

バージョン 8.5.1　管理者ガイド

メモ、注意、警告について

メモ：メモに記載されている内容は、製品の使用方法に関する重要な情報です。

注意：注意は、ハードウェアが破損するかデータが失われるおそれがあることを示し、問題を防止する方法を説明します。

警告：警告は、損害、けが、または死亡の原因となる可能性があることを示しています。

2018 - 08

Rev. A02

はじめに

Dell Wyse ThinOS ファームウェアを実行するシンクライアントは、シンクライアントのセキュリティおよびパフォーマンスの最適化に特化して設計されています。この特定用途向けに設計された効率性の高いシンクライアントは、Citrix、Microsoft、VMware および Dell vWorkspace 環境やその他の主要インフラストラクチャで、ウイルスおよびマルウェアに抵抗力があり、アプリケーション、ファイルおよびネットワークリソースに極めて高速にアクセスできます。ThinOS ベースのシンクライアントは自己管理型で、電源投入から数秒で完全に稼働する、公開されている API がないローカルでアクセス可能なファイルシステムまたはブラウザです。ウイルスまたはマルウェアから保護するためにローカルの McAfee ウイルス対策ソフトウェアやファイアウォールは必要ありません。

このガイドについて

このガイドは、Wyse ThinOS を実行するシンクライアントの管理者を対象としています。このガイドでは、ThinOS 環境の設計および管理に役立つ情報と詳細なシステム設定について説明します。

サポート対象製品

表 1 にはサポート対象の Dell Wyse ThinOS 製品が記載されています。

表 1. サポート対象プラットフォーム（Wyse 5070 シンクライアント）

プラットフォーム	プロセッサ
Wyse 5070 シンクライアント	Celeron
Wyse 5070 シンクライアント	Pentium
Wyse 5070 Extended シンクライアント	Pentium

表 2. ファームウェアおよび BIOS のバージョン（Wyse 5070 シンクライアント）

プラットフォーム	ThinOS	ThinOS（PCoIP 対応）	BIOS バージョン	BIOS BIN ファイル名
Wyse 5070 シンクライアント（Celeron Processor）	X10_wnos	PX10_wnos	Dell BIOS 1.1.1	X10_bios.bin
Wyse 5070 シンクライアント（Pentium Processor）	X10_wnos	PX10_wnos	Dell BIOS 1.1.1	X10_bios.bin
Wyse 5070 Extended シンクライアント（Pentium Processor）	X10_wnos	PX10_wnos	Dell BIOS 1.1.1	X10_bios.bin

このガイドで必要な情報を見つける方法

有効な PDF ドキュメントで、Search ウィンドウまたは Find ツールバーを使用して、単語、一連の単語または部分語を探すことができます。これらの機能の詳細については、PDF リーダーのヘルプを参照してください。

テクニカルサポート

テクニカルリソース（セルフサービスポータル、ナレッジベース、ソフトウェアダウンロード、登録、延長保証／RMA、リファレンスマニュアル、お問い合わせ窓口など）にアクセスするには、www.dell.com/wyse/support を参照してください。

使用開始にあたって

次の情報を利用すると、短時間で基本事項を習得し、シンクライアントを使い始めることができます。

- First Boot ウィザードを使用した ThinOS の設定
- リモートサーバへの接続
- デスクトップの使用
- シンクライアント設定および接続設定の設定
- プリンタとの接続
- モニタとの接続
- シンクライアントのロック
- サインオフとシャットダウン
- 使用開始にあたっての補足情報

メモ：
ThinOS は、INI ファイルによって一元的に管理、設定され、使用環境内のすべてのサポート対象シンクライアントに対して、自動でアップデートと要求されたデフォルト設定を強制的に実行します。「一元設定：アップデートと設定の自動化」を参照してください。

INI ファイルが検出されない場合は、各シンクライアントのローカルのダイアログボックスを使用して、使用可能な設定を作成できます。ThinOS では、解像度、マウス、キーボードなど、ローカルで設定されるこれらの設定の多くを保存し、再起動後も維持します。ただし、INI ファイルが検出されると、再起動によって ThinOS はステートレスとなり、再起動後、ローカルで設定した設定は無視されて、INI ファイルに指定した設定が使用されます。

First Boot ウィザードを使用した ThinOS の設定

First Boot ウィザードは、ThinOS バージョン 8.5.1 を搭載した新しいシンクライアントを、初めて起動するときに実行されます。シンクライアントは、ThinOS システムのデスクトップに入る前に First Boot ウィザードアプリケーションを起動し、システム環境設定、インターネット接続設定、USB 設定の読み込み、管理ソフトウェア設定、ブローカー接続設定などの一連のタスクが実施できるようにします。

シンクライアントを工場出荷時のデフォルト設定にリセットして、First Boot ウィザードを開始することもできます。

次のフローチャートは、First Boot ウィザードの作業の流れを表わしています。

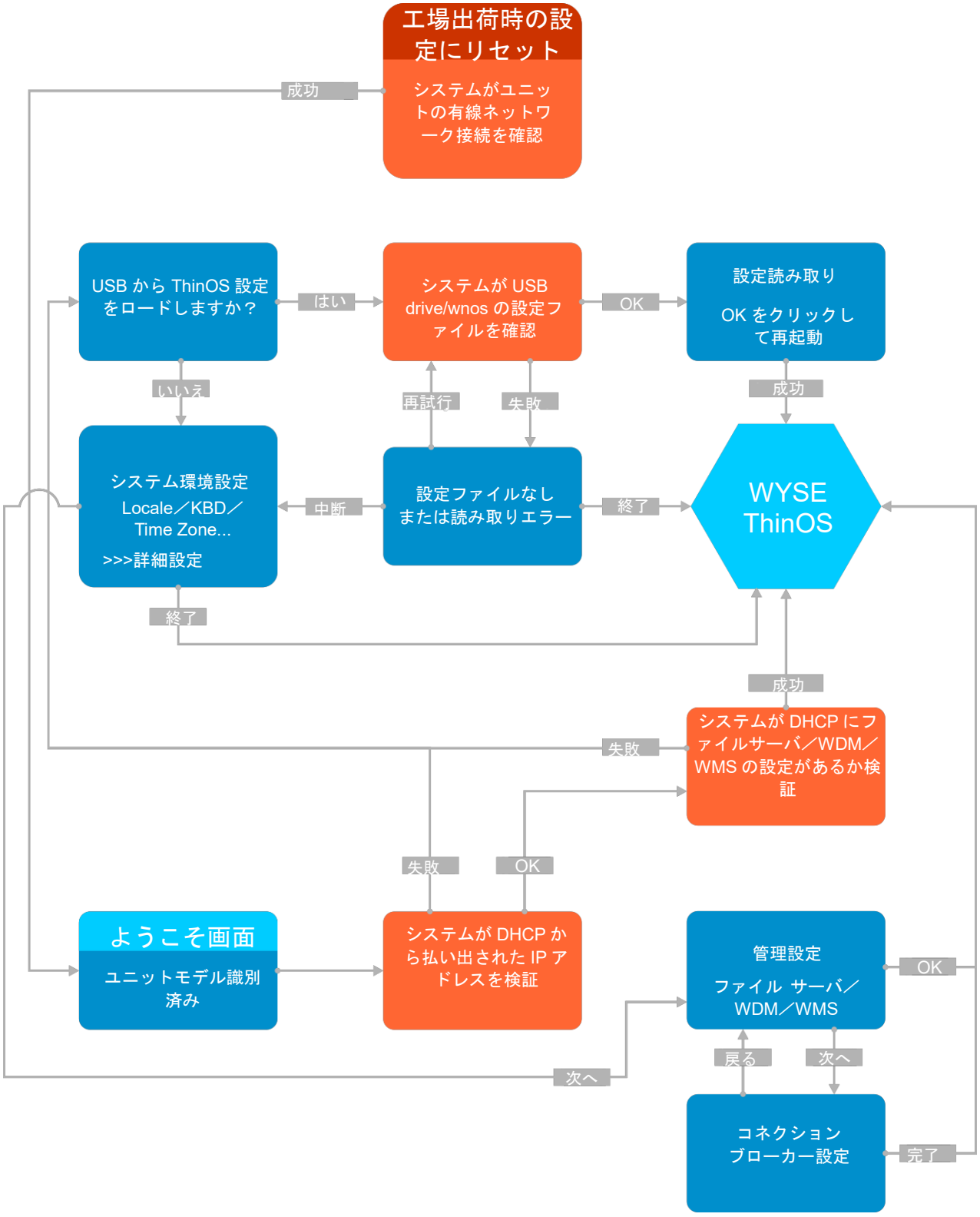


図 1.　First Boot ウィザード—ネットワーク接続に成功

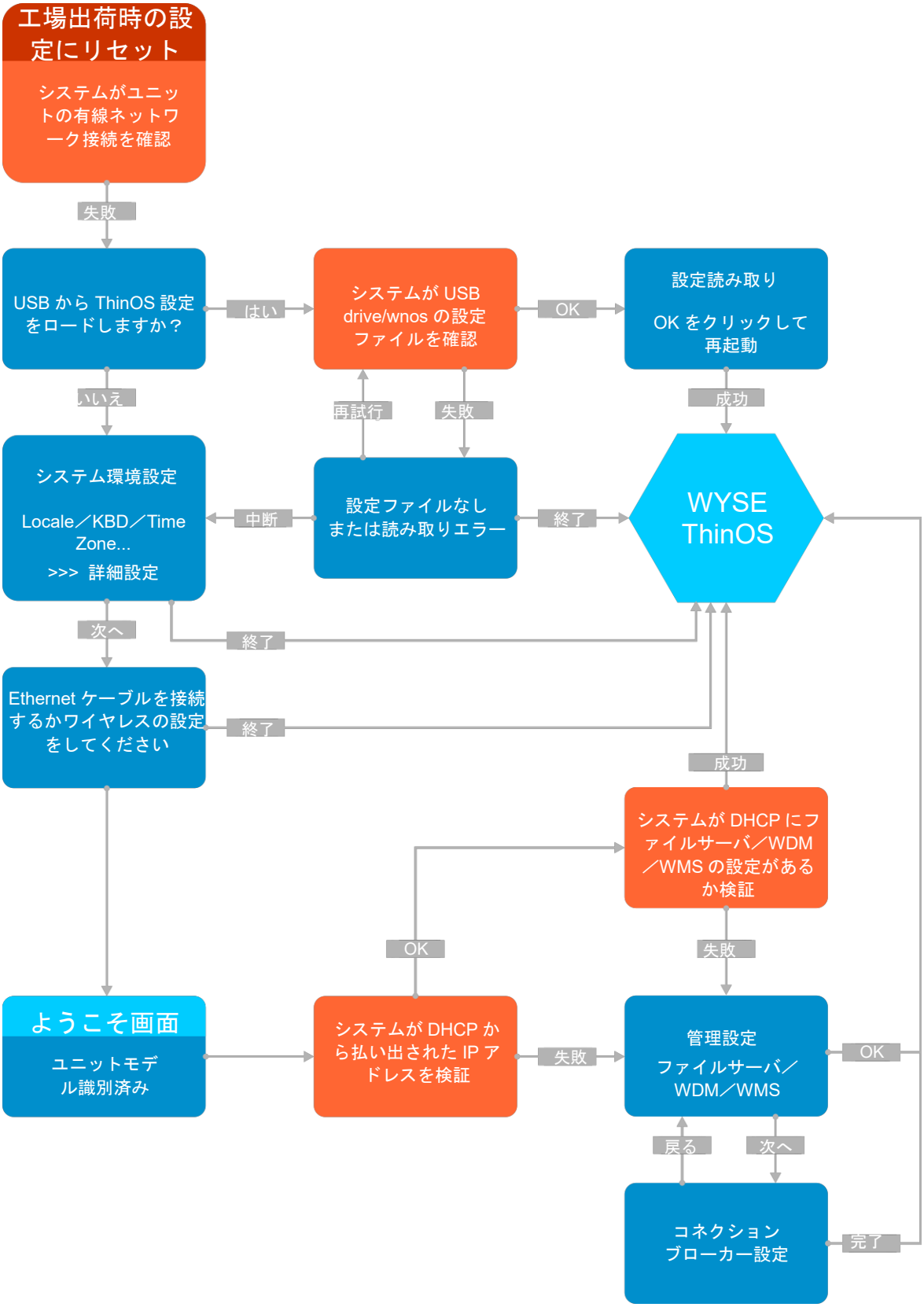


図 2.　First Boot ウィザード—ネットワーク接続に失敗

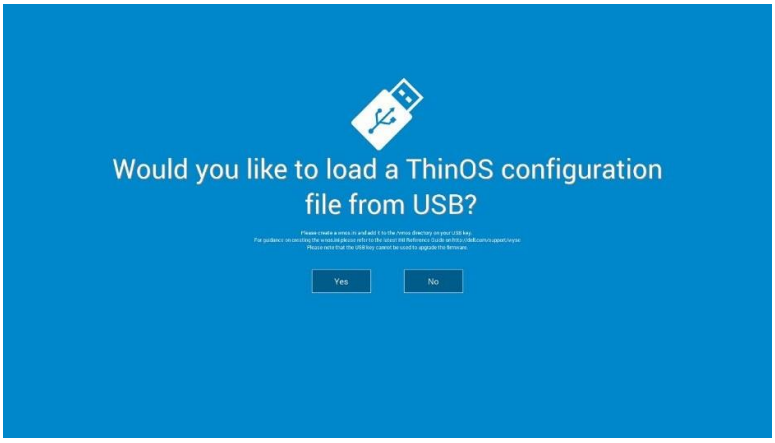
First Boot ウィザードを設定するには:

1 新しいシンクライアントまたは既存のシンクライアントを、有線接続を使って Ethernet に接続します。First Boot ウィザードを開始するためには、既存のシンクライアントを工場出荷時のデフォルト設定にリセットする必要があります。

2 シンクライアントの電源をオンにします。
シンクライアントが有線ネットワーク接続をチェックします。ネットワーク接続に成功したら、シンクライアントのモデル名が入った「ようこそ」画面が表示されます。
シンクライアントが DHCP から払い出された IP アドレスを検証します。DHCP にファイルサーバがあるか、Wyse Device Manager または Wyse Management Suite の設定がある場合、First Boot ウィザードを起動せず、ThinOS システムのデスクトップがロードされます。DHCP の検証でエラーになるか、Ethernet に接続していない場合は、次の手順に従います。

メモ：ようこそ画面でネットワーク接続状況のチェック中に First Boot ウィザードを終了する場合は、Ctrl + Esc キーを押します。

3 **ThinOS の設定を USB から読み込みますか** 画面で、次のいずれかの操作を行います。



- ThinOS 設定ファイルを USB メモリからロードするには、wnos.ini ファイルを作成し、USB ドライブの/wnos ディレクトリに、このファイルを追加する必要があります。このオプションを使えば、パッケージと、INI ファイルで指定されている壁紙をロードできます。USB メモリをシンクライアントに接続し、**はい**をクリックします。

メモ：USB メモリは FAT、FAT32、ExFAT ファイルシステムのみサポートされています。NTFS ファイルシステムはサポートされていません。

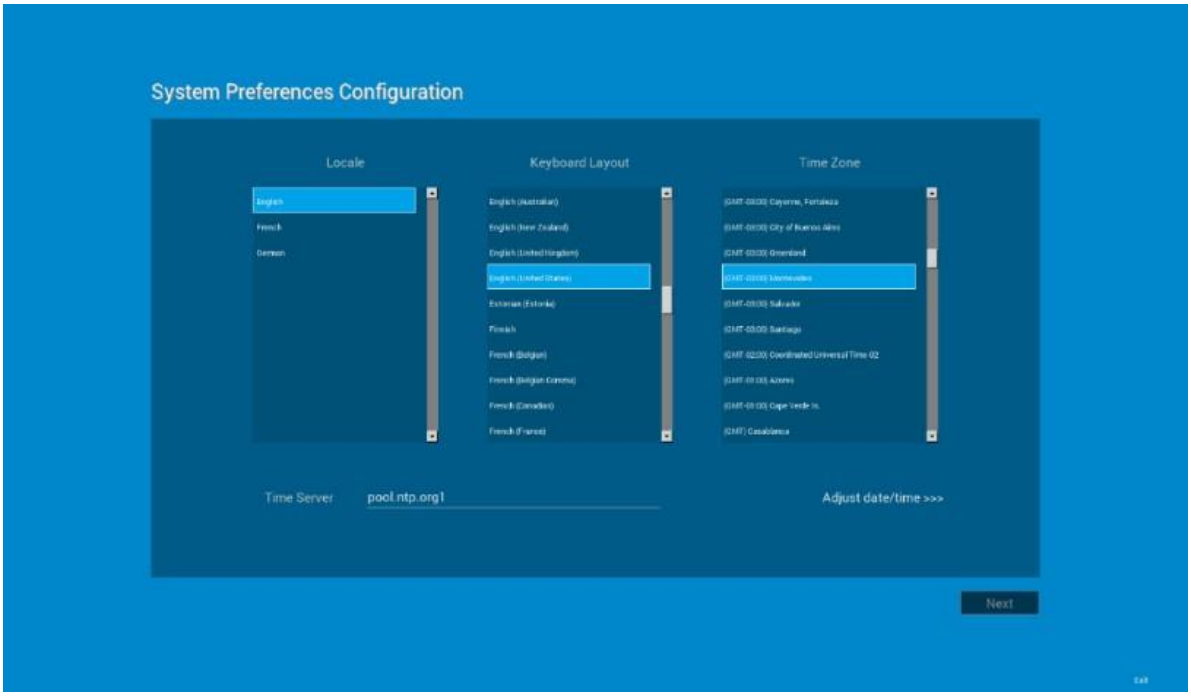
シンクライアントによって、USB ドライブの設定ファイルが検証されます。

– USB ドライブの ThinOS 設定ファイルが正しい場合は、**設定の読み込みに成功しました** メッセージが表示されます。**OK** をクリックして First Boot ウィザードを終了し、ThinOS システムデスクトップにログインします。
– USB ドライブの ThinOS 設定ファイルが破損したり、適切なファイルが使用できない場合、**設定ファイルが見つかりません、または設定ファイルの読み込みに失敗しました** メッセージが表示されます。USB ドライブに正しいファイルをアップロードした後、再度 USB メモリを接続し、リトライをクリックします。ファイルが正しい場合、**Read configuration success** メッセージが表示されます。**OK** をクリックして First Boot ウィザードを終了し、ThinOS システムデスクトップにログインします。
リトライオプションを使って ThinOS 設定ファイルをロードしない場合、**中止**をクリックして**システム設定**を開きます。

メモ：設定ファイルが見つかりません、または設定ファイルの読み込みに失敗しました メッセージ画面を終了して ThinOS システムデスクトップをロードするには、終了をクリックします。

- **システム**設定を開くには、**いいえ**をクリックします。

4 **システム**画面で、次のオプションを設定します。



- **ロケール**——言語を選択して、地域特定の言語で ThinOS を開始します。
- **キーボードレイアウト**——キーボードレイアウトを選択して、地域特定の言語のキーボードレイアウトを設定します。
- **タイムゾーン**——タイムゾーンを選択して、シンクライアントのタイムゾーンを設定します。
- **Time サーバー**——オプションのタイムサーバのポート番号とともに、IP アドレスまたはホスト名を表示します。
- **Advanced**——**Advanced** をクリックして、夏時間、時間のフォーマット、日付のフォーマット、タイムサーバなどの設定を行います。

メモ：システム設定 画面を終了して ThinOS システムデスクトップをロードするには、終了をクリックします。

Ethernet に接続していない場合は設定を続けることができず、**Ethernet ケーブルを接続してください**画面が表示されます。

次のいずれかの操作を行います。

- Ethernet ケーブルをシンクライアントに接続します。

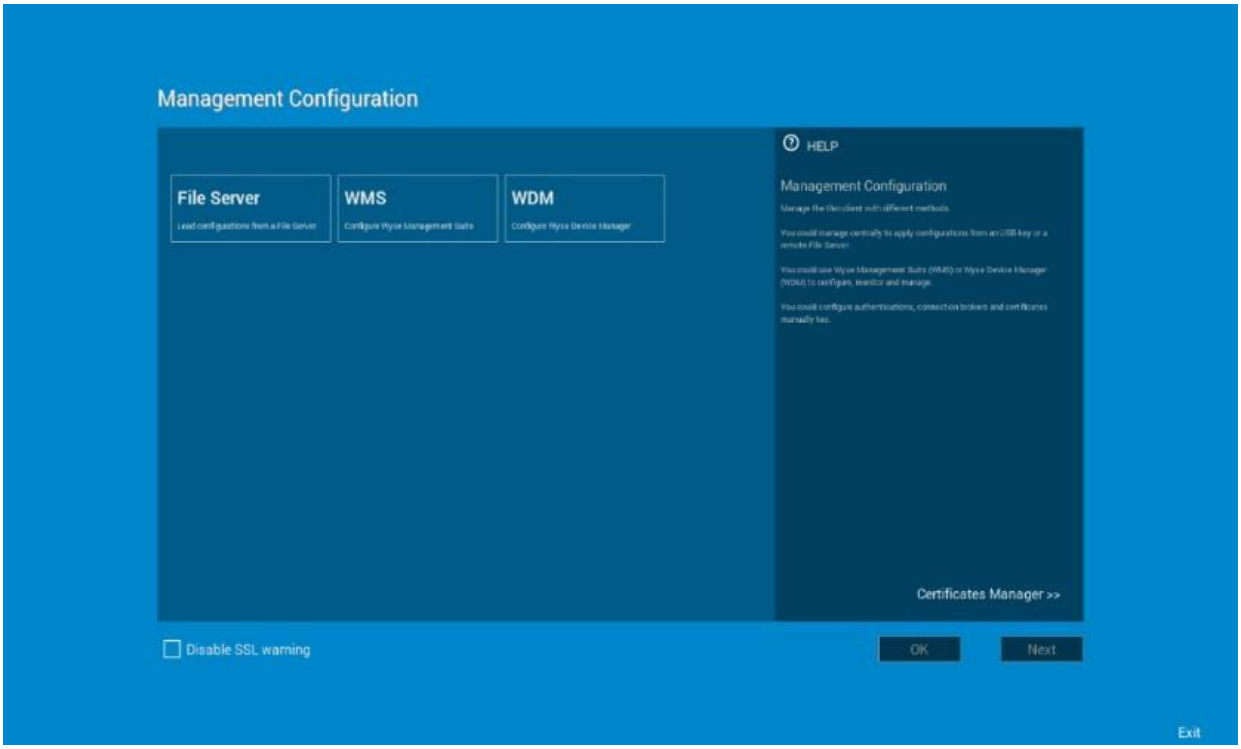
- **または無線接続を設定してください** をクリックします。一覧からワイヤレスネットワークを選択して、接続をクリックします。

メモ：
- ワイヤレス接続を設定するオプションは、WLAN モジュールを搭載していないシンクライアントでは利用できません。
- **Ethernet ケーブルを接続してください** 画面を終了して ThinOS システムデスクトップをロードするには、**終了**をクリックします。

接続が確立されると、シンクライアントは DHCP から払い出された IP アドレスを検証します。DHCP にファイルサーバがあるか、Wyse Device Manager または Wyse Management Suite の設定がある場合、ThinOS システムデスクトップがロードされます。DHCP の検証でエラーになるか、ネットワーク接続に失敗すると、**管理の構成** 画面が表示されます。手順 6〜9 に従います。

5 **次へ**をクリックし、**管理の構成**設定を開きます。

6 **管理の構成**画面で次の項目を設定します。

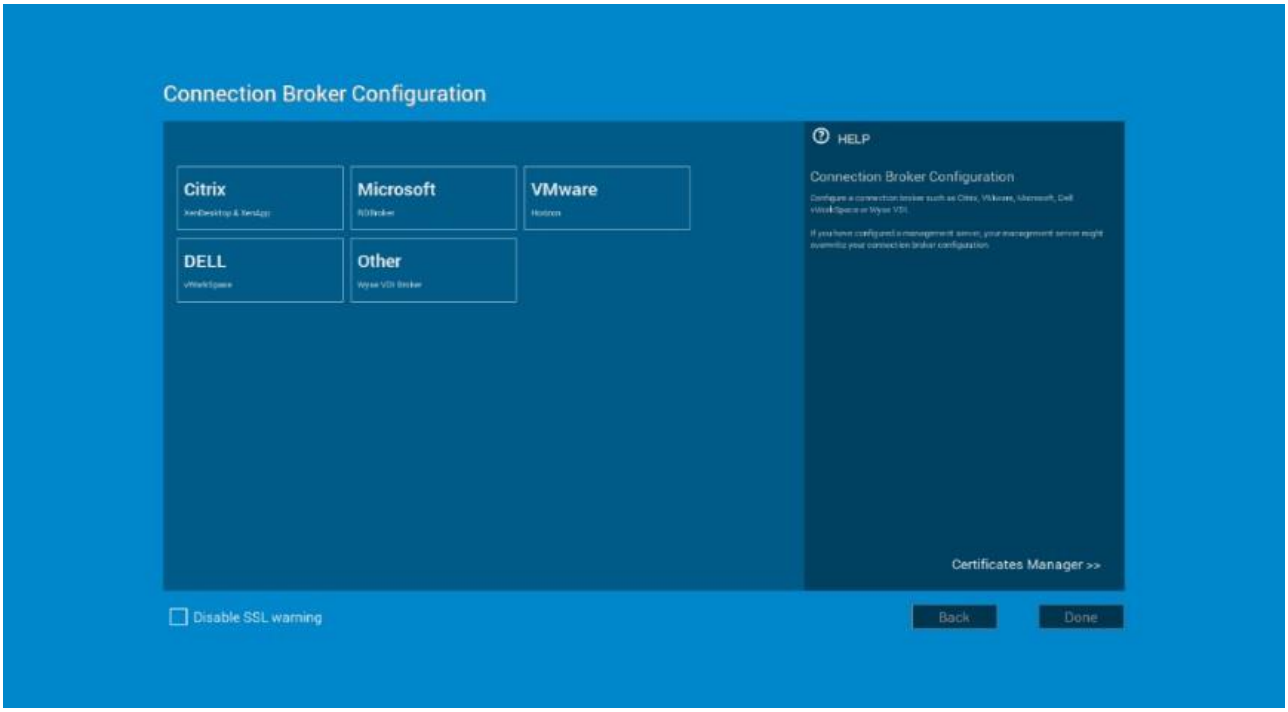


- ファイルサーバー——ファイルサーバの詳細情報を入力し、INI ファイル、ファームウェア、パッケージなど、ファイルサーバの設定を適用します。
- **WMS**——グループ登録キーと Wyse Management Suite サーバの URL を入力し、シンクライアントを Wyse Management Suite に登録します。
- **WDM**——IP アドレスまたはホスト名を入力します。
- **SSL 無効化の警告**——このチェックボックスをオンにすると、SSL（Secure Sockets Layer）接続に対する警告が無効になります。
- **証明書マネージャー**——**証明書マネージャー**をクリックし、証明書をインポートまたは要求します。

メモ：管理の構成画面を終了して ThinOS システムデスクトップをロードするには、終了をクリックします。

7 **完了**をクリックして First Boot ウィザードを終了するか、**次へ**をクリックして**接続ブローカーの構成を** 設定を入力します。

8 **接続ブローカーの構成** 画面で次の項目を設定します。



- **Citrix**——ブローカーによって、XenDesktop を使用してフルデスクトップに接続、または Citrix Receiver Client 経由で一元化されたホストから XenApp を使用して個々のアプリケーションに接続できます。
  - **サーバアドレス**——ブローカー接続のホスト名または IP アドレスを入力します。
  - **テーマの有効化:ThinOS Lite**——このチェックボックスをオンにすると、シンクライアンを ThinOS Lite モードで起動します。
  - **StoreFront スタイル**——このチェックボックスをオンにすると、シンクライアントで公開されたアプリケーションとデスクトップを、Citrix StoreFront ベースのレイアウトにすることが可能になります。
- **Microsoft**——ブローカーによって、RemoteApp と Desktop 接続を使用して仮想デスクトップに接続できます。ブローカー接続のホスト名または IP アドレスを入力します。
- **VMware**——ブローカーによって、VMware Horizon Client を使用してリモート デスクトップに接続できます。
  - **サーバアドレス**——ブローカー接続のホスト名または IP アドレスを入力します。
  - テーマの有効化:**VMware View**——このチェックボックスをオンにすると、ThinOS のデスクトップテーマが VMware View モードに設定されます。
- **DELL**——ブローカーによって、Dell vWorkspace を使用して仮想デスクトップまたはアプリケーションに接続できます。ブローカー接続のホスト名または IP アドレスを入力します。
- **Amazon WorkSpaces**——ブローカーによって、PCoIP クライアントが、AWS で稼働している仮想デスクトップに接続できます。ブローカー接続のホスト名／IP アドレス／FQDN を入力します。

メモ：Amazon WorkSpaces オプションは、PCoIP クライアントにのみ使用可能です。

- **その他**——ブローカーによって、その他のサポートしているプロトコルを使用して仮想デスクトップまたはアプリケーションに接続できます。ブローカー接続のホスト名または IP アドレスを入力します。
- **証明書マネージャー**——**証明書マネージャー**をクリックすると、証明書のインポートまたは要求を行います。
- **SSL 無効化の警告**——このチェックボックスをオンにすると、SSL（Secure Sockets Layer）接続に対する警告が無効になります。

9 **完了**をクリックします。

メモ：管理の構成 を再設定するには、戻るをクリックし、手順 6 と 7 に従います。

デバイスは First Boot ウィザードモードを終了し、ThinOS デスクトップが表示されます。

リモートサーバへの接続

一元設定への初回の接続では、ネットワークに接続された Ethernet ケーブルの**有線接続**プラグを使用してシンクライアントに接続してから、シンクライアントを起動して、管理者が指定した設定を取得することをお勧めします。この**有線接続**では、INI ファイルを介して管理者が提供するワイヤレス設定もすべて利用することができます。

初回にワイヤレスで一元設定に接続する必要がある場合は、**ネットワーク設定**ダイアログボックスの**無線**タブを使用して、ネットワーク管理者が要求するか、または設定した SSID と暗号化設定を入力します。詳細については、「ネットワーク設定の設定」を参照してください。

一元設定——INI ファイルを使用して自動検出を設定している場合は、「Dell Wyse ThinOS INI ガイド」を参照してください。シンクライアントは、起動プロセス中に、設定済みのリモートサービスを検出し、そのリモートサービスに自動で接続します。電源ボタンを押して、シンクライアントに電源を入れると **Login** ダイアログボックスが表示されます。ユーザー名、パスワード、およびドメインを入力し、**Login** をクリックします。認証に成功すると、使用可能な接続が表示されます。

メモ：

INI の下位互換性を確保するため、シンクライアントはデフォルトでクラシックデスクトップを使用します。ただし、INI ファイルの SysMode = VDI パラメータを使用するか、ダイアログボックスのデスクトップオプションを選択すると、ゼロデスクトップを表示するようシンクライアントを構成できます。詳細については、「デスクトップの使用」を参照してください。

手動接続——まだ一元設定を設定していない場合は、ゼロツールバーが表示されます。ゼロツールバーでは、**リモート接続設定**ダイアログボックスを使用して初回のサーバ接続を設定し、ログインできるようにすることができます。詳細については、「手動によるリモートサーバの接続」を参照してください。

この手動設定を完了する必要があるのは 1 回だけです。または、再起動して工場出荷時のデフォルトに戻した後だけです。シンクライアントによってサーバの場所が認識されると、今後シンクライアントを起動すると、自動的にサーバに接続してログインします。使用環境への導入の準備が整っていることを確認したら、一元設定用の INI ファイルを作成できます。

手動によるリモートサーバの接続

手動でリモートサーバに接続するには、次の手順を完了します。

1. ゼロツールバーで**システム設定**アイコンをクリックし、システム設定メニューを開き、リモート接続設定をクリックして、**リモート接続設定**ダイアログボックスを開きます。
2. **リモート接続設定**ダイアログボックスの**ブローカー**タブをクリックし、次のいずれかの接続を設定します。
   - ICA 接続または RDP 接続——**なし**を選択し、**ICA** または **RDP** を選択します。**接続設定の編集**をクリックし、ウィザードに従います。
   - 特定のブローカーサーバ接続——Microsoft、Citrix Xen、Dell vWorkspace、VMware View、Amazon WorkSpaces または Other を選択し、**ブローカーサーバ**ボックスにサーバの IP アドレスを入力します。

   メモ：詳細については、「リモート接続の設定」を参照してください。
3. **OK** をクリックし、シンクライアントをリスタートします。
   ゼロツールバーで**シャットダウン**アイコンをクリックして開き、**シャットダウン**ダイアログボックスを使用してシンクライアントをリスタートします。

   メモ：
   - ICA 接続または RDP 接続を設定している場合——シンクライアントのリスタート後、ゼロツールバーで**ホーム**アイコンをクリックし、使用可能な接続のリストを開きます。作成した ICA 接続または RDP 接続をクリックし、ログインします。
   - 特定のブローカーサーバ接続が設定されている場合——シンクライアントがリスタートすると、サーバの **Login** ダイアログボックスが表示されます。ユーザー名、パスワード、およびドメインを入力し、**Login** をクリックします。 認証に成功すると、ゼロツールバーが表示され、ブローカーサーバによって定義された割り当て済みの接続が示されます。

デスクトップの使用

サーバへのログイン後に表示される内容は、管理者が設定した内容によって異なります。

- **クラシックデスクトップを使用するユーザー** - ユーザーが使い慣れているフルタスクバー、デスクトップ、および ThinOS 接続マネージャを備えたクラシック ThinOS デスクトップが表示されます。このオプションは、直ちに使用できるデフォルト設定となっており、公開済みアプリケーションがあるターミナルサーバ環境に対して、および ThinOS 6.x バージョンとの下位互換性を確保する場合にお勧めします。クラシックデスクトップの使用方法の詳細については、「クラシックデスクトップの機能」を参照してください。

- **ゼロデスクトップを使用するユーザー** - ゼロツールバーを備えたゼロデスクトップが表示され、割り当て済みの接続のリストが示され、そのリストから選択できます。このオプションは、VDI およびフルスクリーンのみの接続に対してお勧めします。ゼロデスクトップの使用方法の詳細については、「ゼロデスクトップの機能」を参照してください。

どのデスクトップの場合でも、希望するデスクトップオプション（クラシックデスクトップまたはゼロデスクトップ）を選択し、**リモート接続設定**ダイアログボックスの**表示設定**タブを使用して必要な接続を作成できます。**リモート接続設定**ダイアログボックスを開くには、次のいずれかの手順を実行します。

- **クラシックデスクトップ**——ユーザー名をクリックし、**システム設定** → **リモート接続設定**を選択します。

  メモ：ユーザーは、ログインしているユーザーのことで、タスクバーの左下ペインに表示されています。
- **ゼロデスクトップ**——ゼロツールバーで**システム設定**アイコンをクリックし、リモート接続設定を選択します。

シンクライアント設定および接続設定の設定

INI ファイルを使用して、ユーザー向けにシンクライアント設定および接続設定を設定することを推奨しています。「自動アップデートおよび自動設定の設定方法」を参照してください。また、シンクライアントでダイアログボックスを使用して、次のことができます。

- シンクライアントハードウェア、外観と操作性、およびシステム設定を設定できます。「ローカルでのシンクライアント設定の設定」を参照してください。
- 接続設定を設定できます。「ローカルでのシンクライアント設定の設定」を参照してください。

プリンタとの接続

ローカルプリンタをシンクライアントに接続するには、適切なアダプタケーブルを入手して、使用してください。アダプタケーブルは同梱されていません。場合によっては、使用前に、次に示すプリンタドライバのインストール手順に従って、プリンタ用のプリンタドライバをインストールする必要があります。プリンタとの接続方法については、「プリンタセットアップの設定」を参照してください。

モニタとの接続

シンクライアントモデルによっては、モニタとの接続に、VGA（アナログ）モニタポート、DVI（デジタル）モニタポート、または DisplayPort（デジタル）のいずれかと、デルの適切なモニタケーブル／スプリッタ／アダプタを使用できます。デュアルディスプレイ設定の設定については、「ディスプレイ設定の設定」を参照してください。

メモ：
デュアルモニタをサポートするシンクライアントの場合——DVI - DVI／VGA スプリッタを使用する場合は、必ず DVI モニタをプライマリモニタにします。DisplayPort を使用する場合は、必ず DisplayPort モニタをプライマリモニタにします。

シンクライアントのロック

許可なく自分の個人情報に他の人がアクセスできないようするために、ThinOS では、以下のいずれかを行った後に、シンクライアントをロックし、資格情報がなければそのシンクライアントをアンロックして使用できないようにすることができます。

- **サインオンしたスマートカードを取り外す**——管理者が INI ファイルのサインイン／サインアウト用のパラメータに SCRemovalBehavior=1 を設定している場合にユーザーがシンクライアントへのサインオンに使用したスマートカードを取り外すと、シンクライアントはロックされます。シンクライアントをアンロックして使用するには、同じスマートカードと正しい PIN を使用する必要があります。サインオンしたスマートカードを取り外すと、シンクライアントもログオフする可能性があります。この現象は、管理者が INI ファイルにその設定をしていると、発生することがあります。この場合は、通常どおりにサインオンしてシンクライアントを使用する必要があります。
- **ショートカットメニューとシャットダウンダイアログボックスで端末のロックを使用する**——クラシックデスクトップのデスクトップで右クリックし、**端末のロック**を選択するか、**シャットダウン**ダイアログボックスを使用します。「クラシックデスクトップの機能」を参照してください。ゼロデスクトップで、**シャットダウン**ダイアログボックスを使用します。「サインオフとシャットダウン」を参照してください。シンクライアントを使用するには、正しいパスワードを使用する必要があります。
- **スクリーンセーバを使用する**——管理者が ScreenSaver パラメータに LockTerminal=2 を設定していて、スクリーンセーバーが実行されると、シンクライアントがロックされます。シンクライアントをアンロックするには、**Unlock** ダイアログボックスに、ログインパスワードを入力します。ただし、**Unlock** ダイアログボックスを使用している間は、壁紙を表示できません。

サインオフとシャットダウン

シャットダウンダイアログボックスを使用して、目的の使用可能なオプションを選択します。

- **クラシックデスクトップ**——接続マネージャまたはデスクトップメニューで**シャットダウン**をクリックします。
- **ゼロデスクトップ**——ゼロツールバーで**シャットダウン**アイコンをクリックします。

メモ：リモート接続設定ダイアログボックスを使用すると、すべてのデスクトップセッションが終了した後の自動的な動作を設定することもできます。「一元設定：アップデートと設定の自動化」を参照してください。

使用開始にあたっての補足情報

このセクションでは、次に関する補足情報を示します。

- ゼロデスクトップの機能
- クラシックデスクトップの機能
- Login ダイアログボックスの機能
- システム情報へのアクセス

ゼロデスクトップの機能

このセクションでは、次に関する情報を示します。

- インタラクティブなゼロデスクトップのガイドライン
- ゼロツールバー
- 接続のリスト

インタラクティブなゼロデスクトップのガイドライン

ゼロデスクトップにはデフォルトの背景が表示され、画面左側にゼロツールバーが配置されます。
以下の表では、使用可能なゼロデスクトップのショートカットを示しています。

表 3.　ゼロデスクトップのショートカット

アクション	押すキー
ゼロツールバーを表示する	Ctrl + Alt + 上向き矢印
選択ボックスを開いて、デスクトップと現在アクティブな接続を切り替える	Ctrl + Alt + 下向き矢印
シンクライアントをロックする	Ctrl + Alt + 左向き矢印 または Ctrl + Alt + 右向き矢印
メニューコマンドへのキーボードショートカット	左の Alt + 下線付きの文字 または 右の Alt + 下線付きの文字
デスクトップ全体をクリップボードに取り込む	Print Screen
アクティブウィンドウをクリップボードに取り込む	Alt + PrintScreen

メモ：

- アプリケーションセッション間、およびセッションとデスクトップ間でコピーして貼り付けることができます。ただし、この機能はセッションサーバの設定に依存します。
- 2 つのボタンが付いた標準的なマウス以外にも、シンクライアントでは、Microsoft ホイールマウスを使用してスクロールできます。その他の類似のタイプのホイールマウスについては、動作は保証されていません。

左ボタンと右ボタンを切り替えるには、**周辺機器**ダイアログボックスを使用します。「周辺機器設定の設定」を参照してください。

ゼロツールバー

ゼロツールバーは、通常、ゼロデスクトップの左隅に表示されます。ただし、管理者の設定によって、このツールバーを削除または非表示にすることができます。ユーザーがマウスポインタをデスクトップ画面の左端に移動したときにのみ表示されます。
管理者はダイアログボックス（「リモート接続の設定」を参照）または wnos.ini ファイルの SysMode パラメータ（『Dell Wyse ThinOS INI ガイド』を参照）を使用してツールバーの設定を設定できます。

表 4.　ツールバーアイコン

アイコン	機能
ホーム	使用可能な接続のリストを開きます。「接続のリスト」を参照してください。
システム情報	シンクライアントのシステム情報を表示します。「システム情報へのアクセス」を参照してください。
システム設定	シンクライアントのシステム設定を設定したり、診断を実行したりするシステム設定メニューを開きます。「　接続方法の設定」、「ローカルでのシンクライアント設定の設定」、「一元設定：アップデートと設定の自動化」を参照してください。
シャットダウン	**シャットダウン**アイコンをクリックし、シンクライアントで使用可能な Shutdown オプションを使用します。「サインオフとシャットダウン」を参照してください。**シャットダウン**アイコンは、**管理者モード**ボタンを使用してシステム設定を設定する場合は、ツールバーに表示されません。

メモ：現在の日時は、管理者が表示するように設定している場合、ゼロツールバーに表示されます。シンクライアントは、クロックを簡易ネットワーク管理プロトコル（SNTP）サーバが提供する時刻と同期できます。

接続のリスト

ゼロツールバーで、**ホーム**アイコンをクリックすると、割り当て済みの接続のリストを開くことができます。場合によっては、デフォルトの接続のみがリストに表示されることもあります。
次のガイドラインに従います。ユーザーの権限レベルによっては、一部のオプションが使用できない場合があります。

表 5.　接続オプション

オプション	機能
接続の名前	使用する接続を開きます。 **メモ：すべての開いている接続には、リスト内で接続名の左側に青色のアイコンが表示されます。**
リセットアイコン	接続をリセットします。 **メモ：このアイコンは、接続が正常に機能していないとき、または接続を再起動する必要があるときに役立ちます。**
切断アイコン	接続を閉じます。

オプション	機能
	メモ：**開いていない接続の Close アイコンは、グレーアウトされます。**
編集アイコン	接続オプションを変更するには、**Connection Settings** ダイアログボックスを開きます。 メモ：**ユーザーの権限レベルによっては、編集オプションは使用できない場合があります。**
接続設定の追加	新しい接続を設定または追加できます。
接続設定全般	INI ファイルを使用しないでグローバル接続設定を提供する場合は、**接続設定全般**をクリックして**接続設定全般**ダイアログボックスを開いて使用し、リスト内のすべての接続に影響する設定を設定できます。

ゼロテーマの使用

ゼロテーマオプションを使用して、Citrix、VMware、Classic または VDI モードの、ThinOS の画面レイアウトや操作性をカスタマイズします。ゼロテーマを有効にするには、ゼロテーマ環境設定に基づいて INI パラメータをデプロイし、シンクライアントを再起動します。**表示設定が変更されました**メッセージが表示され、シンクライアントが選択されたゼロテーマをロードします。

ZeroTheme={Classic,VDI,Citrix,VMware}

SysMode={Classic,VDI,Citrix,VMware}

INI パラメータは wnos.ini ファイルと連携します。Wyse Management Suite を使用して設定を管理することもできます。

- **Citrix ゼロモード**—ThinOS を Citrix ゼロモードに設定すると、デバイスは xen.ini ファイルを検索し、Citrix ゼロモードをロードします。xen.ini ファイルが使用できない場合、設定中は wnos.ini ファイルが使用されます。Citrix ゼロモードから切り替える必要がある場合、設定中は wnos.ini ファイルを使用する必要があります。
- **VMware ゼロモード**——ThinOS を VMware ゼロモードに設定すると、デバイスは VMware ゼロモードをロードします。

  メモ：**VMware の壁紙は、VMware ゼロモードで使用されます。**

クラシックデスクトップの機能

このセクションでは、次に関する情報を示します。

- インタラクティブなクラシックデスクトップのガイドライン
- ショートカットメニューの使用
- デスクトップメニューの使用
- 接続マネージャの使用

インタラクティブなクラシックデスクトップのガイドライン

クラシックデスクトップには Dell Wyse のデフォルトの背景が表示され、画面最下部に水平タスクバーが配置されます。

次のガイドラインに従います。

- 使用可能なサーバ接続および公開済みアプリケーションを表すアイコンが、背景に表示されます。アイコンの上にマウスポインタを静止させると、接続に関する情報が表示されます。アイコンを右クリックすると、接続の追加情報を表示する**設定**ダイアログボックスが開きます。デスクトップに表示できるアイコンの数は、デスクトップの解像度と管理者の設定によって異なります。
- サーバ接続および公開済みのアプリケーションは、デスクトップアイコンをダブルクリックして開くことができます。または、TAB キーを使用して目的のデスクトップアイコンに移動し、**Enter** キーを押すと接続を開始できます。

- デスクトップで右クリックすると、ショートカットメニューが表示されます。「ショートカットメニューの使用」を参照してください。
- ユーザー名をクリックするか、デスクトップをクリックすると、デスクトップメニューが開きます。「デスクトップメニューの使用」を参照してください。

メモ：
- ユーザーは、ログインしているユーザーのことで、タスクバーの左下ペインに表示されています。
- 管理者が表示するよう設定している場合、ボリュームコントロールはタスクバーの右隅に表示され、現在の日時は、カーソルが時刻の上に置かれると表示されます。シンクライアントは、クロックを簡易ネットワーク管理プロトコル（SNTP）サーバが提供する時刻と同期できます。

ショートカットメニューの使用

ショートカットメニューを使用するには：

1 管理者としてログインします。

2 デスクトップで右クリックします。
ショートカットメニューが表示されます。

3 **ショートカット**メニューには、次のオプションが表示され、使用できます。

a **管理者モード**——管理者がシンクライアントでさまざまなローカルの設定を設定できます。

b **すべてのウィンドウを隠す**——デスクトップ全体を前景に表示します。

c **クリップボードへのコピー**——画面全体、現在のウィンドウまたはイベントログのイメージをクリップボードにコピーします。クリップボードの内容は、ICA セッションまたは RDP セッションに貼り付けることができます。トラブルシューティングの場合は、画面全体または現在のウィンドウをクリップボードにコピーし、**スクリーンショットのエクスポート**オプションを使用して、スクリーンショットをエクスポートできます。

d **クリップボードの消去**——クリップボードの内容を破棄し、メモリを解放します。

e **端末のロック**——ユーザーがパスワードを使用してシステムにサインオンした場合に、シンクライアントをロック状態にします。同じパスワードを使用する場合にのみ、シンクライアントをアンロックできます。

f **セッションのグループ化**——ICA セッション、RDP、PCoIP、Blast、ICA シームレスセッションを 4 つ以上開くことができます。セッションは、タスクバーにグループとして表示されます。

デスクトップメニューの使用

デスクトップメニューを使用するには

1 デスクトップをクリックするか、ユーザー名をクリックします。
ユーザー名は、ログインしているユーザーで、タスクバーの左下に表示されます。

デスクトップメニューが表示されます。

2 デスクトップメニューには、次のオプションが表示され、使用できます。

a **システム設定**——次のローカルのシステム設定ダイアログボックスにアクセスできます。

- **ネットワーク設定**——DHCP またはネットワーク設定の手動入力の選択、およびシンクライアントの動作に不可欠なサーバの場所の入力を行うことができます。このメニューの選択は、権限の弱いユーザーに対しては無効になっています。「ネットワーク設定の設定」を参照してください。
- **リモート接続設定**——Microsoft、Citrix Xen、Dell vWorkspace、VMware View、Amazon WorkSpaces およびその他のブローカーサーバ接続など、シンクライアントブローカー接続を設定できます。詳細については、「リモート接続の設定」を参照してください。
- **管理サーバ設定**——ファイルサーバおよびオプションの WDA サーバ設定など、シンクライアントの一元的な接続設定を設定できます。詳細については、「一元設定の設定」を参照してください。
- **WAN 設定**——シンクライアントの VPN マネージャを設定できます。詳細については、「VPN マネージャの設定」を参照してください。
- **システム設定**——個人の環境設定に関するシンクライアントパラメータをユーザーが選択できます。詳細については、「システム環境の設定」を参照してください。
- **ディスプレイ**——モニタの解像度とリフレッシュレートを設定できます。詳細については、「ディスプレイ設定の設定」を参照してください。
- **周辺機器**——オーディオ、キーボード、マウス、シリアル、カメラ、ブルートゥース、タッチスクリーンの設定など、周辺機器設定を選択できます。詳細については、「周辺機器設定の設定」を参照してください。

- **プリンタ**——シンクライアントに接続されたネットワークプリンタおよびローカルプリンタを設定できます。詳細については、「プリンタ設定の設定」を参照してください。

b **システム情報**——シンクライアントのシステム情報を提供します。「システム情報へのアクセス」を参照してください。

c **システムツール**—デバイス、証明書、パッケージ、グローバル INI、ユーザーINI、wdm または ccm.ini に関する情報を提供します。「システムツール」を参照してください。

d **システム診断**——クライアントの CPU、メモリ、ネットワーク情報を表示するパフォーマンスモニタのグラフ、追跡およびイベントログの設定、CMOS 管理の抽出と復元設定、および ThinOS のトラブルシューティングに有用なその他のオプションを表示します。詳細については、「トラブルシューティングのオプションの使用」および「システムツール」を参照してください。

e **アプリケーション**——ローカルで設定したすべてのアプリケーションのサブメニューを含み、PNLite または PNAgent のいずれかを使用してサインオンすると、公開済みアプリケーションが表示されます。

f **シャットダウン——サインオフ/端末のロック/シャットダウン/システムのシャットダウンと再起動**の各ダイアログボックスを開きます。「サインオフとシャットダウン」を参照してください。

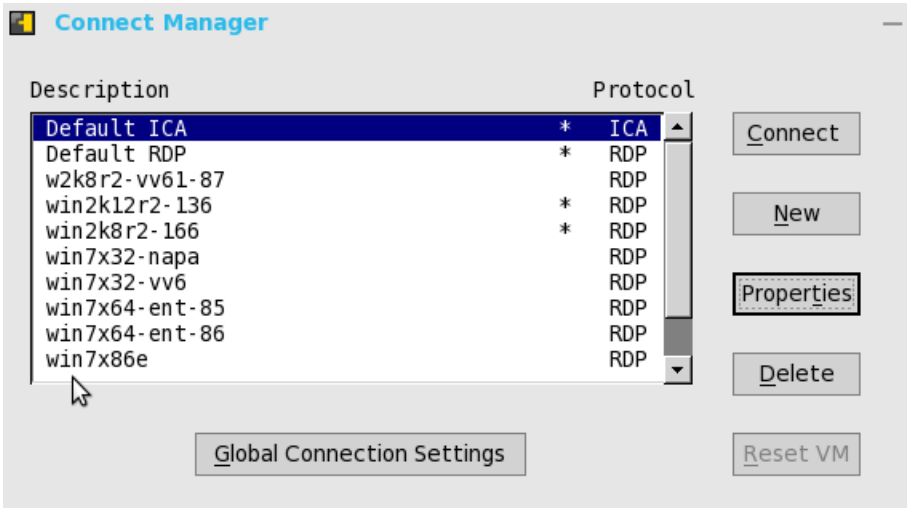
接続マネージャの使用

接続マネージャを使用するには

1 タスクバーで**接続マネージャ**をクリックします。

- 接続マネージャには、接続エントリーのリストと、接続で使用可能な一連のコマンドボタンが用意されています。
- 権限のないユーザーは接続マネージャを表示できません。

接続マネージャダイアログボックスが表示されます。



2 **接続マネージャ**ダイアログボックスで、次のボタンを使用して接続マネージャの設定を設定します。

a 接続をクリックし、リストから接続を選択して、接続を作成します。

b 直接、または Connection Protocol メニューの項目を選択してから**新規**をクリックして、**接続プロトコル**ダイアログボックスを開き、新しい接続の定義を作成します。
ローカルで定義した接続が、接続のリストに追加されます。次の情報に注意してください。

- **権限の強いユーザー**——通常、ローカルで定義した接続の定義は、すべて一時的なものであり、ユーザーがログオフしてシンクライアントがリスタートまたはシャットダウンされると失われます。ただし、このような場合でも、管理者によって設定されていれば（enablelocal = yes）、ローカルで定義された接続の定義は保存されます。
- **スタンドアロンユーザー**——シンクライアントがリスタートまたはシャットダウンし、ログオンしていない場合、ローカルで定義された接続は維持されます。ネットワーク構成設定はローカルで作成する必要があります。

c **設定**をクリックし、選択した接続の**接続**ダイアログボックスを開きます。
次の情報に注意してください。

- **権限の強いユーザー**——現在選択している定義を表示、編集できます。編集内容は、ユーザーがサインオフすると、永続的には保持されません。
- **権限の弱いユーザー**——接続を作成したり、編集したりすることはできませんが、接続の定義を表示できます。
- **スタンドアロンユーザー**——PNAgent／PNLite サービスが使用されている場合を除き、永続的な接続を変更し維持できます。

d **サインオフ**をクリックし、シンクライアントからクリックします。

e リストから接続を選択し、**削除**をクリックして、選択した接続を削除します。

f リストから仮想接続を選択し、**再起動**をクリックして、選択した接続をリセットします。

g **接続設定全般**タブをクリックして**接続設定全般**ダイアログボックスを開いて使用し、リスト内のすべての接続に影響する設定を設定します。

接続設定全般ダイアログボックスの詳細については、「3　　グローバル接続設定」を参照してください。

Login ダイアログボックスの機能

Login ダイアログボックスでは、サーバへのログインの他にも、次のことが行えます。

- システム情報の取得
- シンクライアント設定を設定するための管理者モードへのアクセス
- 自分自身のパスワードの変更またはリセット、および自分のアカウントのアンロック
- CTRL + ALT + DELETE を使用して、**シャットダウン**ダイアログボックスを開く

Login ダイアログボックスでは、次のガイドラインに従います。

- **システム情報**——システム情報ボタンをクリックし、**システム情報**ダイアログボックスを開きます。システムのバージョン、IP アドレス、シンクライアントに接続されているデバイスに関する情報、イベントログなどのシンクライアントのシステム情報を表示できます。詳細については、「システム情報へのアクセス」を参照してください。
- **管理者モード**——**管理者モード**ボタンをクリックし、ブローカーデスクトップ設定以外のさまざまなローカルの設定をシンクライアントで設定します。たとえば、リモート接続に関する説明に従って**リモート接続設定**ダイアログボックスを使用して、Citrix Xen ブローカーサーバの URL を手動で設定するか、またはファイルサーバによって一元的に定義された URL をオーバーライドするかを選択できます。
  - **クラシックデスクトップ**——**シャットダウン**ダイアログボックスの**管理者モードの終了**オプションを使用します。
  - **ゼロデスクトップ**——**シャットダウン**ダイアログボックスの**管理者モードの終了**オプションを使用するか、**システム設定**メニューの右上ペインにある管理者モードの終了アイコン（X）を使用します。

  メモ：デフォルトでは、管理者モードボタンは log on ダイアログボックスに表示されません。このボタンは、シャットダウンダイアログボックスの Show local admin button チェックボックスをオンにすると表示できます。「サインオフとシャットダウン」を参照してください。

  メモ：デフォルトでは、管理者モードボタンを使用するのにパスワードは必要ありません。wnos.ini ファイルの AdminMode パラメータを使用すると、管理者モードボタンをパスワードで保護できます（ログイン資格情報を求めることができます）。『Dell Wyse ThinOS INI ガイド』を参照してください。
- **シャットダウン**——**シャットダウン**ボタンをクリックして、**シャットダウン**ダイアログボックスを開いて使用し、サインオフ、シャットダウン、リスタート、システム設定の工場出荷時のデフォルトへのリセットなどを行います。これについては、「サインオフとシャットダウン」を参照してください。
- **アカウントセルフサービス**——PasswordServer INI パラメータの AccountSelfService オプションを使用して設定している場合に表示される**アカウントセルフサービス**アイコンをクリックし、**アカウントセルフサービス**ダイアログボックスを開いて使用し、自分自身のパスワードを変更またはリセットし、アカウントをアンロックします。INI パラメータについては、『Dell Wyse ThinOS INI ガイド』を参照してください。

この手順は、ユーザーが Windows 環境でセキュリティに関する質問と回答を事前に登録していることを前提としています。ユーザーは、**ブローカー**タブで、https://IPAddress のように、（HTTP ではなく）HTTPS をアカウントセルフサービスサーバのアドレスに使用する必要があります。詳細については、「リモート接続の設定」を参照してください。セキュリティに関する質問に回答した後、新しいパスワードが設定されて、アカウントがアンロックされます。

システム情報へのアクセス

システム情報ダイアログボックスを使用して、システム情報を表示します。

- **クラシックデスクトップ**——デスクトップメニューで**システム情報**をクリックします。
- **ゼロデスクトップ**——ゼロツールバーで**システム情報**アイコンをクリックします。

システム情報ダイアログボックスには、次が含まれます。

- **全般タブ**——システムのバージョン、シリアルナンバー、メモリサイズ（合計と空き）、CPU 速度、ROM サイズ、モニタ、パラレルポート、ターミナル名、起動元、メモリ速度、SSD サイズ、解像度、およびシリアルポートなどの一般的な情報を表示します。
- **著作権タブ**——ソフトウェアの著作権と特許に関する注意が表示されます。
  システム情報の**著作権**タブに **Acknowledgements** ボタンが追加されています。このボタンは、サードパーティのソフトウェアに関連しています。

- **イベントログタブ**——シンクライアントの起動ステップを表示します。通常は、システムのバージョンから始まり、ファームウェアのチェックまでを表示します。または問題のデバッグに役立つエラーメッセージを表示します。シンクライアントに接続されているモニタと USB の詳細、およびブルートゥースの初期設定も表示されます。
- **統計タブ**——TCP パフォーマンス関連パラメータ、UDP パフォーマンス関連パラメータ、CPU のビジー状態、システムの稼働時間、Wyse Management Suite ステータス、空きメモリ、アクティブなセッション、および WDM ステータスに関するステータス情報を表示します。
- **IPv6 タブ**——リンクローカルアドレス、IPv6 アドレス、および IPv6 デフォルトゲートウェイなどの IPv6 情報を表示します。

  メモ：このタブは、ネットワーク設定ダイアログボックスの全般タブで IPv6 が有効な場合に表示されます。「ネットワーク設定の設定」を参照してください。
- **有線タブ**——有線ネットワーク接続に関する情報を表示します。

  Wyse 5070 シンクライアントに、RJ-45 モジュールまたは SFP モジュールのいずれかが含まれている場合、Dual NIC 機能がサポートされます。**有線**タブで、**詳細**をクリックすると両方の Ethernet 接続のネットワーク情報が表示されます。
- **無線タブ**—ワイヤレスネットワーク接続に関する情報を表示します。
- **About タブ**——ThinOS オペレーティングシステムに関する情報を表示します。次の属性が一覧になっています。
  - プラットフォーム名
  - オペレーティングシステムのタイプ
  - ThinOS ビルド名
  - ThinOS ビルドバージョン
  - BIOS 名
  - BIOS バージョン
  - Citrix Broker または Receiver のバージョン——これは ThinOS バージョン間の ICA のリビジョンを表わします。
  - Dell vWorkspace のバージョン
  - VMware Horizon のバージョン——これは ThinOS バージョン間の Horizon のリビジョンを表わします。
  - Microsoft Broker または RDP のバージョン
  - Teradici PCoIP のバージョン——これは ThinOS バージョン間の PCoIP のリビジョンを表わし、PCoIP デバイスにのみ適用されます。
  - Imprivata のバージョン
  - Caradigm のバージョン
  - SECUREMATRIX のバージョン
  - HealthCast のバージョン

  メモ：
  - **Kernel モード**——コンポーネントは仕様に従って Kernel で実行されます。バージョンは、[max].[min]で表示され、これがプロトコルまたはサーバのベースバージョン、またはコンポーネントのクライアントです。たとえば、Microsoft RDP プロトコルのバージョンは 10.0 で、Imprivata のバージョンは 5.2、など。
  - **User モード**——コンポーネントはソースから、または ThinOS にコンパイルされたか組み込まれたサードパーティのバイナリから構成されます。バージョンは、[max].[min].[svn_revision]で表示されます。[max]と[min]はサードパーティのコンポーネントのベースバージョンで、[svn_revision]は ThinOS のソース管理リビジョンです。バージョン指定の ThinOS を使用すると、リビジョンの違いによる変更点を特定できます。たとえば、Citrix Receiver バージョンが 14.0.44705 で、VMware Horizon のバージョンが 4.6.45422、など。コンポーネントはインストールされたパッケージに適合しています。パッケージが削除されると、**About** タブのフィールドは空欄になります。

Energy Star 適合

Energy Star は、米国の環境保護庁（Environmental Protection Agency：EPA）が制定するエネルギー効率要件に適合するデバイスの標準ラベルです。Wyse 5070 シンクライアント（ThinOS 搭載）は、Energy Star 適合です。Energy Star プログラムの詳細については、www.energystar.gov を参照してください。サポート対象の ThinOS ビルドバージョンの詳細については、www.dell.com/support の『Dell Wyse ThinOS 8.5_113 Release Notes』を参照してください。

IPv6 対応

すべてのネットワークは Internet Protocol バージョン 6（IPv6）に対応している必要があります。Wyse 5070 シンクライアント（ThinOS 搭載）は、IPv6 対応です。サポート対象の ThinOS ビルドバージョンの詳細については、www.dell.com/ support の『Dell Wyse ThinOS 8.5_113 Release Notes』を参照してください。

グローバル接続設定

INI ファイルを使用しないで一元設定（グローバル接続設定）をユーザーに提供する場合は、**接続設定全般**ダイアログボックスを使用して、次のようにリスト内のすべての接続に影響する設定を設定できます。

- ゼロデスクトップ——接続のリストで**接続設定全般**をクリックします。
- クラシックデスクトップ——接続マネージャで**接続設定全般**をクリックします。

グローバル接続設定を設定するには：

1 デスクトップタスクバーで、**接続マネージャ** → **接続設定全般**をクリックします。
接続設定全般ダイアログボックスが表示されます。

2 **全セッション共通**タブをクリックし、すべてのセッションで使用可能にするオプションのチェックボックスをオンにします。
スマートカードチェックボックスで、起動時にスマートカードリーダーに接続するときのデフォルト設定を指定します。

> **メモ：**
> ICA セッションでは、接続されているスマートカードリーダーへの自動接続をいつでも使用できます。**ディスク**チェックボックスを使用して、接続されている USB スティックと自動接続する場合は、以下のガイドラインに従います。
>
> - 同時に 2 つ以上のディスクを使用できますが、異なるサブエリアを含め、USB スティックの最大数は 12 です。
> - すべてのデータを保存し、USB スティックをマップしているセッションからサインオフした後に USB スティックを取り外します。

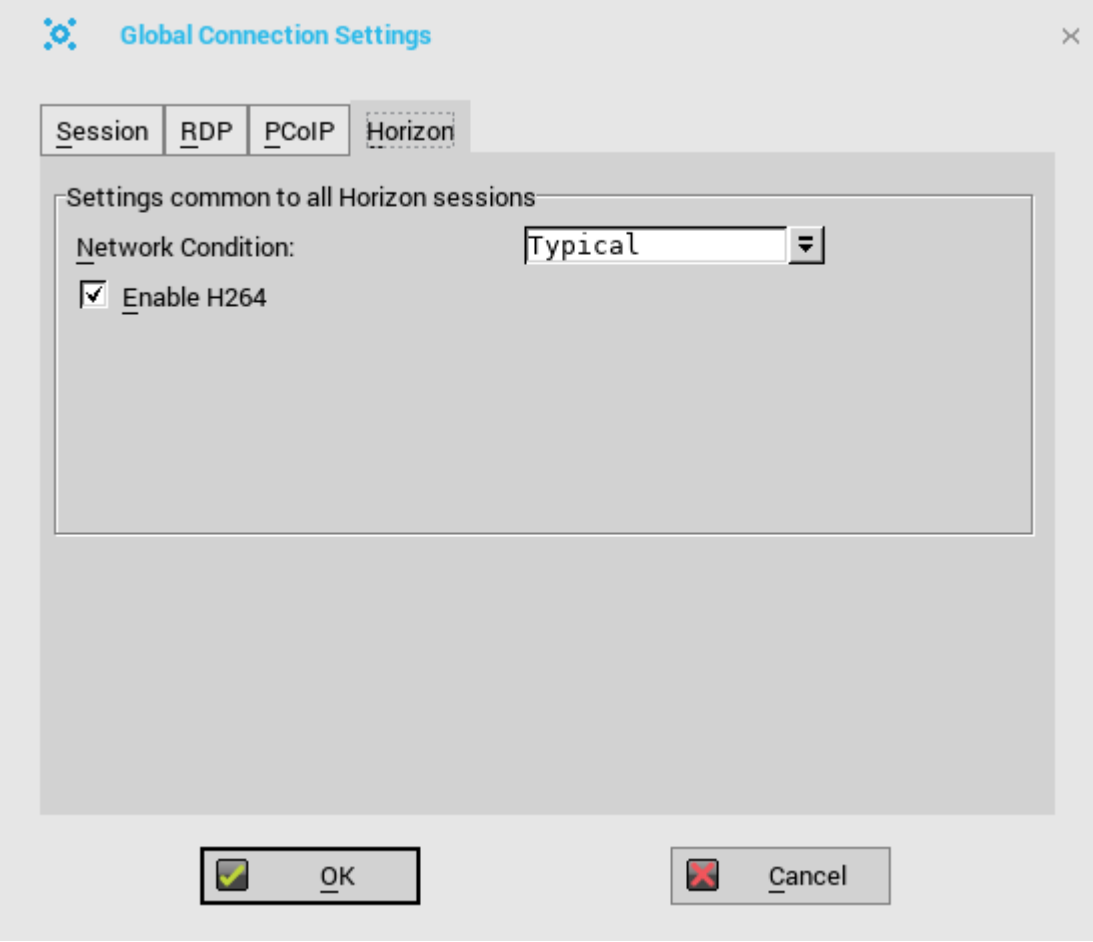
> **メモ：USB デバイスリダイレクション——デフォルトでは、オーディオ、ビデオおよびプリンタデバイスでは、リダイレクトに HDX USB を使用しません。接続設定全般ダイアログボックスの全セッション共通タブで、USB デバイスのリダイレクトを選択できます。**

3 **ICA** タブをクリックし、次の操作を行います。
   a すべての ICA セッションで使用可能にするオプションのチェックボックスをオンにします。
   b 接続に最適化したオーディオ品質を選択します。
   c **マップ**オプションを使用してディスクのマッピングをします。ドライブが入力されると、その特定のドライブの下でディスクがマッピングされます。

4 **RDP** タブをクリックし、次の操作を行います。
   a ネットワークレベル認証（NLA）の有効化または無効化——NLA 認証方式では、ユーザーを確認してから、ユーザーに完全なリモートデスクトップ接続を使用した接続を許可します。
   b スパンモードの有効化または無効化——このオプションによって、セッションを接続済みのモニタすべてに広げることができます。広がったモニタすべてが、1 個の巨大なモニタとみなされます。このセッションにはフルスクリーンモードで接続する必要があります。
   c RDP マルチメディアリダイレクト（MMR）の有効化または無効化。
   d ローカルからの録音の有効化または無効化（ローカルのマイクからの録音）。
   e RemoteFX の有効化または無効化。
   f USB リダイレクトタイプ（TCX USB または RDP USB）の選択——TCX USB がデフォルトです。RDP USB を使用するには、Windows 7／Windows 2008 R2 セッション用の RemoteFX セッションを使用する必要があります。ただし、標準の Windows 7／Windows 2008 R2 セッションの使用時に RDP USB はサポートされません。Windows 8 セッション以降は、RDP USB がサポートされています。

5 PCoIP が使用可能なクライアントでは、**PCoIP** という追加のタブが使用可能です。ドロップダウンリストから **USB リダイレクション**タイプを選択します。利用可能なタイプは **PCoIP USB** および **TCX USB** です。

6 **Horizon** タブをクリックし、次の操作を行います。



a **H264 の有効化**チェックボックスをオンにします。このオプションによって、Horizon Client で H.264 デコードが可能となります。

H.264 デコードを検証するには、次の操作を行います。

- INI パラメータに「BlastDebugClientH264=yes」を設定します。
- VMware Blast セッションを開始します。
- 画面の左上隅に、H264 の標準電子透かしが表示されているかどうか検証します。

ⓘ **メモ：Performance Tracker は、性能評価とデータ収集をするために、VMware が導入したものです。**

b **ネットワークの状態**ドロップダウンリストから、Blast 接続に用いるネットワーク状況を選択します。

ⓘ **メモ：Blast Extreme プロトコルは、BEAT（Blast Extreme Advanced Transport）の一部です。**

- **大変良い**を選択して、Blast 接続が Transmission Control Protocol（TCP）を使用できるようにします。
- **普通**を選択して、Blast 接続が Transmission Control Protocol（TCP）を使用できるようにします。デフォルトでは、これが選択されています。
- **弱い**を選択して Blast 接続が User Datagram Protocol（UDP）を使用できるようにします。UDP はエンドユーザーエクスペリエンスを実現するために、利用可能な帯域幅を使用します。

  UDP を有効にするには、VMware View Connection Server、Agent host desktop、VMware Horizon Client にいくつかの変更を加える必要があります。Server と Agent host desktop に必要な設定の詳細については、code.vmware.com/group/euc/thin-client/certs/4.6 の VMware の認定資格に関するガイドの記事を参照してください。

接続方法の設定

この章は、安全な接続に対するさまざまな構成設定を理解するのに役立ちます。Connectivity メニューでは、次の操作を行うことができます。

- ネットワーク設定の設定
- リモート接続の設定
- 一元設定の設定
- VPN マネージャの設定

メモ：クラシックデスクトップ設定を設定するには、デスクトップメニューでシステム設定をクリックし、設定用のタブを使用します。ゼロデスクトップ設定を設定するには、ゼロツールバーで**システム設定**アイコンをクリックし、設定用のタブを使用します。

ネットワーク設定の設定

ネットワーク設定を設定するには、次のオプションを使用します。

- 一般設定の設定
- オプション設定の設定
- 有線設定の設定
- WLAN 設定の設定
- プロキシ設定の設定

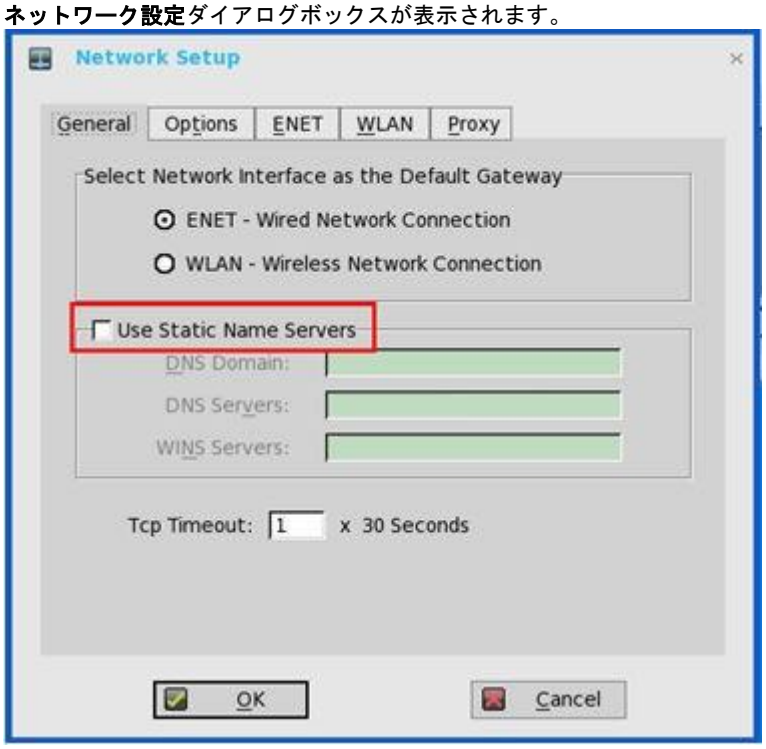
一般設定の設定

メモ：Wyse 5070 シンクライアントに Wireless LAN（WLAN）モジュールが含まれている場合は、このセクションが適用されます。Wyse 5070 シンクライアントが、オプションモジュール（Registered Jack 45（RJ45）または Small form-factor pluggable（SFP）モジュール）を含んでいる場合、「一般設定の設定」を参照してください。

一般ネットワーク設定を設定するには

1 デスクトップメニューで、**システム設定**をクリックし、**ネットワーク設定**をクリックします。

ネットワーク設定ダイアログボックスが表示されます。



2 **全般**タブをクリックし、次のガイドラインに従います。

a デフォルトゲートウェイを設定するには、使用可能なオプションからネットワークインターフェイスのタイプを選択します。

1 **シングルネットワークのサポート**——ワイヤレスネットワークまたは有線ネットワークのいずれかに接続します。

- **ENET**——Ethernet 有線ネットワーク接続を設定する場合に、このオプションをクリックします。
- **WLAN**——ワイヤレスネットワーク接続を設定する場合に、このオプションをクリックします
- ユーザーが ENET 接続の選択後にワイヤレスネットワークを使用する場合、または WLAN 接続の選択後に有線接続ネットワーク使用する場合は、最初の場合についてはシステムログ「WLAN:set default gate way xx.xx.xx.xx」が、2 番目の場合は「ENET:set default gate way xx.xx.xx.xx」が記録され、UI 設定に実際の使用状況が反映されます。

メモ：ユーザーインターフェイス（UI）は、自動では変更されません。

2 **デュアルネットワークのサポート**——ワイヤレスネットワークと有線ネットワークの両方に接続します。デフォルトゲートウェイは、UI 設定によって決定されます。

b **固定のネームサーバの使用**——デフォルトではこのチェックボックスはオフで、シンクライアントは DHCP からサーバの IP アドレスを取得します。このチェックボックスをオンにすると、手動で静的 IP アドレスを割り当てます。

GUI、INI またはリンクダウン／アップによってネームサーバが変更された場合、イベントログに詳細が表示されます。

ダイナミックモードでは、ネットワークが稼働していない場合、DNS／WINS は有線と無線からマージされる可能性があります。

1 **DNS ドメイン**ボックスに DNS ドメインの URL アドレスを入力します。

2 **DNS サーバ**ボックスに DNS サーバの IP アドレスを入力します。
DNS の使用はオプションです。DNS によって、IP アドレスではなく、ホスト名を使用してリモートシステムを指定できます。接続用に（名前の代わりに）特定の IP アドレスを入力すると、そのアドレスを使用して接続を作成できます。使用可能な DNS サーバの DNS ドメイン名とネットワークアドレスを入力します。DNS ドメインへの入力によって、名前解決で使用するデフォルトのサフィックスが指定されます。これら 2 つのボックスの値は、DHCP サーバによって提供されます。DHCP サーバによってこれらの値が提供される場合は、ローカルで設定した値が置き換えられます。DHCP サーバによってこれらの値が提供されない場合は、ローカルで設定した値が使用されます。

メモ：セミコロン、カンマまたはスペースで区切って、最大 16 個の DNS サーバアドレスを入力できます。最初のアドレスはプライマリ DNS サーバで、その他はセカンダリ DNS サーバまたはバックアップ DNS サーバです。

3 WINS サーバボックスに WINS サーバの IP アドレスを入力します。

WINS の使用はオプションです。使用可能な WINS ネームサーバのネットワークアドレスを入力します。WINS によって、IP アドレスではなく、ホスト名を使用してリモートシステムを指定できます。接続用に（名前の代わりに）特定の IP アドレスを入力すると、そのアドレスを使用して接続を作成できます。DHCP を使用している場合は、これらのエントリーは DHCP を介して提供できます。DNS と WINS は、基本的には名前解決という同じ機能を提供します。DNS と WINS の両方が使用可能な場合、シンクライアントは最初に DNS を使用して名前の解決を試行してから、次に WINS を使用します。

セミコロン、カンマまたはスペースで区切って、2 つの WINS サーバアドレス（プライマリとセカンダリ）を入力できます。

c 30 秒の乗数を **TCP Timeout** ボックスに入力し、TCP 接続のタイムアウト値を入力します。この値は、**1** または **2** にする必要があります。つまり、接続タイムアウト値は 30 秒（1 x 30）から 60 秒（2 x 30）となります。サーバに接続するためのデータの受信が確認されず、接続がタイムアウトする場合、タイムアウト時間を設定しておくと、接続が確立されるまで送信したデータを再送信し、サーバへの接続を再試行します。

3 **OK** をクリックして設定を保存します。

一般設定の設定

メモ：Wyse 5070 シンクライアントに、オプションモジュール（Registered Jack 45（RJ45）または Small form-factor pluggable（SFP）モジュール）が含まれている場合は、このセクションが適用されます。Wyse 5070 シンクライアントが無線 LAN（WLAN）モジュールを含んでいる場合は、「一般設定の設定」を参照してください。

一般ネットワーク設定を設定するには

1 デスクトップメニューで、**システム設定**をクリックし、**ネットワーク設定**をクリックします。
ネットワーク設定ダイアログボックスが表示されます。

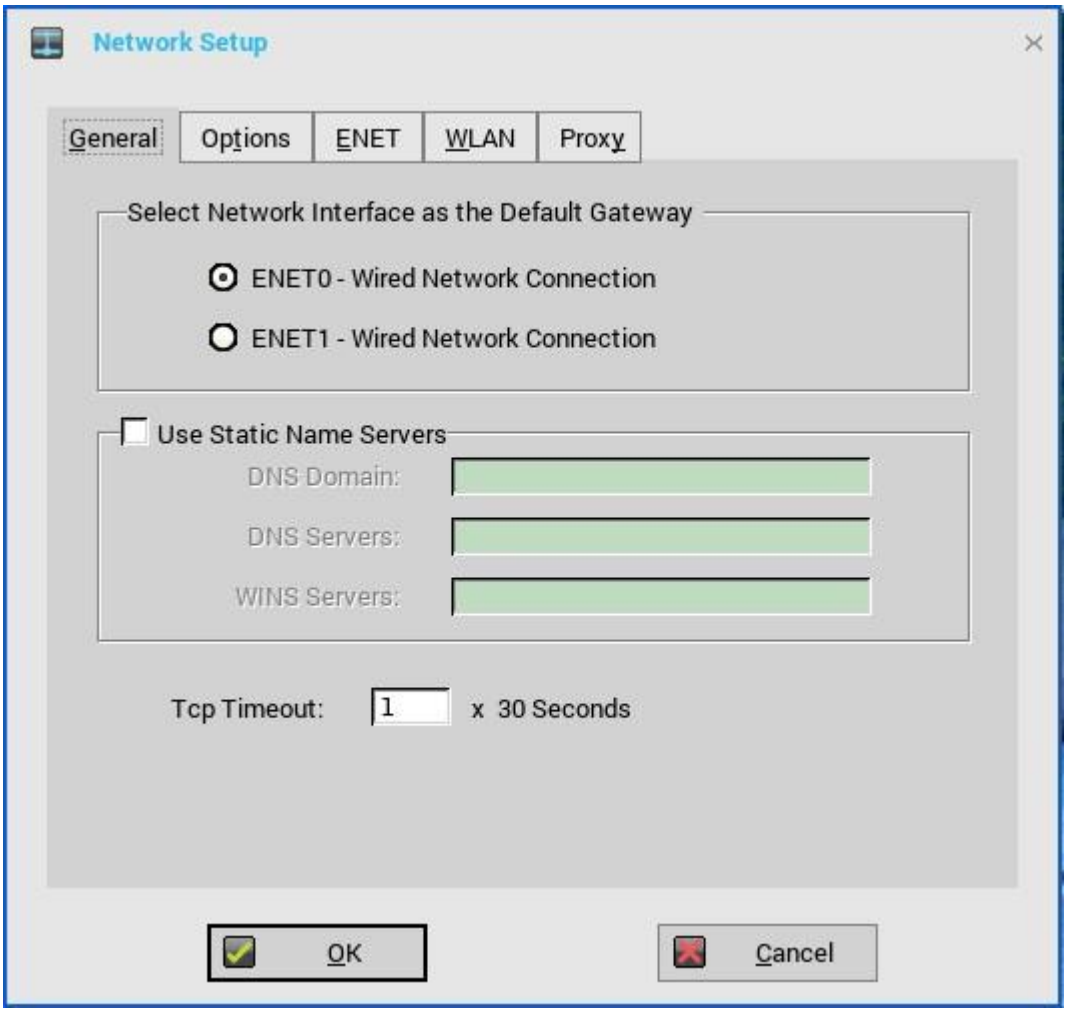


図 3. 一般設定

2 **全般**タブをクリックし、次のガイドラインに従います。

a デフォルトゲートウェイを設定するには、次のオプションからネットワークインターフェイスのタイプを選択します。

- **ENET0**——1 番目の Ethernet 有線ネットワーク接続をセットアップできるようにします。
- **ENET1**——2 番目の Ethernet 有線ネットワーク接続をセットアップできるようにします。

メモ：シンクライアントを 2 つの有線ネットワーク接続に同時に接続できます。デフォルトゲートウェイは、UI 設定によって決定されます。ただし、UI は自動では変更されません。

b **固定のネームサーバを使用**——デフォルトではこのチェックボックスはオフで、シンクライアントは DHCP からサーバの IP アドレスを取得します。このチェックボックスをオンにすると、手動で静的 IP アドレスを割り当てます。
GUI、INI またはリンクダウン／アップによってネームサーバが変更された場合、イベントログに詳細が表示されます。
ダイナミックモードでは、ネットワークが稼働していない場合、DNS／WINS は Ethernet 0 と Ethernet 1 からマージされる可能性があります。

1 **DNS ドメイン**ボックスに DNS ドメインの URL アドレスを入力します。
2 **DNS サーバ**ボックスに DNS サーバの IP アドレスを入力します。
DNS の使用はオプションです。DNS によって、IP アドレスではなく、ホスト名を使用してリモートシステムを指定できます。接続用に（名前の代わりに）特定の IP アドレスを入力すると、そのアドレスを使用して接続を作成できます。使用可能な DNS サーバの DNS ドメイン名とネットワークアドレスを入力します。DNS ドメインへの入力によって、名前解決で使用するデフォルトのサフィックスが指定されます。これら 2 つのボックスの値は、DHCP サーバによって提供されます。DHCP サーバによってこれらの値が提供される場合は、ローカルで設定した値が置き換えられます。DHCP サーバによってこれらの値が提供されない場合は、ローカルで設定した値が使用されます。

メモ：セミコロン、カンマまたはスペースで区切って、最大 16 個の DNS サーバアドレスを入力できます。最初のアドレスはプライマリ DNS サーバで、その他はセカンダリ DNS サーバまたはバックアップ DNS サーバです。

3 **WINS サーバ**ボックスに WINS サーバの IP アドレスを入力します。
WINS の使用はオプションです。使用可能な WINS ネームサーバのネットワークアドレスを入力します。WINS によって、IP アドレスではなく、ホスト名を使用してリモートシステムを指定できます。接続用に（名前の代わりに）特定の IP アドレスを入力すると、そのアドレスを使用して接続を作成できます。DHCP を使用している場合は、これらのエントリーは DHCP を介して提供できます。DNS と WINS は、基本的には名前解決という同じ機能を提供します。DNS と WINS の両方が使用可能な場合、シンクライアントは最初に DNS を使用して名前の解決を試行してから、次に WINS を使用します。

セミコロン、カンマまたはスペースで区切って、2 つの WINS サーバアドレス（プライマリとセカンダリ）を入力できます。

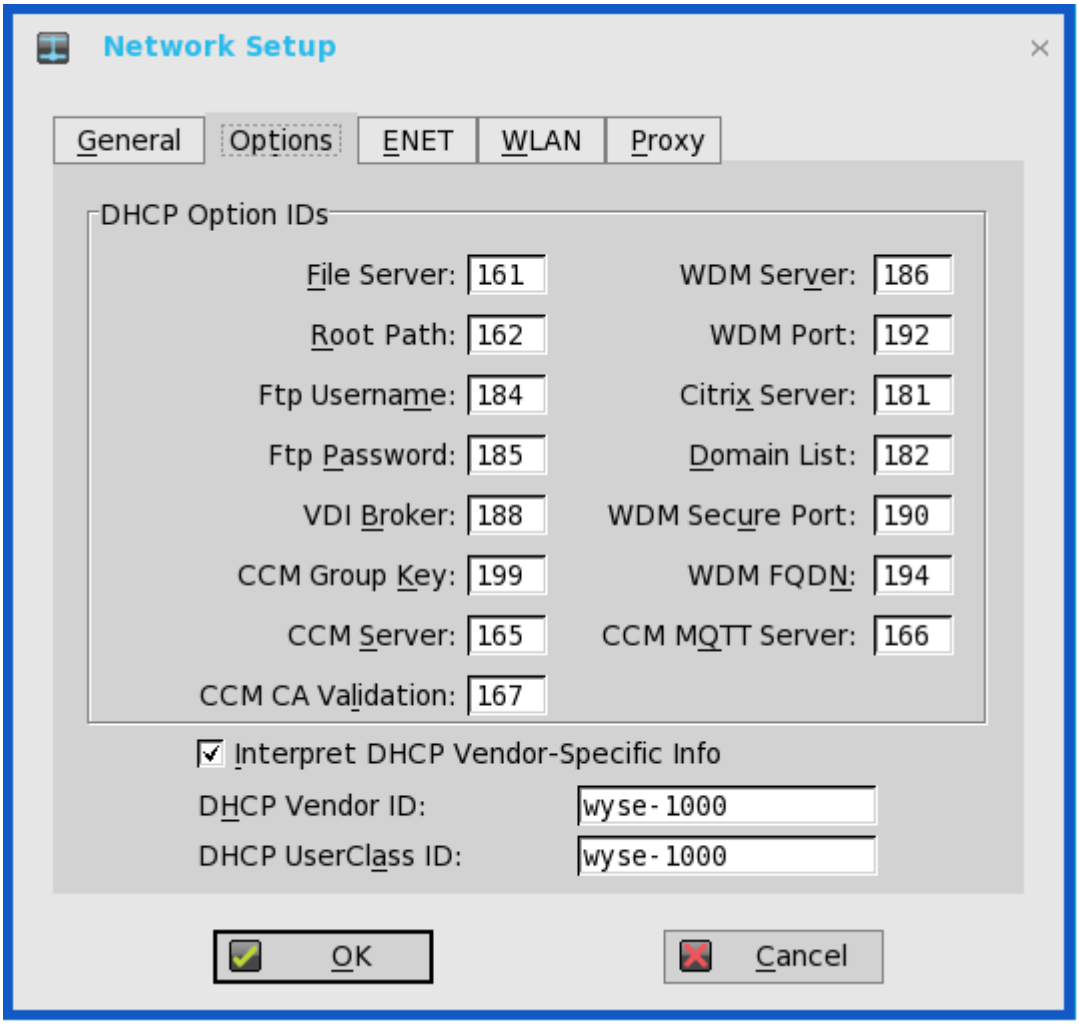
c 30 秒の乗数を **TCP Timeout** ボックスに入力し、TCP 接続のタイムアウト値を入力します。この値は、**1** または **2** にする必要があります。つまり、接続タイムアウト値は 30 秒（1 x 30）から 60 秒（2 x 30）となります。サーバに接続するためのデータの受信が確認されず、接続がタイムアウトする場合、タイムアウト時間を設定しておくと、接続が確立されるまで送信したデータを再送信し、サーバへの接続を再試行します。

3 **OK** をクリックして設定を保存します。

DHCP オプション設定の設定

DHCP オプション設定を設定するには

1 デスクトップメニューで、**システム設定**をクリックし、**ネットワーク設定**をクリックします。
ネットワーク設定ダイアログボックスが表示されます。
2 **オプション**タブをクリックし、次のガイドラインに従います。



a **DHCP オプション IDs**——サポートする DHCP オプションを入力します。それぞれの値は 1 回だけ使用可能で、**128～254** の間にする必要があります。DHCP オプションについては、DHCP オプションを参照してください。

b **DHCP ベンダ固有情報を解釈する**——ベンダー情報を自動で解釈するには、このチェックボックスをオンにします。

c **DHCP ベンダ ID**——Dynamically allocated over DHCP/BOOTP オプションが選択されている場合に、DHCP ベンダーID を表示します。

d **DHCP ユーザクラス ID**——Dynamically allocated over DHCP/BOOTP オプションが選択されている場合に、DHCP ユーザークラス ID を表示します。

3 **OK** をクリックして設定を保存します。

有線設定の設定

有線設定を設定するには

1 デスクトップメニューで、**システム設定**をクリックし、**ネットワーク設定**をクリックします。
ネットワーク設定ダイアログボックスが表示されます。

2 **有線**タブをクリックし、次のガイドラインに従います。

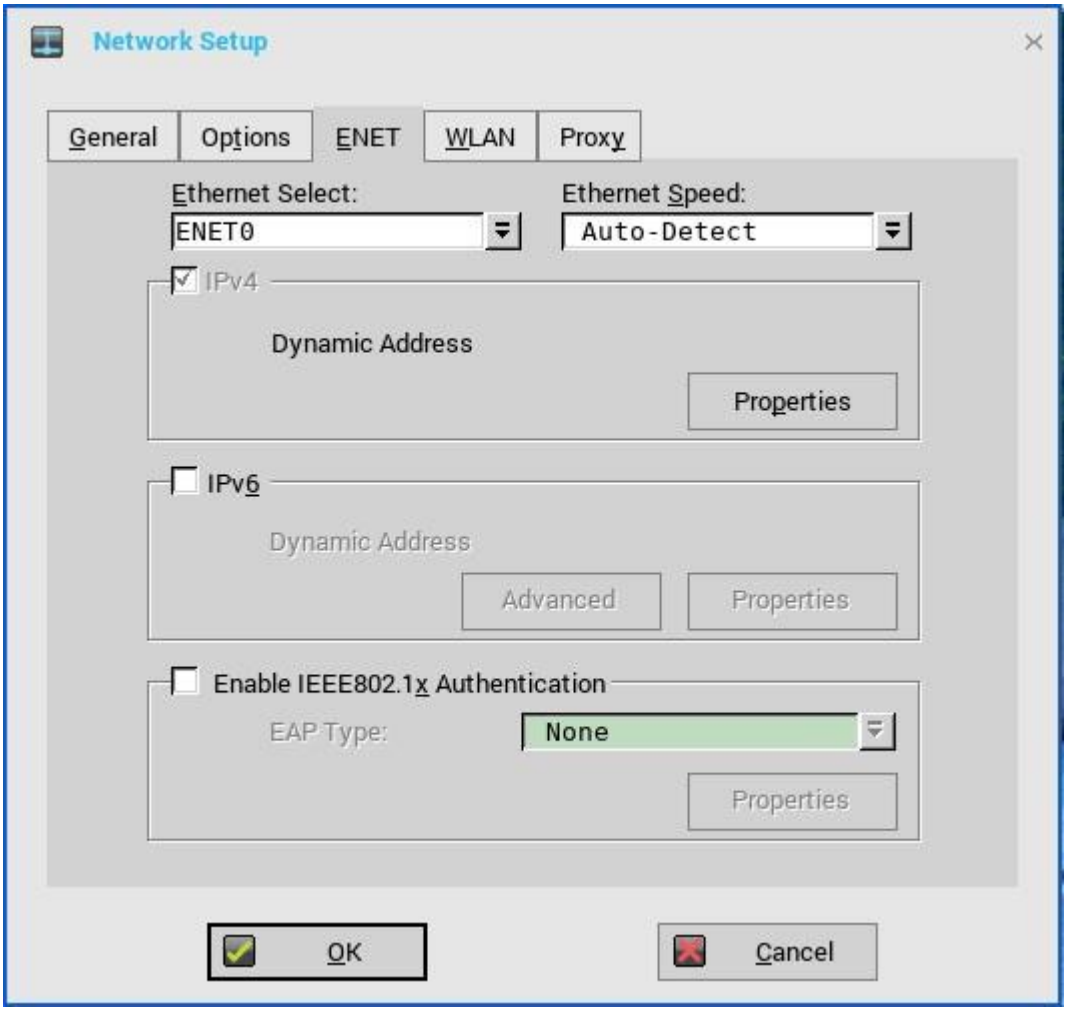


図 4.　ENET タブ

a　**Ethernet Select**——有線ネットワーク接続を選択できます。Wyse 5070 シンクライアント（SFP または RJ-45 モジュールなし）の場合、**ENET0** オプションがデフォルトで選択されています。Wyse 5070 シンクライアント（SFP または RJ-45 モジュール搭載）の場合、個々のネットワークの好みに基づいて **ENET0** または **ENET1** を選択します。

b　**イーサネット速度**——デフォルト値は**自動検出**です。ご利用ネットワーク機器がオートネゴシエーションに対応していない場合、利用可能なオプション（**10 MB 半二重**、**10 MB 全二重**、**100 MB 半二重**、**100 MB 全二重**、**1 GB 全二重**）から 1 つを選択します。

10 MB 全二重オプションはローカルで選択できます。ただし、このモードでは**自動検出**によるネゴシエートが可能です。

c　デフォルトでは **IPv4** チェックボックスが選択されます。**プロパティ**をクリックして次のオプションを設定します。

- **DHCP/BOOTP による自動取得**——このオプションを選択すると、シンクライアントが DHCP サーバから自動的に情報を受信できます。ネットワーク管理者は、DHCP オプションを使用して DHCP サーバを設定し、情報を提供する必要があります。**オプション**タブにローカルで入力された値は、DHCP の値に置き換えられます。DHCP サーバが置き換える値を提供できない場合は、ローカルで入力された値が使用されます。
- **静的 IP アドレスを指定**——このオプションを選択すると、IP アドレス、サブネットマスクおよびデフォルトゲートウェイを手動で入力できます。
  - **IP アドレス**——サーバ環境内の有効なネットワークアドレスを入力します。ネットワーク管理者は、この情報を入力する必要があります。
  - **ネットマスク**——サブネットマスクの値を入力します。サブネットマスクを使用すると、他のサブネット上のマシンにアクセスできます。

    サブネットマスクを使用すると、**同一サブネット**または**他のサブネット**という 2 つの選択肢によって、他の IP アドレスの場所を区別できます。IP アドレスの場所が他のサブネットである場合、そのアドレスに送信するメッセージは、デフォルトゲートウェイ経由で送信する必要があります。このことは、IP アドレスがローカル設定または DHCP のいずれによって指定されても同じです。ネットワーク管理者は、この値を入力する必要があります。
  - **ゲートウェイ**——ゲートウェイの使用はオプションです。ゲートウェイを使用すると、複数のネットワークを相互接

続できます（ネットワーク間でルーティング、つまり IP パケットを送信します）。デフォルトゲートウェイを使用すると、インターネットまたは複数のサブネットがあるイントラネットにアクセスできます。ゲートウェイが指定されていない場合、シンクライアントがアドレス指定できるのは同一サブネット上の他のシステムのみです。シンクライアントをインターネットに接続するルーターのアドレスを入力します。このアドレスは、IP アドレスとサブネットマスクで定義されているとおりに、シンクライアントと同じサブネットに存在する必要があります。DHCP を使用している場合は、アドレスは DHCP を介して提供できます。

d **IPv6** チェックボックスをオンにし、**詳細**をクリックして、使用可能なチェックボックスで、IPv6 をサポートするさまざまな設定オプションを選択します。
次のチェックボックスが、**IPv6 詳細設定**ダイアログボックスに表示されます。

- **IPv6 有効時、IPv4 無効化を可能にする**
- **両方有効時、IPv6 より IPv4 を優先する**
- **ステートレスアドレス自動設定（SLAAC）を無効にする**
- **重複アドレス検出（DAD）を無効にする**
- **ICMPv6 エコー応答を無効にする**
- **ICMPv6 リダイレクトサポートを無効にする**
- **標準 DHCPv6 タイマーを利用する**

プロパティをクリックして、以下のガイドラインに従います。

- **DHCP 待機**——このオプションを選択すると、ログイン前にシンクライアントが IPv6 DHCP を考慮に入れることを可能とします。このオプションを選択しなければ、DHCP が有効となり、システムは引き続き IPv4 DHCP を待ちます。
- **DHCP/BOOTP による自動取得**——このオプションを選択すると、シンクライアントが DHCP サーバから自動的に情報を受信できます。ネットワーク管理者は、（DHCP オプションを使用して）DHCP サーバを設定し、情報を提供する必要があります。**オプション**タブにローカルで入力された値は、DHCP の値に置き換えられます。DHCP サーバが置き換える値を提供できない場合は、ローカルで入力された値が使用されます。
- **静的 IP アドレスを指定**——このオプションを選択すると、IP アドレス、サブネットマスクおよびデフォルトゲートウェイを手動で入力できます。
  - **IP アドレス**——サーバ環境内の有効なネットワークアドレスを入力します。ネットワーク管理者は、この情報を入力する必要があります。
  - **Subnet Prefix 長**——IPv6 サブネットのプレフィックスの長さを入力します。
  - **ゲートウェイ**——ゲートウェイの使用はオプションです。詳細については、このセクションで、IPv4 がサポートするさまざまなオプションを参照してください。
- **DNS サーバ**——DNS の使用はオプションです。DNS によって、IP アドレスではなく、ホスト名を使用してリモートシステムを指定できます。接続用に（名前の代わりに）特定の IP アドレスを入力すると、DNS ではなく、そのアドレスを使用して接続を作成できます。使用可能な DNS サーバのネットワークアドレスを入力します。このボックスの値は、DHCP サーバによって提供されます。DHCP サーバによってこの値が提供される場合は、ローカルで設定した値が置き換えられます。DHCP サーバによってこの値が提供されない場合は、ローカルで設定した値が使用されます。

メモ：ENET0 と ENET1 の両方に IPv6 を有効にした場合は、最初に IPv6 アドレスを取得した Ethernet 接続を経由して IPv6 が送信されます。

e **IEEE802.1x 認証を有効にする**チェックボックスをオンにして、**EAP 選択**ドロップダウンリストから、**TLS、LEAP、PEAP、FAST** のいずれかを選択します。

- **TLS**——このオプションを選択し、**プロパティ**をクリックして、**認証設定**ダイアログボックスを設定します。
  - サーバ証明書の検証に必須であるため、**サーバ証明書を検証**チェックボックスをオンにします。

    メモ：シンクライアントに CA 証明書をインストールする必要があります。サーバ証明書のテキストフィールドは、最大約 255 文字で、複数のサーバ名がサポートされます。
  - **これらのサーバに接続**チェックボックスをオンにして、サーバの IP アドレスを入力します。
  - **参照**をクリックして、目的のクライアント証明書ファイルとプライベートキーファイルを探して選択します。

    メモ：必ず PFX 形式のファイルだけを選択します。
  - **認証**ドロップダウンリストから、ユーザーの選択に基づいてユーザー認証かマシン認証かを選択します。
    次の種類のサーバ名がサポートされています。例は、すべて company.dell.com という Cert Common name に基づいています。
    - *.dell.com
    - *dell.com
    - *.com

    メモ：FQDN のみ（つまり、company.dell.com）を使用しても機能しません。次のいずれかを使用します。たとえば servername.dell.com（複数の認証サーバが存在する可能性があるため、*.dell.com を使用するのが最も一般的です）。

- **LEAP**——このオプションを選択し、**プロパティ**をクリックして、**認証設定**ダイアログボックスを設定します。認証には、正しいユーザー名とパスワードを使用します。ユーザー名またはパスワードの最大長は 31 文字です。
- **PEAP**——このオプションを選択し、**プロパティ**をクリックして、**認証設定**ダイアログボックスを設定します。**EAP_GTC** または **EAP_MSCHAPv2** のいずれかを選択し、正しいユーザー名、パスワードおよびドメインを使用します。サーバ証明書を検証はオプションです。
- **FAST**——このオプションを選択し、**プロパティ**をクリックして、**認証設定**ダイアログボックスを設定します。**EAP_GTC** または **EAP_MSCHAPv2** のいずれかを選択し、正しいユーザー名、パスワードおよびドメインを使用します。サーバ証明書を検証はオプションです。

  EAP-GTC を構成するには、ユーザー名のみを入力します。認証時には、パスワードまたは PIN が必要です。EAP-MSCHAPv2 を設定するには、ユーザー名、パスワードおよびドメインを入力します。

  メモ：Username ボックスではドメイン／ユーザー名がサポートされますが、Domain ボックスは空白にする必要があります。

  CA 証明書をシンクライアントにインストールする必要があります。サーバ証明書は強制的に検証されます。PEAP または FAST 認証に EAP-MSCCHAPV2 を選択した場合、ドメインを非表示にするオプションを使用できます。ユーザ名およびパスワードボックスは使用できますが、ドメインテキストボックスは無効です。

  PEAP または FAST の認証に EAP-MSCHAPV2 を選択した場合、シングルサインオン機能を有効にするチェックボックスを使用できます。

  ThinOS 8.3 から、EAP-FAST 認証がサポートされています。初回の接続時に、認証システムから Tunnel PAC の要求がある場合は、認証を完了させるために PAC が使用されます。初回の接続は必ずエラーとなり、その後の接続で成功します。自動 PAC プロビジョニングのみサポートされています。CISCO EAP-FAST ユーティリティで生成されるユーザー／マシン PAC プロビジョニングはサポートされていません。

3 **OK** をクリックして設定を保存します。

重要:ThinOS バージョン 8.5 から、ネットワーク設定の変更にクライアントのリブートは必要ありません。すべての変更が即座に有効となります。

たとえば、ThinOS は再起動なしですぐに、新しいワイヤレス SSID に接続します。

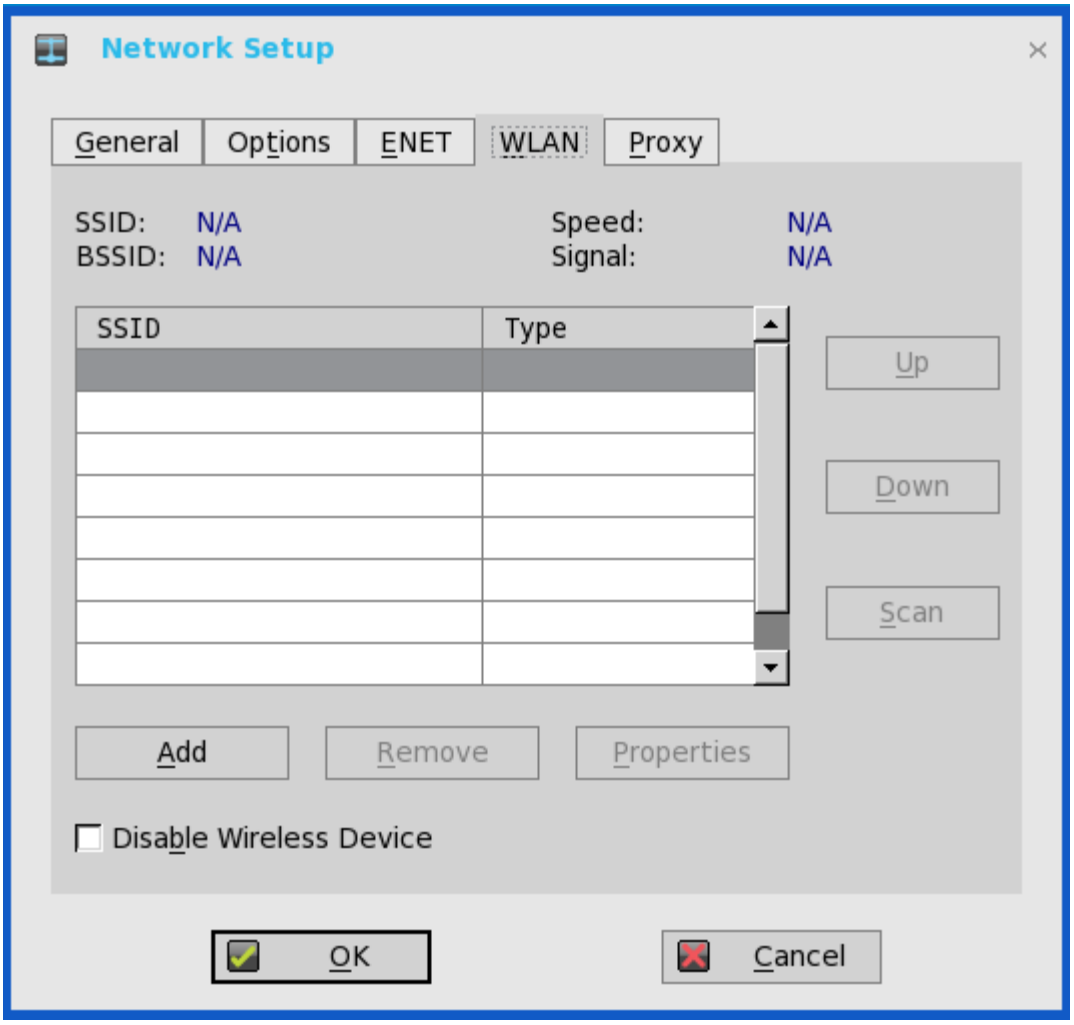
WLAN 設定の設定

メモ：Wyse 5070 シンクライアント（オプションの SFP モジュールまたは RJ45 モジュールを搭載）では、ワイヤレス設定を設定することはできません。

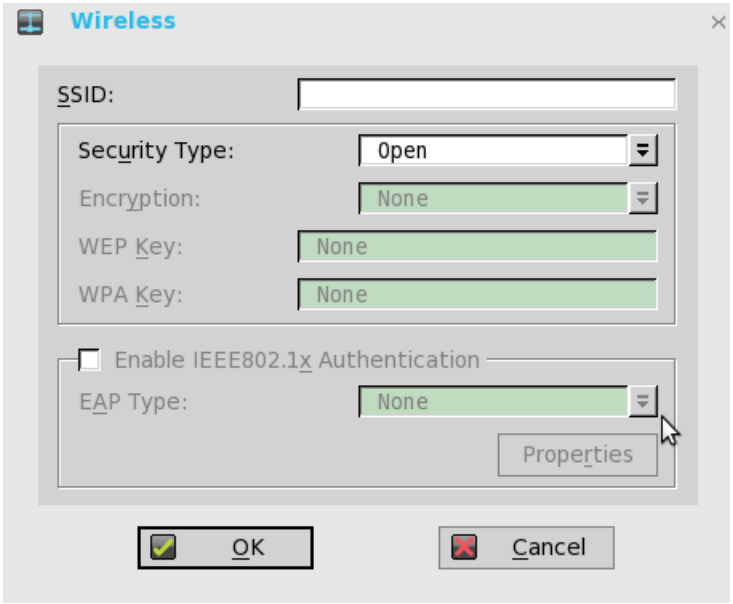
WLAN 設定を設定するには：

1 デスクトップメニューで、**システム設定**をクリックし、**ネットワーク設定**をクリックします。
ネットワーク設定ダイアログボックスが表示されます。

2 **無線**タブをクリックし、次の操作を行います。



a **追加**——このオプションを使用して、新しい SSID 接続を追加、設定します。
使用可能なセキュリティタイプのオプションから SSID 接続を設定できます。



SSID 接続を設定すると、追加した SSID 接続が**無線**タブのページに表示されます。

b **削除**——SSID 接続をリストで選択して削除する場合は、このオプションを使用します。

c **プロパティ**——このオプションを使用して、リストに表示されている SSID 接続の認証プロパティを表示、構成します。

d ワイヤレスデバイスを無効にする場合は、**Wi-Fi 無効化**チェックボックスをオンにします。

- **常に**——ワイヤレスデバイスを常に無効にする場合は、このラジオボタンをクリックします。
- **ENET 検出**——有線ネットワークが接続されているときに必ずワイヤレスデバイスを無効にする場合は、このラジオボタンをクリックします。

3 **OK** をクリックして設定を保存します。

重要:ネットワーク設定を変更するのにデバイスのリブートは必要ありません。すべての変更が即座に有効となります。
たとえば、ThinOS は再起動なしですぐに、新しいワイヤレス SSID に接続します。ただし ARM プラットフォーム、つまり Wyse 3010 シンクライアントと Wyse 3020 シンクライアントについては、再起動が必要となります。

メモ：

- サポート対象のチップセット：Intel Dual Band Wireless AC 9560
- サポート対象の規格：802.11 a/b/g/n/ac

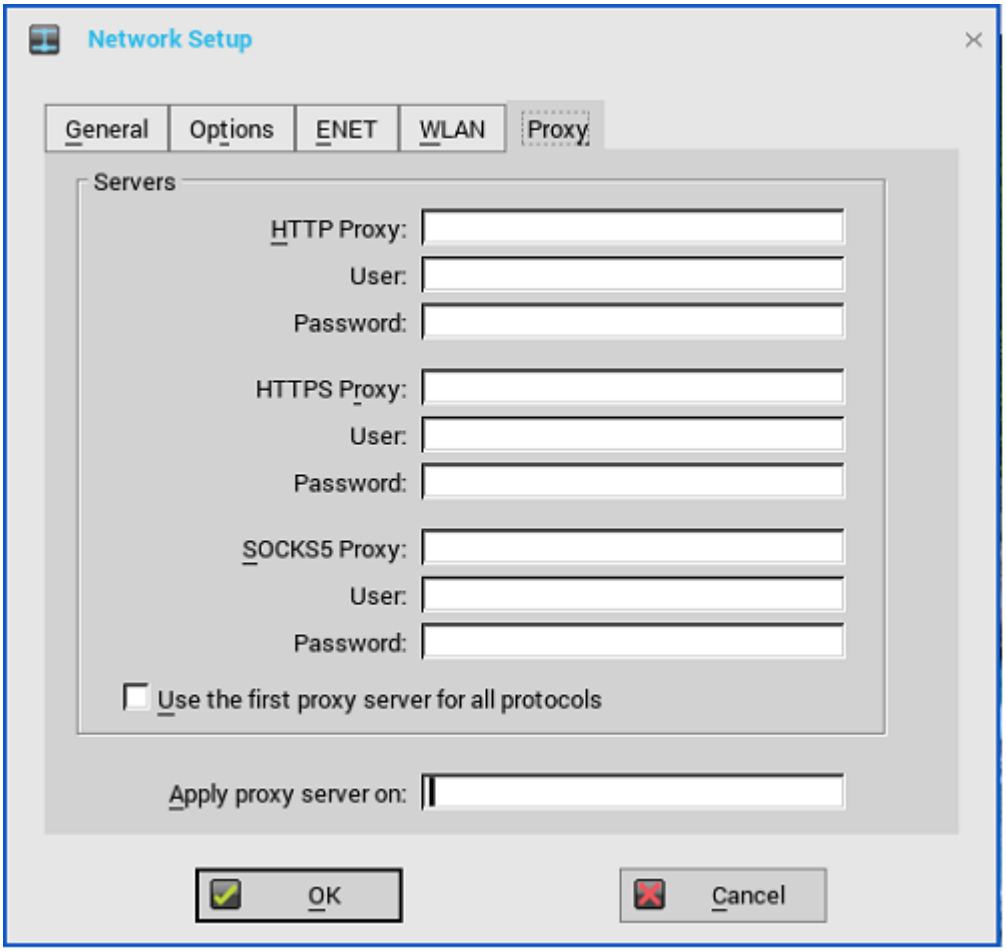
プロキシ設定の設定

ネットワーク**プロキシ**タブは、Wyse Management Suite、HDX Flash リダイレクト、および RealTime Multimedia Engine（RTME）をサポートします。サポート対象のプロトコル——HDX FR、WMS および RTME

- **HDX FR** の場合：HTTP および HTTPS プロトコルはサポート対象です。
  - HTTP と HTTPS の両方が設定されている場合、HDX FR は HTTPS プロキシで稼働します。
  - ユーザー資格情報パススルー認証は、$UN／$PW で実行できます。
- **Wyse Management Suite** の場合： HTTP、HTTPS および Socks5（推奨）プロトコルはサポート対象です。
- **RTME** の場合： HTTP および HTTPS プロトコルはサポート対象です。

1 デスクトップメニューで、**システム設定**をクリックし、**ネットワーク設定**をクリックします。
ネットワーク設定ダイアログボックスが表示されます。

2 **プロキシ**タブをクリックし、次の操作を行います。



a **HTTP プロキシ**ポート番号または **HTTPS プロキシ**ポート番号、**ユーザ**名および**パスワード**を各フィールドに入力します。ただし、資格情報パススルー（$UN／$PW）は、ユーザーサインオン前に開始するので避けてください。
Wyse Management Suite は、WMS／MQTT サーバとの通信には、HTTP／HTTPS および MQTT の両方のプロトコルを使用します。ただし HTTP プロキシは、SOCKS5 プロキシサーバを必要とする MQTT サーバに、TCP パッケージをリダイレクトすることはできません。HTTP サーバのみが使用可能な場合、MQTT を必要とする実時間コマンドは動作しません。

HTTP／HTTPS プロキシのデフォルトポートは 808 で、**SOCKS5 プロキシ**のデフォルトポートは 1080 です。

b すべてのプロトコルに同じプロキシを使用チェックボックスをオンにして、すべてのプロトコルが **HTTP プロキシ**フィールドで同じサーバを使用できるようにします。HTTP と HTTPS のプロキシはどちらも同じホストとポートを使用し、SOCKS5 プロキシエージェントは、HTTP ホストをデフォルトの Socks5 ポート（1080）で使用します。

SOCKS5 プロキシが設定されると、WMS プロキシは SOCKS5 のみを使用します。SOCKS5 が設定されていない場合、WMS プロキシは設定にある別のプロトコル（たとえば HTTP）を探します。

c **プロキシの適用先**フィールドに、サポート対象アプリケーションをセミコロンで区切って、「Wyse Management Suite,FR,RTME」と指定します。

3 **OK** をクリックして設定を保存します。

ユーザーのシナリオ

1 正しいプロキシサーバのホストとポートを設定します。
2 プロキシサーバ設定に従って、ユーザー資格情報を設定します。

システム再起動時に、クライアントは SOCKS5 プロキシサーバ経由で、Wyse Management Suite サーバにチェックインします。MQTT 接続は、SOCKS5 プロキシサーバ経由で確立されます。実時間コマンドは、SOCKS5 プロキシサーバを経由して正しく動作します。

3 Citrix デスクトップに接続し、ブラウザのインターネットオプションでプロキシを設定し、HTTP／HTTPS プロキシ認証を通して HDX FR を再生します。

リモート接続の設定

リモート接続設定ダイアログボックスを使用して、ICA、RDP、Citrix XenDesktop、Microsoft、VMware View、Dell vWorkspace およびその他のブローカーサーバ接続など、シンクライアントのリモート接続を設定します。このダイアログボックスを使用すると、視覚的なオプションおよび一般的な接続設定も設定できます。

- ブローカーセットアップの設定
- 視覚的な設定の設定
- 一般的なオプションの使用
- 認証設定の設定

メモ：クラシックデスクトップオプションでは、リモート接続設定ダイアログボックスによって、デフォルトの RDP 接続を作成して、使用できます。デフォルト以外の接続を作成する場合は、接続マネージャを使用します。詳細については、「接続マネージャの使用」を参照してください。

ブローカーセットアップの設定

ブローカーセットアップを設定するには

1 デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。
リモート接続設定ダイアログボックスが表示されます。
2 **ブローカー**タブのドロップダウンリストで**ブローカー選択**を選択します。
a **なし**を選択し、次のいずれかの接続プロトコルをクリックします。
- **ICA**——詳細については、「ICA 接続の設定」を参照してください。
- **RDP**——詳細については、「RDP 接続の設定」を参照してください。

b 使用可能なブローカー接続の中のいずれか 1 つを選択し、ブローカー設定を設定して、個別の仮想デスクトップ環境に接続します。個別のブローカー設定の手順についての詳細は、「5 コネクションブローカーの設定」を参照してください。
ThinOS に設定できる利用可能なブローカー接続は、次のとおりです。
- **Citrix Xen**
- **VMware View**
- **Microsoft**
- **Dell vWorkspace**
- **Amazon vWorkSpaces**——PCoIP クライアントにのみ使用可能です。

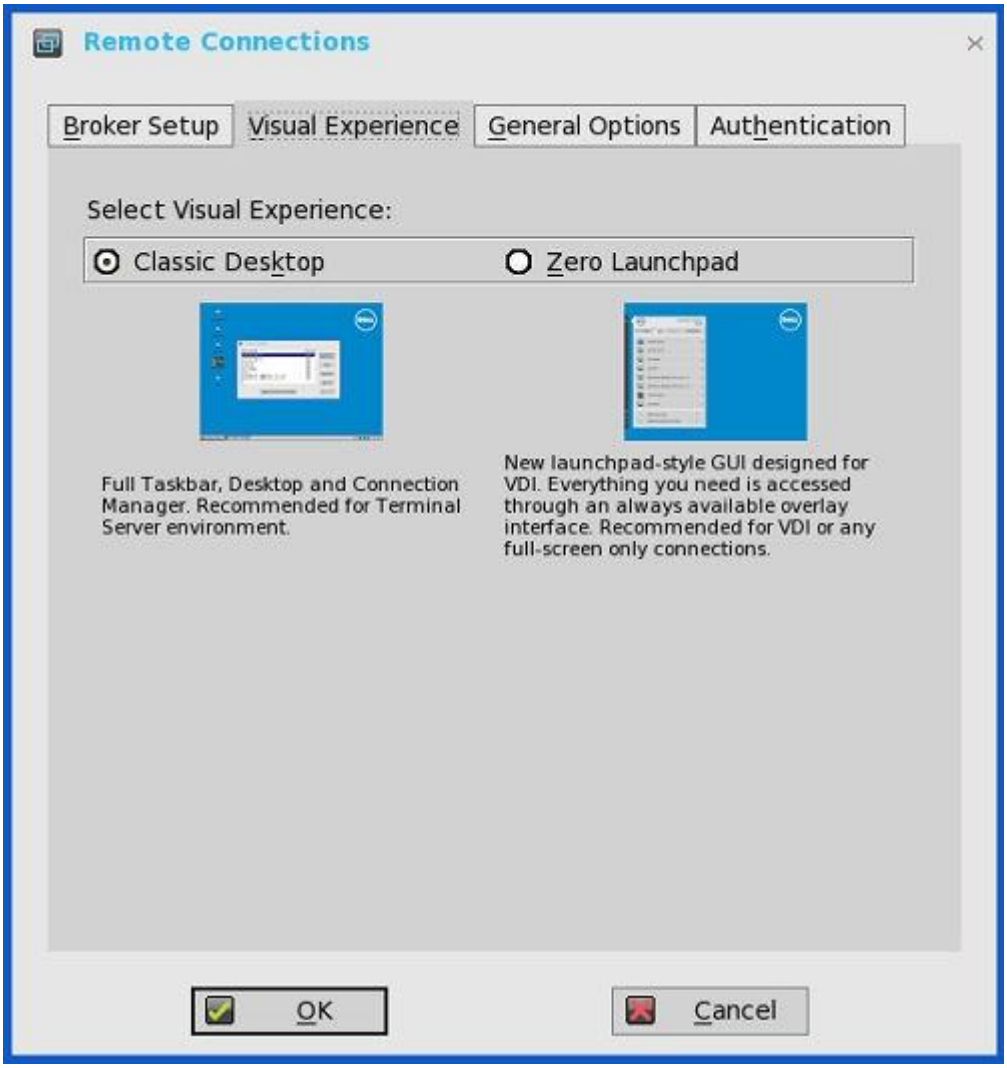
c その他を選択して、次のガイドラインに従います。
- **ブローカーサーバ**——ブローカーサーバの IP アドレスを入力します。
- **自動接続リスト**——個別のブローカーにログイン後、自動的に起動させたいデスクトップの名前を入力します。複数のデスクトップの設定が可能です。各デスクトップの名前はセミコロンで区切り、大文字と小文字は区別します。

3 **OK** をクリックして設定を保存します。

視覚的な設定の設定

視覚的な設定を設定するには

1 デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。
リモート接続設定タブが表示されます。
2 **表示設定**タブをクリックし、次のガイドラインに従います。



メモ：ブローカータブで入力した Citrix ブローカーサーバに対して StoreFront スタイルチェックボックスをオンにしていると、表示設定タブはグレーアウトされます。

a **クラシックデスクトップ**——ThinOS ユーザーが使い慣れているフルタスクバー、デスクトップ、および接続マネージャを表示します。このオプションは、ターミナルサーバ環境に対して、および ThinOS 6.x バージョンとの下位互換性を確保する場合にお勧めします。

b **Zero ラウンチパッド**——VDI を使用するために設計された新しいラウンチパッドスタイルの GUI を表示します。機能には、常に使用できるインターフェイスからアクセスできます。このオプションは、VDI およびフルスクリーンのみの接続に対してお勧めします。設定には、ツールバー、ホットキー、および接続アイコンに関するオプションも使用できます。

Zero ラウンチパッドを選択する場合は、以下のガイドラインに従います。

- チェックボックスをオンにして、左ペインでのゼロツールバーのアクティブ化を有効にします。
  - マウスを画面で静止したときに左ペインでゼロツールバーをアクティブにする場合は、ボタンを選択します。ゼロツールバーがアクティブになるまでの時間を、0、0.5、1 秒から選択する必要があります。
  - クリックした後にのみ左ペインでゼロツールバーをアクティブにする場合は、ボタンを選択します。
- チェックボックスをオンにして、ツールバーを表示するホットキーを無効にします。
- チェックボックスをオンにして、使用するセッションが 1 つのときにツールバーを常に無効にします。
- チェックボックスをオンにして、ホームアイコンを無効にします。

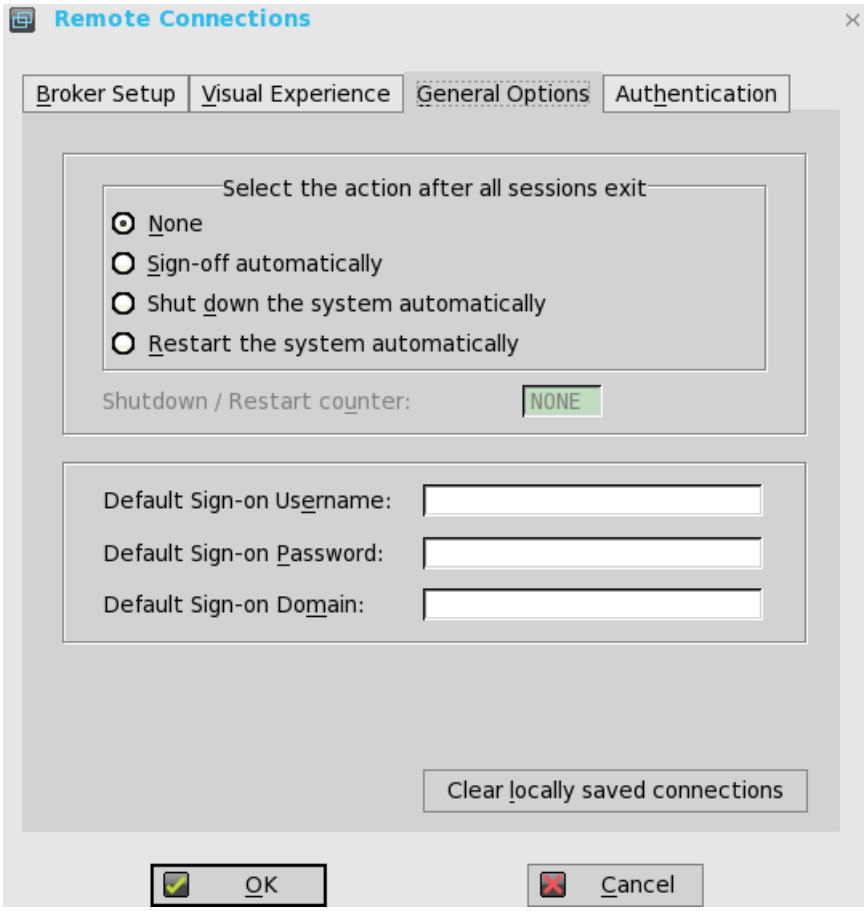
3 **OK** をクリックして設定を保存します。

一般的なオプションの設定

一般的なオプションを設定するには

1 デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。

リモート接続設定ダイアログボックスが表示されます。



2 **一般設定**タブをクリックし、次のガイドラインに従います。

a 使用可能なオプションをクリックし、開いているすべてのデスクトップを終了した後のアクションを選択します。使用できるオプションは、**無し、自動的にサインオフ、自動的にシャットダウン**および**自動的に再起動**です。

ⓘ **メモ：デフォルトでは、無しが選択され、シンクライアントは自動的にターミナルデスクトップに戻ります。**

b **既定のユーザ**——デフォルトのユーザー名を入力します。

c **既定のパスワード**——デフォルトのパスワードを入力します。

d **既定のドメイン**——デフォルトのドメインを入力します。

e **ローカル接続設定の削除**をクリックして、ローカルに保存した接続をクリアします。

ⓘ **メモ：3 つのデフォルトのサインオン資格情報（ユーザー名、パスワード、ドメイン）をすべて入力した場合は、システムが起動すると、自動的にデスクトップにログオンします。**

認証設定の設定

認証設定を設定するには

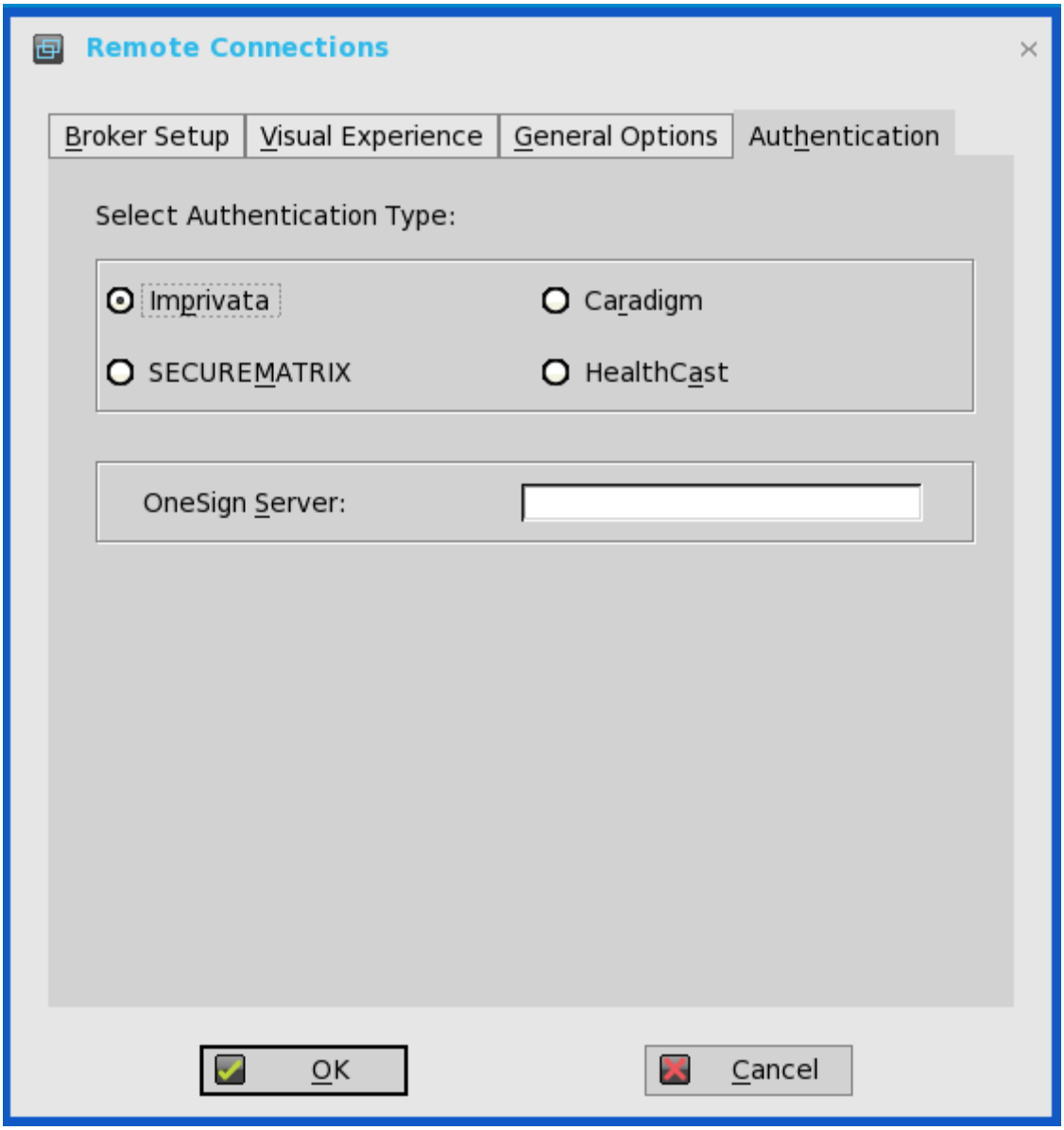
1 デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。

リモート接続設定ダイアログボックスが表示されます。

2 **認証設定**タブをクリックし、認証タイプを選択します。

次の認証のオプションが表示されます。

- Imprivata——Imprivata OneSign サーバの設定
- Caradigm——Caradigm サーバの設定
- SECUREMATRIX——SECUREMATRIX の設定
- HealthCast——HealthCast 入門



3 望ましい認証を設定し、**OK** をクリックして設定を保存します。

Imprivata OneSign サーバの設定

OneSign Virtual Desktop Access では、仮想デスクトップ環境で、シームレスな認証処理を提供し、No Click Access と統合してデスクトップとアプリケーションへのシングルサインオンを可能にします。

OneSign サーバを設定するには、OneSign サーバの詳細を入力し（https://ip または https://FQDN のいずれかの値）、クライアントを再起動して **Log on** ダイアログボックスを表示します。次に、資格情報を入力し、ログオンに使用する **VDI broker** ダイアログボックスを開きます。この機能を INI ファイルに設定することもできます。『Dell Wyse ThinOS INI Reference Guide』を参照してください。

次の OneSign 機能またはアクションをサポートします。

- クライアントおよびブローカーの認証
  - Citrix XenApp
  - Citrix XenDesktop
  - VMware View
- キオスクモード
- 迅速なユーザー切り替え
- OneSign 以外のユーザーによる VDI アクセス
- ホットキーの切断
- 近接カードリーダーのリダイレクト
- 質問と回答でガイドするログイン
- パスワードによる認証
- パスワードによる認証およびパスワードの変更
- パスワードによる認証およびパスワードの変更または無効な新規パスワード
- 近接カードとパスワードによる認証
- 近接カードと PIN による認証
- 近接カードと PIN による認証または PIN 未登録
- 近接カードによる認証のみまたはパスワードの取得
- ユーザーID のパスワードの取得
- ユーザーID のパスワードのリセット
- ユーザーID のパスワードの更新
- 近接カードの登録
- 近接カードによるターミナルのロック／アンロック

ThinOS は、最新の Imprivata WebAPI バージョン 5 をサポートします。これには、OneSign Objects（WebAPI v4）および Fingerprint Authentication（WebAPI v5）が含まれます。

Imprivata サーバ上のオブジェクトの設定

Imprivata WebAPI は、バージョン 4 からバージョン 5 にアップデートされています。前のバージョンから、クライアントの動作のさまざまな側面を制御できる設定オブジェクトがサポートされています。Imprivata WebAPI 機能は、OneSign サーバ 4.9 以降のバージョンで使用できます。設定オブジェクトは、クライアントの動作のさまざまな側面を制御します。

次のガイドラインに従って、Imprivata サーバ上のオブジェクトを設定します。

1 **一般的な設定オブジェクトの設定**

a Imprivata サーバで、**Computer policy** をクリックし、**General** タブをクリックします。

b ユーザーがシャットダウンしてロック画面からワークステーションをリスタートするためのチェックボックスをオンにします。

メモ：OneSign GINA では、シャットダウン用のボタンとリスタート用のコマンドがユーザーに表示されます。

Imprivata サーバでは、次の設定オブジェクトがサポートされます。

- **シャットダウン Allow**

– チェックボックスをオンにしてこの機能を有効にすると、**シャットダウン**して**リスタート**するためのアイコンが、ThinOS のログインウィンドウとロックされたウィンドウに表示されます。

– チェックボックスをオフにすると、**シャットダウン**して**リスタート**するためのアイコンはグレーアウトされます。

- **FailedOneSignAuth Allow**——Yes または No のオプションのみサポートされます。No ラジオボタンをクリックすると、OneSign 以外のユーザーがブローカーにログインできます。
- **Logging Allow**
  – この機能を使用すると、OneSign ログを ThinOS に出力できます。これに応じた INI 設定が必要です。
  – Loglevel = 0/1/2/3。デフォルト値は 0 です。0 を設定すると、ログは表示されません。
- **Display name format**——ポップアップ通知にさまざまな形式でアカウント名を正しく表示できます。

2 **Walk Away 設定オブジェクトの設定**

Imprivata サーバで、**Computer policy** をクリックし、**Walk Away** タブをクリックします。

- **Key mouse inactivity enabled and behavior**——**in addition to keyboard and mouse inactivity** チェックボックスはサポートされていません。
- **Passive proximity cards**
  – 近接カードを使用してコンピュータをロックするには、**Tap to lock** チェックボックスをオンにします。
  – コンピュータをロックし、別のユーザーとしてログインする場合は、**Switch users** チェックボックスを選択します。
  – INI パラメータは、TapToLock = 0/1/2 です。
- **Lock warning enabled and type**——None、Notification balloon および Screensaver の 3 つのタイプをサポートします。
  – None——警告メッセージは表示されません。
  – Notification balloon——ThinOS によって、通知ウィンドウが表示されます。
  – Screensaver——ワークステーションがロックする前に、ディスプレイの内容を非表示にします。
- **Warning message**——警告メッセージをカスタマイズできます。
- **Lock Screen type**——覆い隠すタイプのみサポートします。
- **Hot key to lock workstation or log off user**——ThinOS では、次のキーをサポートします。
  「F1～F12」、「BKSP」、「DEL」、「DOWN」、「END」、「ENTER」、「ESC」、「HOME」、「INS」、「LALT（左 ALT）」、「LEFT」、「LCONTROL（左 CONTROL）」、「NUMLOCK」、「PGDN」、「PGUP」、「RCONTROL（右 CONTROL）」、「RIGHT」、「RTALT（右 ALT）」、「SPACE」、「TAB」、「UP」、「a～z」、「A～Z」、「0～9」および修飾キー「 + 」、「%」、「^」（Shift、Alt および Control）

- **Suspend action**——サーバ設定が、ThinOS 上でこの機能を制御します。そのため、SuspendAction = 0/1 という新しい INI が追加されました。0 はロックを意味し、1 はサインオフを意味します。

3 **SSPR 設定オブジェクトの設定**

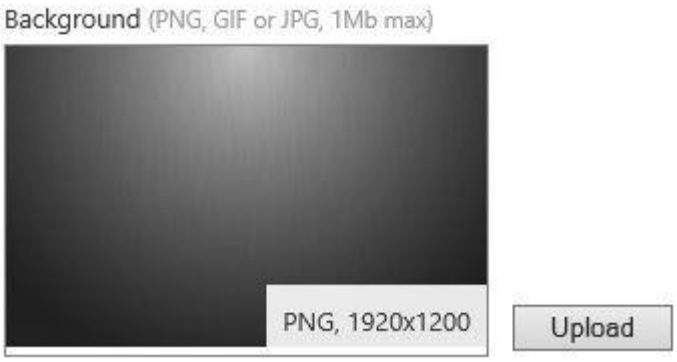
SSPR 設定オブジェクトが、ユーザーによるセルフサービスのパスワードリセット操作を制御します。有効化された属性によって、緊急でアクセスが必要な場合に、パスワードのリセットをユーザーに許可するかどうかを指定できます。必須の属性によって、緊急でアクセスが必要な場合に、ユーザーが必ずパスワードをリセットする必要があるかどうかを指定できます。

4 **RFIDeas 設定オブジェクトの設定**

RFIDeas 設定オブジェクトが、RFIDeas リーダーの動作を制御します。この設定は、2 つの方法で設定できます。1 つは OneSign サーバのコンピュータポリシーで、もう 1 つは ThinOS INI です。

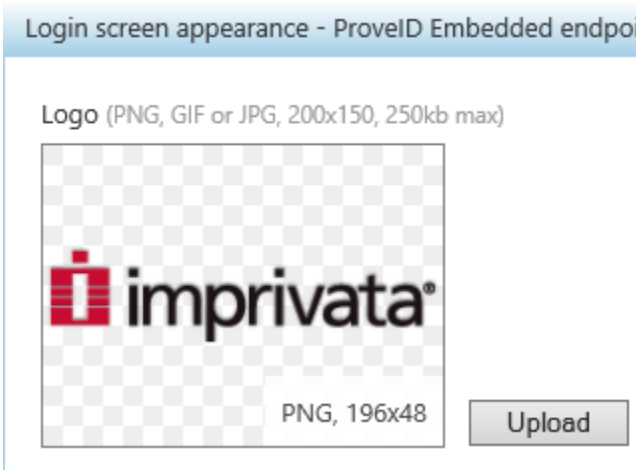
5 **カスタム背景設定オブジェクトの設定**

Imprivata サーバで、**Computer policy** をクリックし、**Customization** タブをクリックします。



6 **共同ブランディング設定オブジェクトの設定**

Imprivata サーバで、**Computer policy** をクリックし、**Customization** をクリックします。



ロゴイメージが、そのままの状態で ThinOS のすべてのダイアログボックスに表示されます。

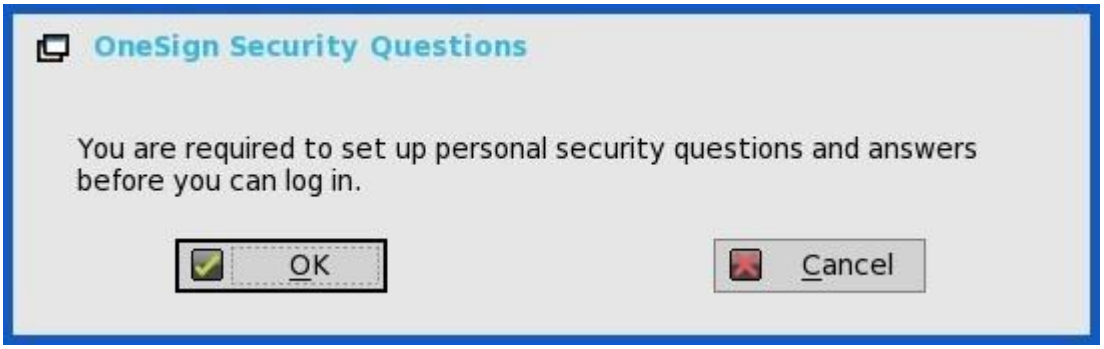
7 **SSPR カスタマイズ設定オブジェクトの設定**

- サインオン UI とロックウィンドウに表示されるテキストはカスタマイズできます。
- ThinOS がサポートする最大サイズは 17 文字です。

ThinOS の UI:

8 **Password Self-Services force enrollment 機能**

このチェックボックスをオンにすると、プライマリの認証パスワードをリセットできます。



Imprivata OneSign サーバの INI 設定

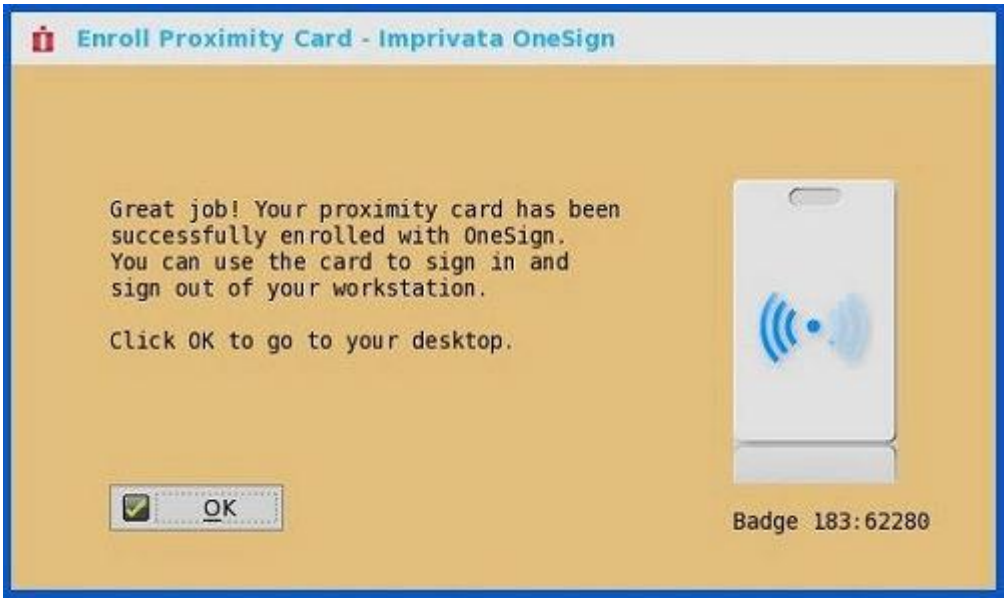
新しい INI パラメータ、AutoAccess = command が追加されました。新しい値は AutoAccess = Local です。AutoAccess が Local に設定されている場合、ThinOS は Imprivata OneSign アプライアンスに設定されているブローカーを無視し、wnos.ini またはクライアントでローカルに定義したブローカー／接続を開始します。Imprivata ユーザー認証をサポートしながら、vWorkspace、Microsoft およびその他の ThinOS 接続を開始できます。

近接カードの登録

1 近接カードをタップします。カードを登録するページが表示されます。

2 資格情報を入力し、**OK** をクリックします。

近接カードが正常に登録されます。



Imprivata の生体認証によるシングルサインオン

指紋認証機能は信頼性が高く、複製、改ざん、悪用が簡単にはできません。

OneSign サーバの前提条件は、次のとおりです。

- WebAPI v5 以降のバージョンをサポートする、Imprivata v4.9 以降のアプライアンスのバージョンが必要となります。
- 指紋認証ライセンスが必須です。

メモ：

- サポート対象のプロトコルは、RDP、ICA、および PCoIP です。
- 必要となる指紋リーダーデバイスは、次のとおりです。
  - ET710（PID 147e VID 2016）
  - ET700（PID 147e VID 3001）

サポート対象のシナリオ

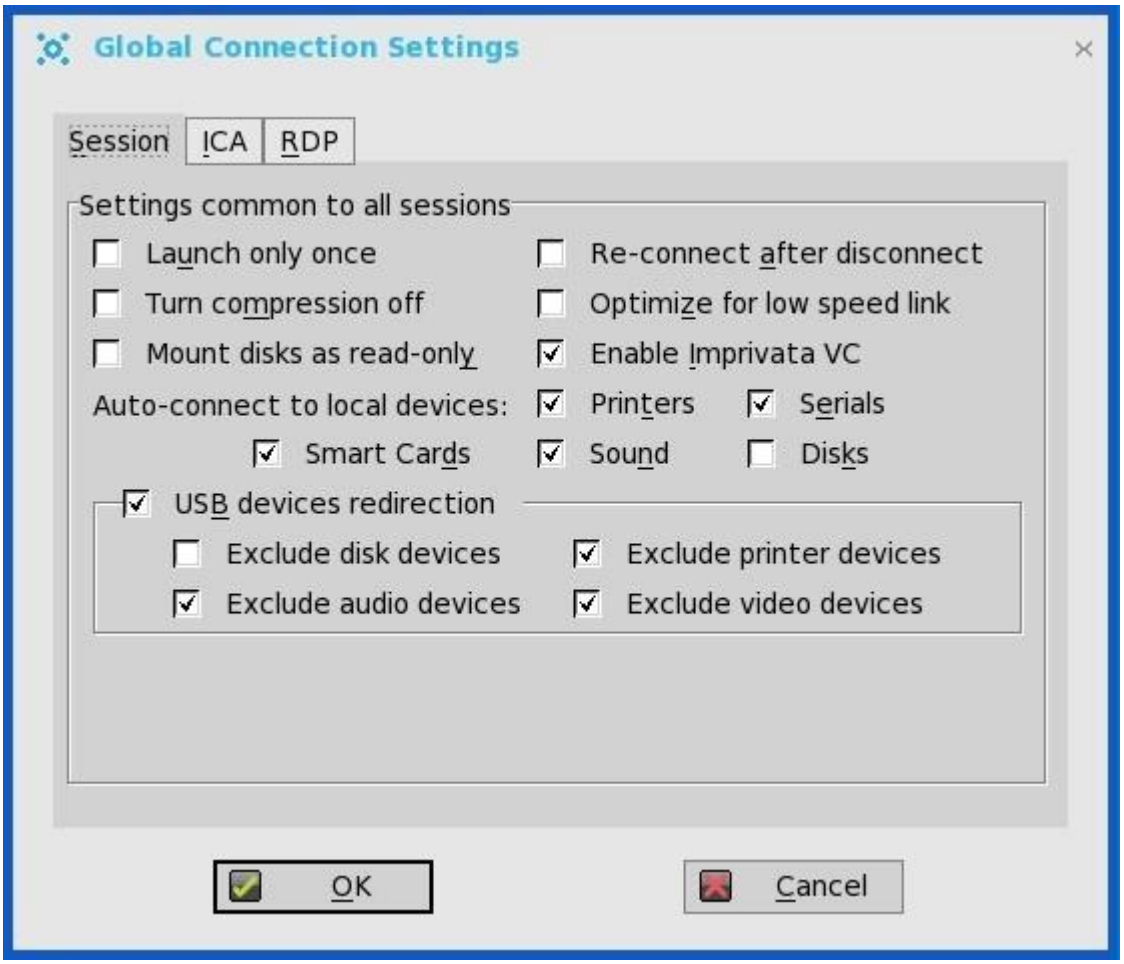
1 指紋認証を使用して、ThinOS デバイスへのサインインまたはロック解除を行います。

- ThinOS に OneSign サーバを設定し、指紋リーダーデバイスをプラグインします。
- OneSign サーバが初期化されると、ThinOS Fingerprint ウィンドウが自動的に表示されます。

- 指紋認証は ThinOS アンロックウィンドウで稼働します。

2 指紋認証を使用して、仮想デスクトップのロック解除を行います。

- ThinOS Global Connection 設定から、Imprivata の仮想チャネルを有効にします。



- セッション中に仮想デスクトップをロックすると、Fingerprint ウィンドウが自動的に表示されます。

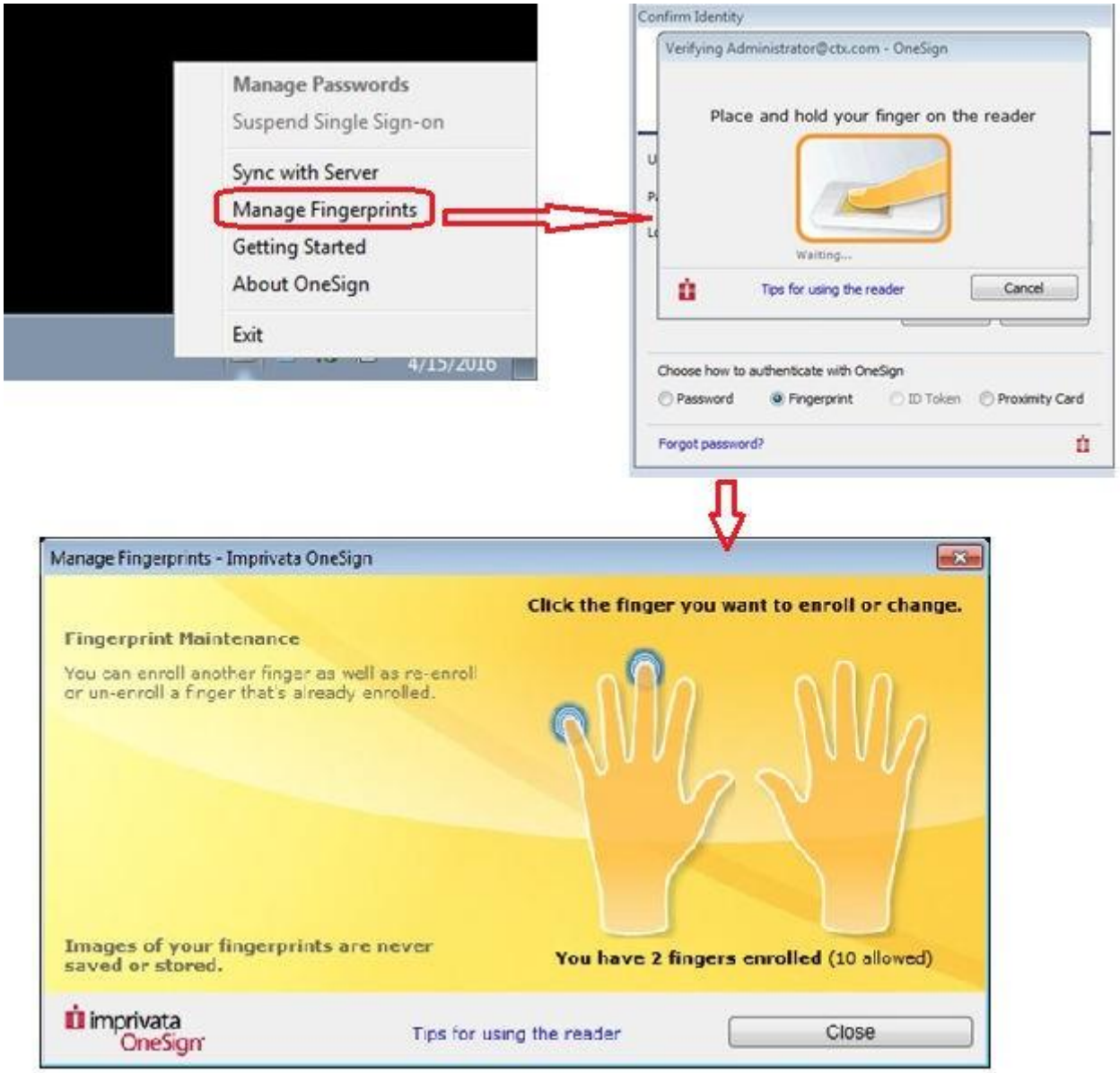
3 仮想デスクトップで Fingerprints を管理します。

- Legend Fingerprint Management は、サポートされています。
- Imprivata Confirm ID が有効になった Fingerprint 管理は、サポートされていません。登録を終了するには管理者とユーザーの両方が必要となり、この操作を行う際は Windows プラットフォームを使用することをお奨めします。

指紋を管理するには、以下の操作を行います。

a システムトレイの OneSign agent アイコンを右クリックします。

b **Manage Fingerprints** をクリックし、指紋を管理するために、表示されたウィンドウに正しい資格情報を入力します。

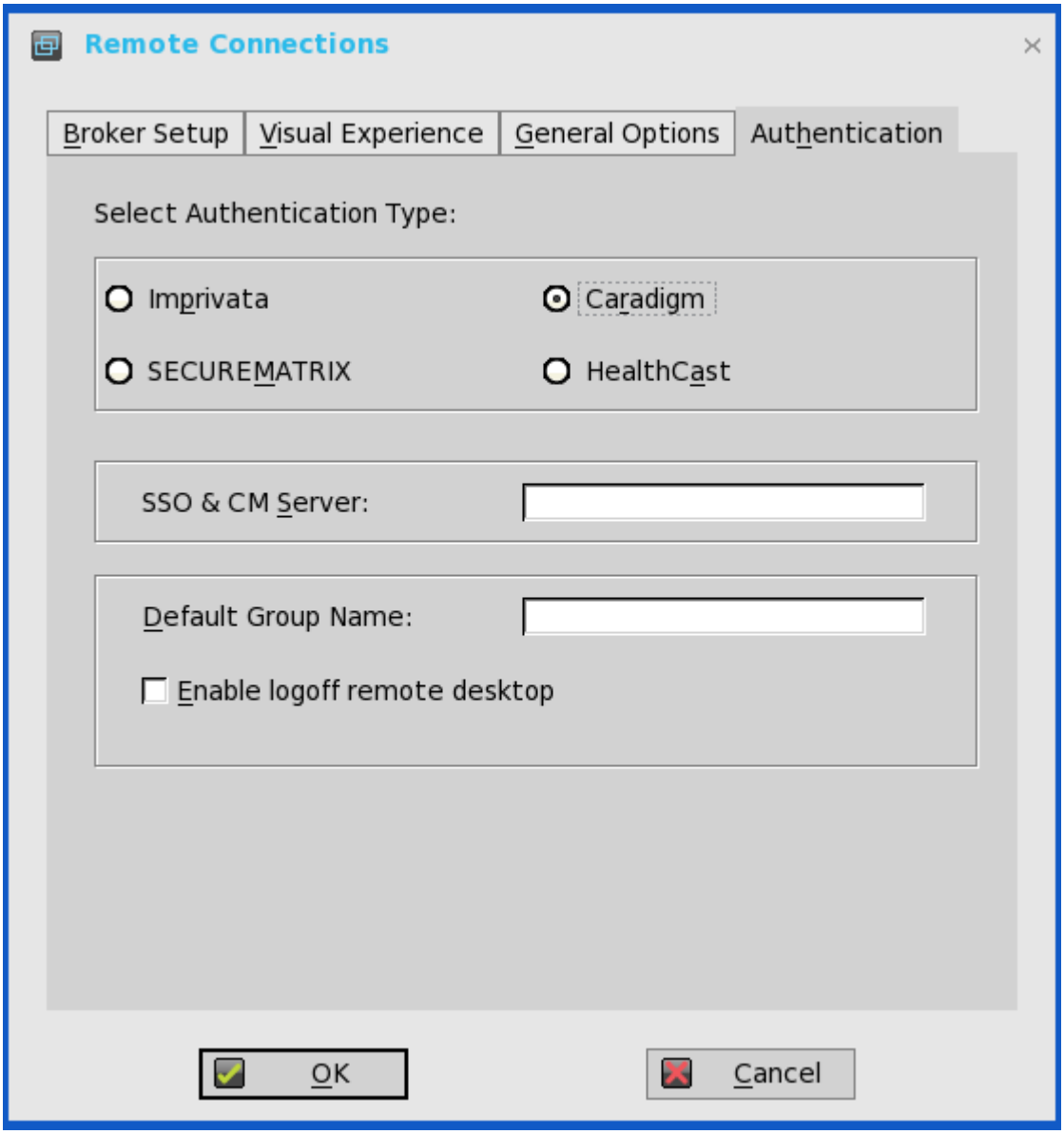


Caradigm サーバの設定

Caradigm Single Sign-on and Context Management（SSO & CM）は、Caradigm 社の製品で、シングルサインオンサービスとコンテキスト管理サービスを提供します。Caradigm のソリューションは、ThinOS 8.1 から統合されています。

ThinOS への Caradigm 統合を設定するには、以下の操作を行います。

1 デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。
リモート接続設定ダイアログボックスが表示されます。
2 **Authentication** タブをクリックし、**Caradigm** をクリックします。



a **SSO & CM Server**——シングルサインオン（SSO）サーバとコンテキスト管理（CM）サーバの IP アドレスを入力します。

b **Default Group Name**——**Default Group Name** ボックスに、デフォルトグループの名前を入力します。

c **Enable logoff remote desktop**

- チェックボックスをオンにし、システムサインオフの前に現在のユーザーをサインオフします。
- チェックボックスをオフにし、セッションを切断します。

3 **OK** をクリックして設定を保存します。

Caradigm Vault Server の設定

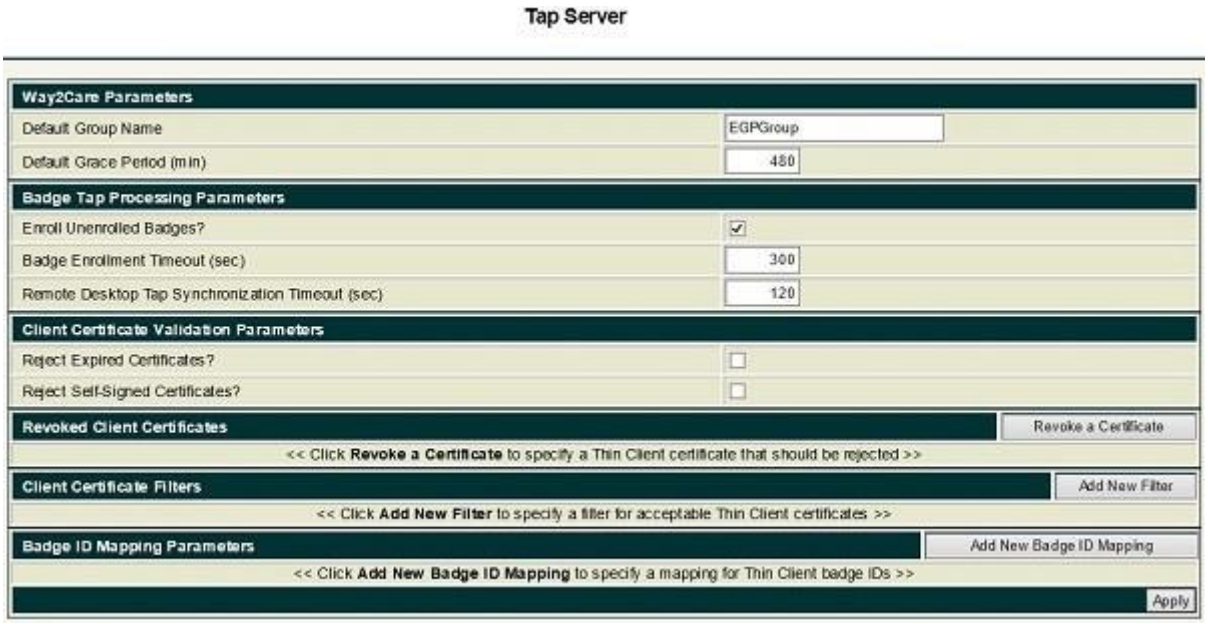
ThinOS で Caradigm Vault Server を設定するには

1 デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。
リモート接続設定ダイアログボックスが表示されます。

2 **Authentication** タブをクリックし、**Caradigm** ボタンをクリックし、**SSO & CM Server** の IP アドレスを入力し、**OK** クリックします。

3 Caradigm Vault Server で、次のガイドラインに従います。

- **Enroll unenrolled badges** オプションがオンになっていることを確認します。
- すべてのバッジ ID マッピングのエントリーが削除されていることを確認します。



4 **SSO&CM** → **Advanced Configurations** をクリックし、次のガイドラインに従います。

a **Enable Proximity Support** チェックボックスがオンになっていることを確認します。

b **Enable way2care** チェックボックスがオンになっていることを確認します。

5 Caradigm Vault Server に対して証明書を準備するには、次のガイドラインに従います。
Caradigm Vault Server では、Tap Server とシンクライアント間の接続の検証に、証明書を使用します。

a 証明書を要求するには、次の操作を行います。

- 証明書は、自社の証明機関によって発行される必要があります。
- 証明書を以下の 2 つの形式で用意します。
  - プライベートキーを含む PFX 形式
  - PEM 形式。つまり、Base64 でエンコードされたテキストベースの DER ファイル。Caradigm.cer、Caradigm.pfx などです。

b 証明書をシンクライアントにインポートするには、次の 2 つのオプションのいずれかを行います。

- **システム設定** → **システムツール** → **Certificates** をクリックし、USB ストレージからファイルサーバに証明書をインポートします。
- INI ファイルを使用して証明書をインポートします。

```
AddCertificate = client_cert.pfx password = passpass
```

c Vault サーバに証明書を追加するには、次の操作を行います。

Thin Client Certificates ページを使用して、シンクライアントデバイスの証明書を追加します。証明書は PEM 形式のテキスト、つまり Base64 でエンコードされたテキストベースの DER ファイルにする必要があります。

- メモ帳で DER cert ファイルを開きます。
- Vault Server Admin Console にログインし、**Appliance** → **Thin Client Certificates** をクリックします。
- メモ帳のテキストを Vault サーバにコピーします。

VDI サーバおよびデスクトップでの設定
Caradigm の ThinOS ソリューションでは、VMware View Horizon 6、Citrix XenApp 6.5、Citrix XenDesktop 5.6 および Citrix XenDesktop 7.6 など、複数のタイプの VDI サーバをサポートします。

VDI サーバおよびデスクトップを設定するには

- サーバとデスクトップに Caradigm デスクトップコンポーネントをインストールします。
- Vault サーバの IP を指定し、有効なセキュリティトークンを指定します。
- 次の行を、\programdata\sentillion\vergence\Authenticator.ini 設定ファイルの Service セクションに追加します。

```
TapServerIdentification = True
RemotePromptForPassword = Badge
```

この機能をサポートするには、VDI サーバとデスクトップにインストールされている SSO および CM クライアントを、最新バージョンの 6.2.5 にアップグレードする必要があります。

SECUREMATRIX の設定

SECUREMATRIX は、エンタープライズアプリケーションとクラウドベースのアプリケーションのセキュリティを拡張するとともに、デスクトップ、Windows、VPN、イントラネット、エクストラネット、Web サーバ、e コマースおよびその他のネットワークリソースへの認証に使用可能なワンタイムパスワード（OTP）をエンドユーザーがシームレスに操作できるようにします。

SECUREMATRIX サーバを設定するには、https://ip の値または https://FQDN の値を入力し、クライアントを再起動して **log on** ダイアログボックスを表示します。次に、資格情報を入力して、ログオンに使用する **VDI broker** ダイアログボックスを開きます。この機能を INI ファイルに設定することもできます。『Dell Wyse ThinOS INI ガイド』を参照してください。詳細については、SECUREMATRIX のドキュメントを参照してください。

HealthCast 入門

HealthCast シングルサインオン（SSO）ソリューションは、要求の厳しい環境で、ユーザーの利便性を改善し、ワークフローを効率化し、セキュリティ順守を強化するように設計されています。物理的アクセスに使用されるのと同じ近接型カードを用いて、個別のユーザーセッションへのタップイン、タップアウトや、ThinOS のデバイスにうっかり開いたままのセッションのタップオーバーを行います。通常、パスワードの入力は 1 日 1 回のみ行い、近接カードを使用してワークフローを効率化し、時間を節約しつつ、安全に共有コンピュータ間を移動します。また近接カードは、組織で設定されている場合は、PIN で保護することも可能です。HealthCast SSO ソリューションは、ユーザーのセルフサービスによるパスワードリセットにも対応しているので、ヘルプデスクにコールせずに、自分でパスワードがリセットできます。

メモ：ThinOS の HealthCast SSO ソリューションはクライアント／サーバソリューションです。ThinOS はクライアント側の機能を提供しますが、このソリューションを正しく機能させるには、サーバシステムに HealthCast サーバのコンポーネントをインストール、設定することも必要です。1 つまたは複数のサーバインストール実行ファイル、サーバ要件、設定情報については、HealthCast Web サイトの HealthCast にご連絡ください。

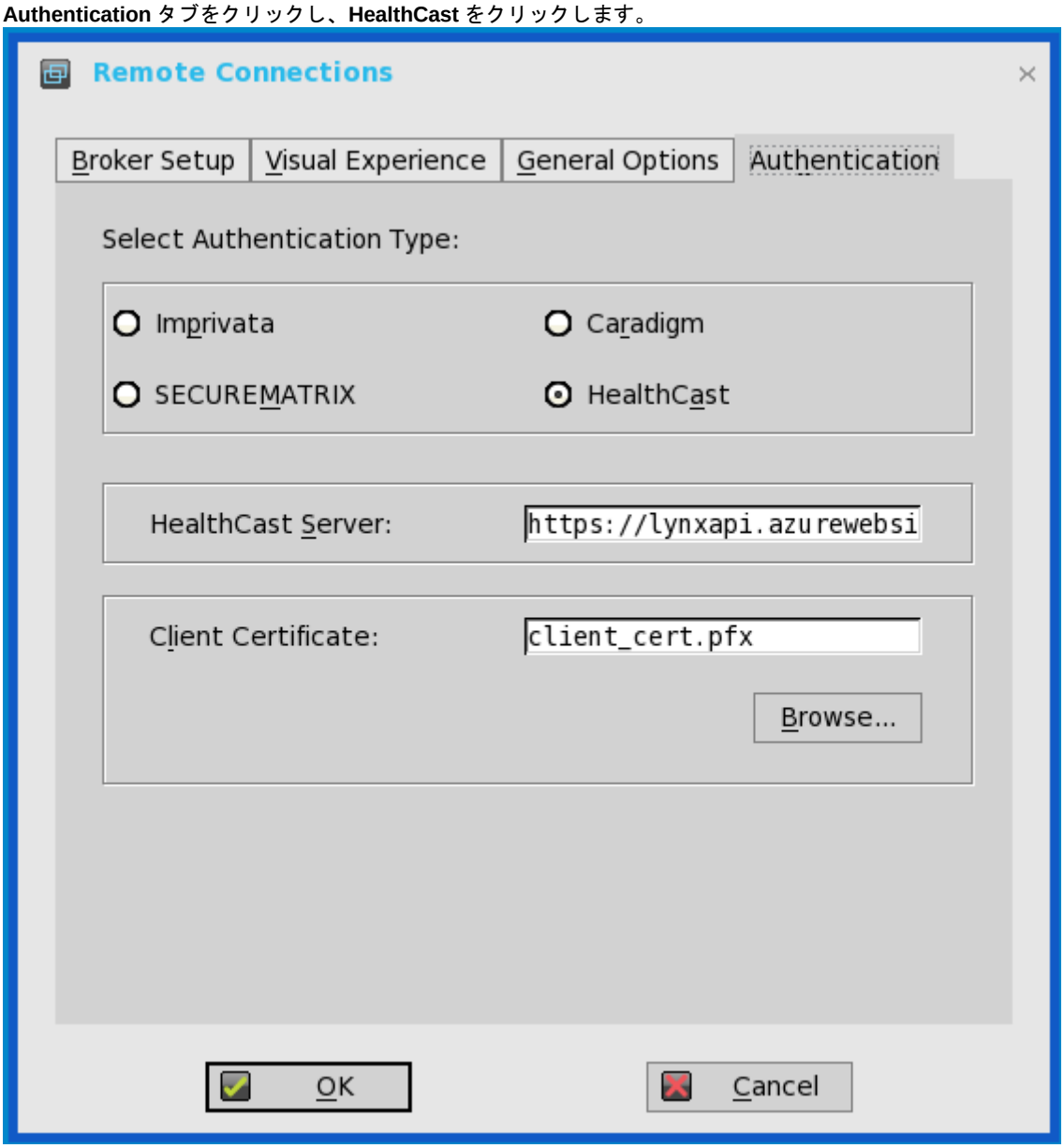
ThinOS での HealthCast の設定

HealthCast SSO ソリューションを実装するには、HealthCast Web API サーバと ThinOS リリースを統合します。HealthCast SSO ソリューションを使用するには、ThinOS を設定して HealthCast Web API サーバを使用する必要があります。これは、INI ファイル（wnos.ini）または ThinOS UI を使用して実施できます。デルは、大規模な導入には、INI ファイルを使用することをお勧めします。

ThinOS UI 設定

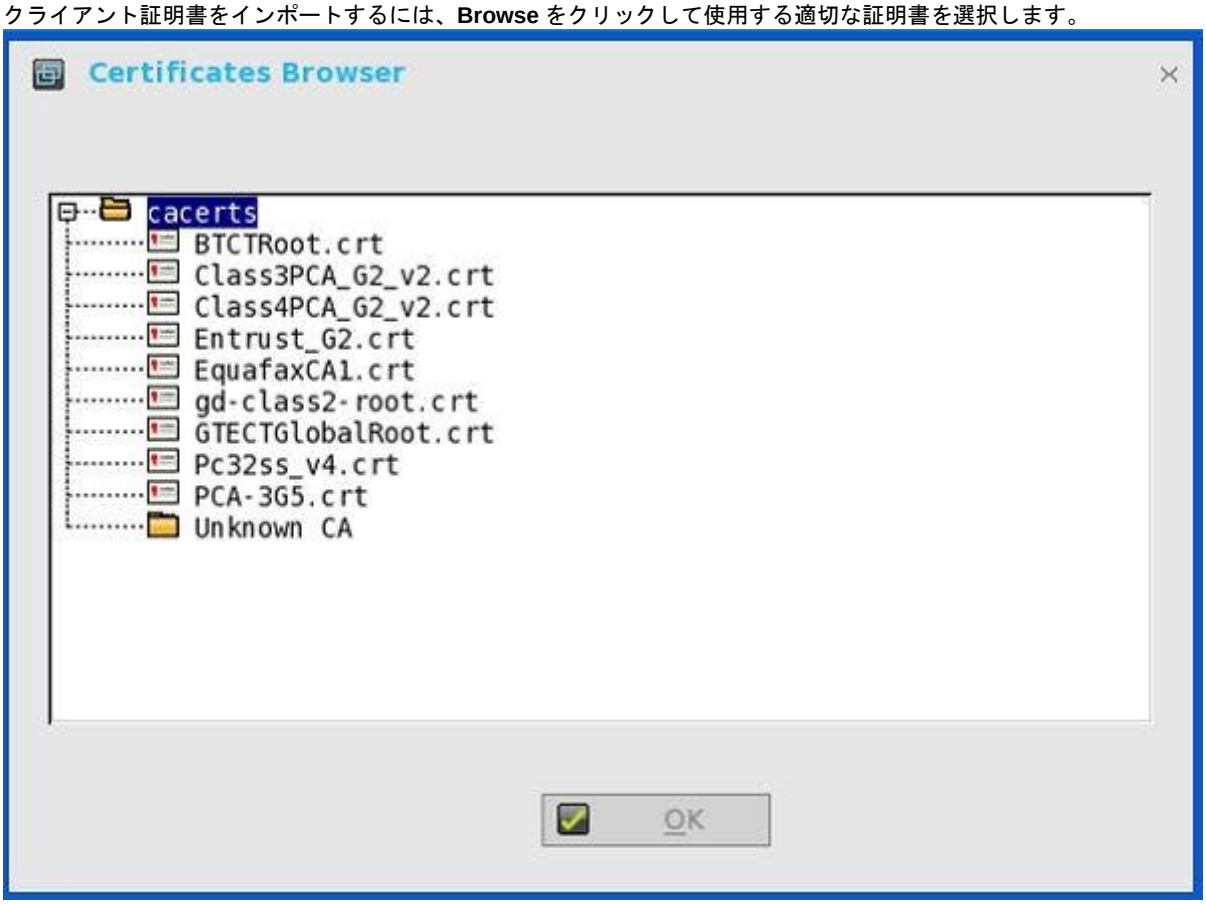
- HealthCast Web API を使用するには、シンクライアント側に HealthCast 設定を行います。設定するには、次の操作を行ってください。
  a デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。
  リモート接続設定ダイアログボックスが表示されます。

b **Authentication** タブをクリックし、**HealthCast** をクリックします。



c 表示されたボックスに、HealthCast サーバの詳細情報を入力します。

d クライアント証明書をインポートするには、**Browse** をクリックして使用する適切な証明書を選択します。



e **OK** をクリックして設定を保存します。

INI 設定

INI パラメータで設定するには、次の INI パラメータを wnos.ini ファイルに追加します。

HealthCastServer——クライアントが HealthCast Web API サーバに接続するのに必要なサーバアドレスとオプション。
HealthCastServer=<https address> セキュリティモード=<default, full, warning, low> ClientCertificate=<cert-pfx-file-name>
例：HealthCastServer=https://server1.example.com セキュリティモード=full ClientCertificate=client-cert.pfx.

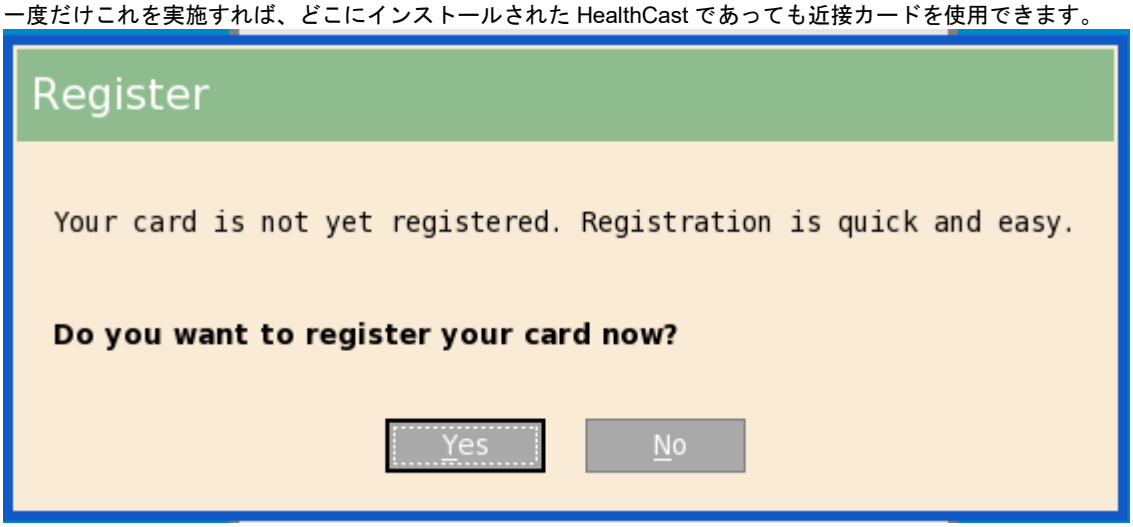
INI パラメータの詳細については、『Dell Wyse INI Reference Guide』を参照してください。

HealthCast SSO 機能と ThinOS 上での機能

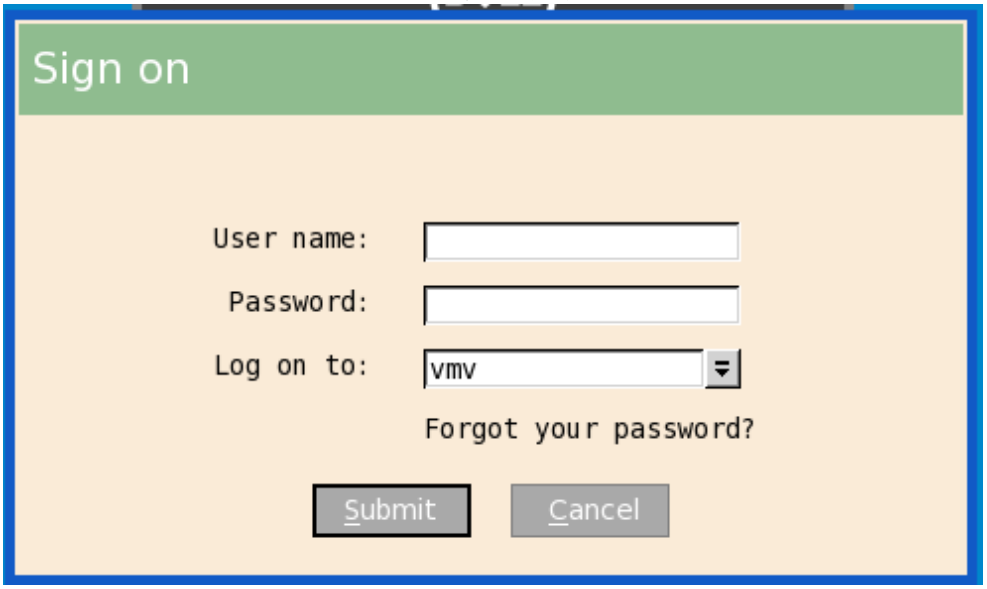
HealthCast SSO 機能と ThinOS 上での機能は次のとおりです。

- **近接カードの登録**——HealthCast はユーザーによる自己登録をサポートします。したがって、近接カードを特別な登録所に持っていったり、IT の担当者に依頼したりする必要はありません。その代わり、非登録の近接カードを端末にタップするだけで、簡単な登録手続きができます。

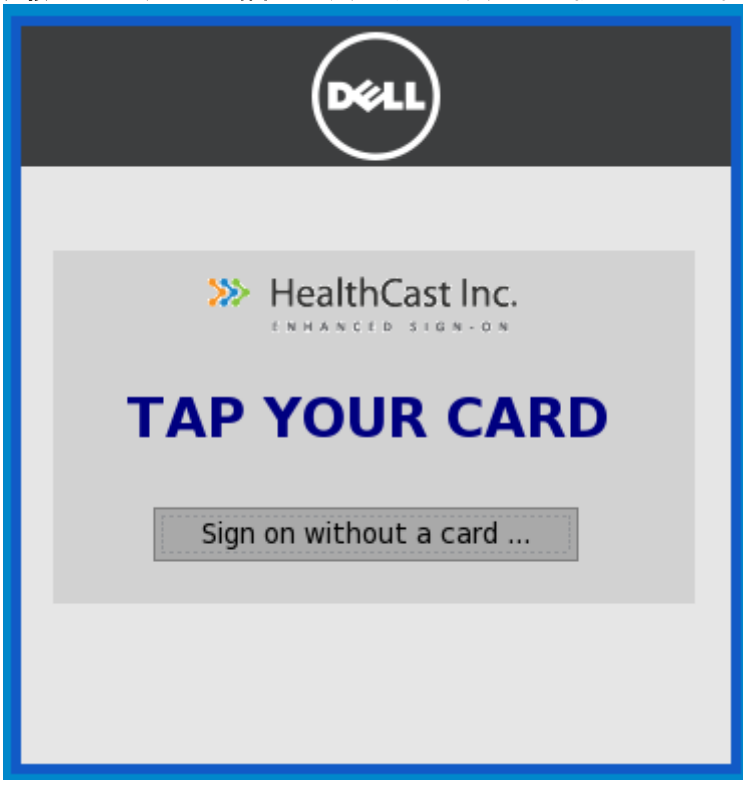
一度だけこれを実施すれば、どこにインストールされた HealthCast であっても近接カードを使用できます。



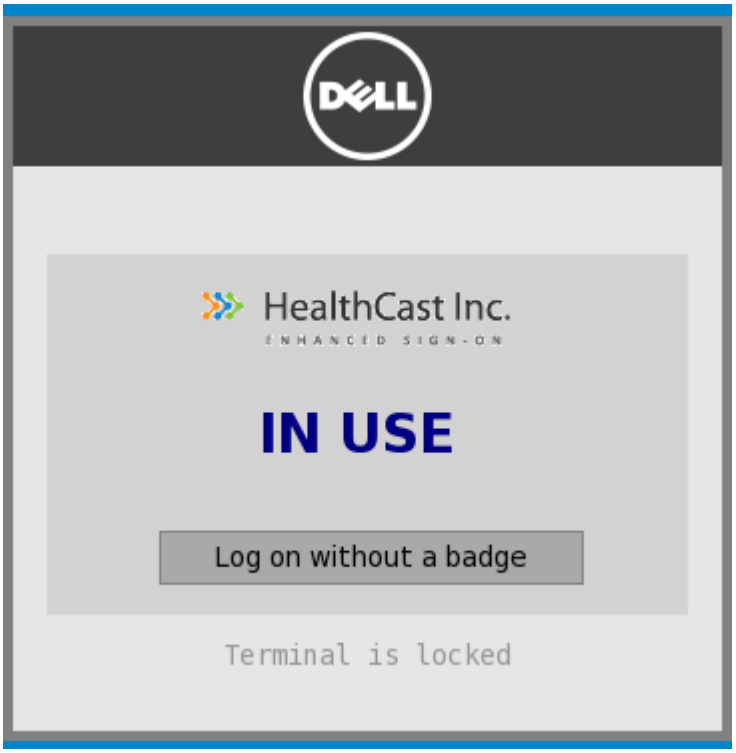
- **手動ログインと端末のロック／アンロック**——カードを持っていない場合やカード使用を選択しない場合、ユーザー名とパスワードを使用して手動でログインします。管理者は、ユーザーが近接カードでサインオンすることを望む場合は、手動ログインを無効にできます。手動ログインでサインオンした場合は、端末をロック／アンロックすることもできます。



- **近接カードログインと端末のロック／アンロック**——近接カードを登録後、カードを端末にタップしてログインします。



安全のためにセッションをロックできますが、戻ったときにすぐにアクセスできるようリモートセッションに接続したままにしておきます。これをするには近接カードをタップし、これでセッションがロックされます。



セッションを再開するには、再度カードをタップします。

- **離席**——セッションがオープンされたままの場合にロックまたはログオフするよう、端末を設定できます。自動的にロックまたはログオフされるまでの時間は、便利なウェブ管理アプリケーションを使用して管理者が設定できます。
- **タップオーバー**——セッションがロックまたはオープンされたままの場合は、次のユーザーは自分の近接カードをタップすることで前のセッションを切断し、自分のセッションにログインできます。

- **カード忘れ**——カードを家に忘れた場合、テンポラリカードを受取って、このセクションで説明した簡単な登録手続きと同じ手続きで、その一日用に登録できます。
- **カードの紛失または盗難**——ユーザーがカードの紛失または盗難の届けをした場合は、便利なウェブ管理アプリケーションを使用して管理者はすぐにそのカードを無効にできます。これによって他人によるカードの使用を防ぎます。
- **セルフサービスパスワードリセット（SSPR）**——管理者が SSPR を有効にした場合、ユーザーは SSPR を登録すると、ヘルプデスクに電話することなくパスワードのリセットができます。

- **使いやすいウェブベースの管理ツール**——管理者は、ウェブベースの管理ツールを使用して、迅速かつ簡単に近接カードとユーザーの設定と管理ができます。

一元設定の設定

管理サーバ設定ダイアログボックスを使用して、ファイルサーバ、オプションの WDM サーバ設定、およびオプションのクラウドクライアントマネージャなど、シンクライアントの一元的な接続設定を設定します。

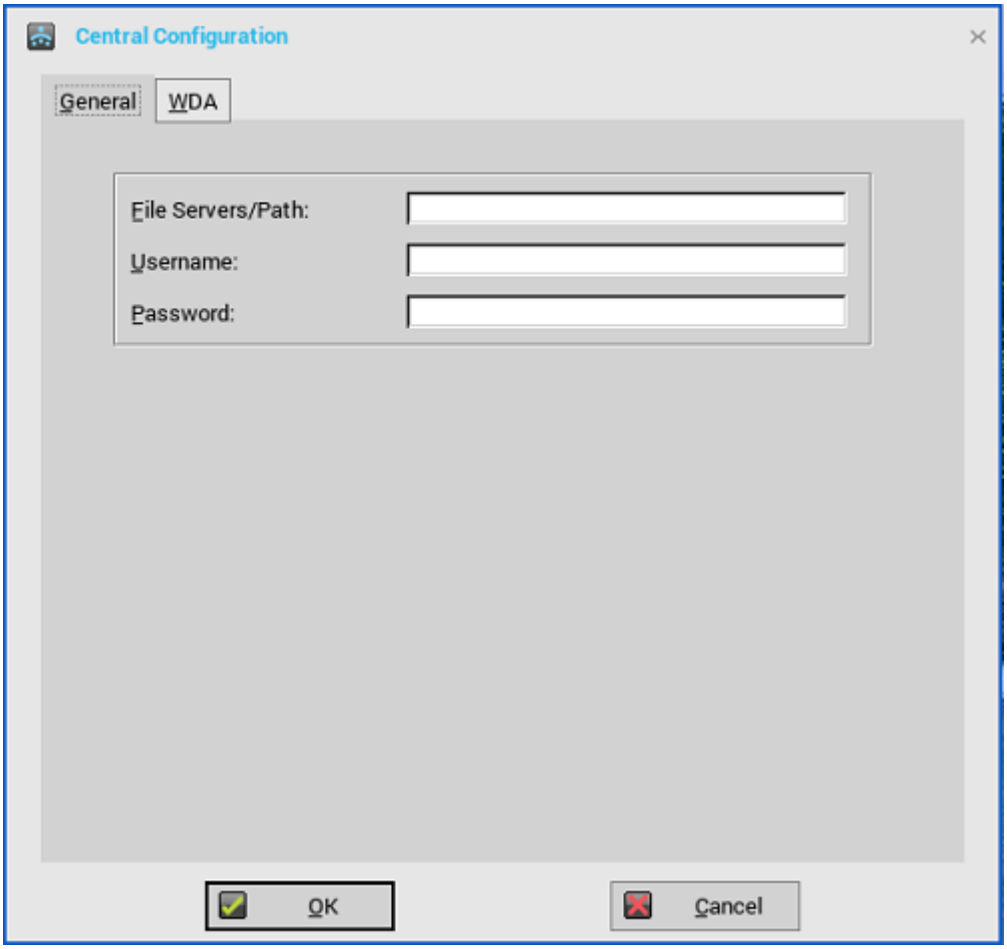
次のオプションを使用して、一元設定を設定します。

- 一般的な一元設定の設定
- WDA 設定の設定

一般的な一元設定の設定

一般的な一元設定を設定するには

1 デスクトップメニューで**システム設定**をクリックし、**管理サーバ設定**をクリックします。
管理サーバ設定ダイアログボックスが表示されます。
2 **全般**タブをクリックし、次のガイドラインに従います。



FTP サーバ/パス、**ユーザ名**および**パスワード**——システムソフトウェアイメージとアップデートイメージを提供するファイルサーバの IP アドレスまたはホスト名を入力します。DHCP を使用している場合は、アドレスは DHCP を介して提供できます。

a **FTP サーバ/パス**——ファイルサーバには最大 127 文字、ルートパスには最大 127 文字を使用できます。このデータによって、サーバにアクセスするときに使用するパスの一部を指定します。すべてのデータが長さの制限に収まる限り、複数のファイルサーバ／パスを指定できます。

b **ユーザ名**——ファイルサーバにログインするユーザー名を入力します。最大 31 文字を使用できます。

c **パスワード**——ファイルサーバにログインするパスワードを入力します。最大 31 文字を使用できます。

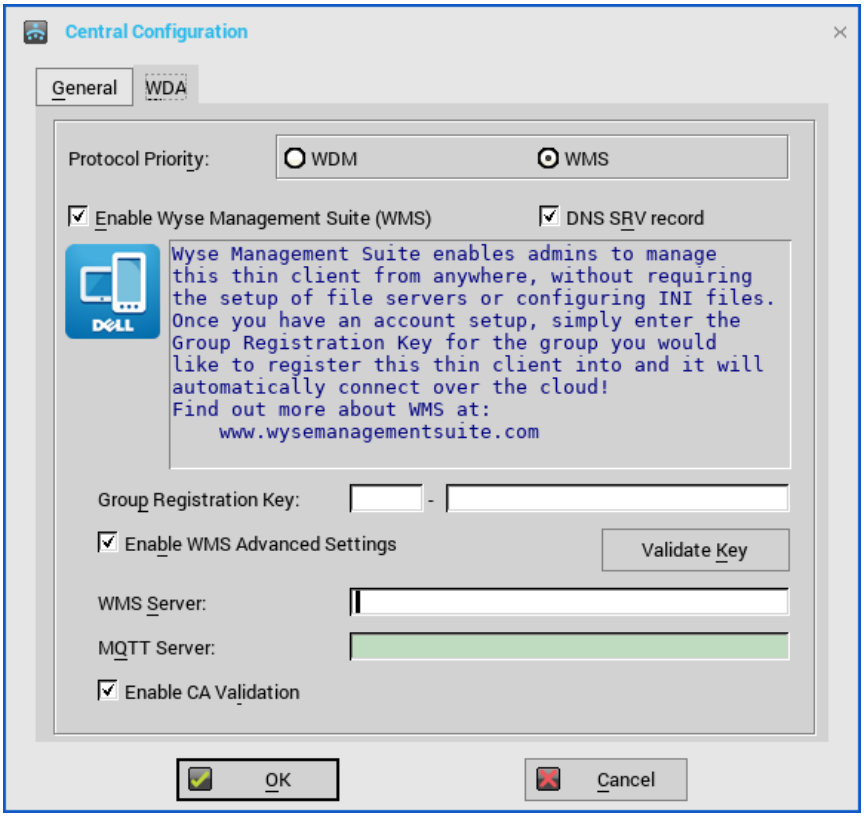
3 **OK** をクリックして設定を保存します。

Wyse Device Agent 設定の設定

このタブを使用して、Wyse Device Manager と Wyse Management Suite の設定を行います。
ThinOS は、すべての Wyse Management Suite Group Policy 設定をサポートしています。Wyse Management Suite 設定を行うには、次の操作を行います。

1 デスクトップメニューで**システム設定**をクリックし、**管理サーバ設定**をクリックします。
管理サーバ設定ダイアログボックスが表示されます。

2 **WDA > WMS** をクリックし、以下のガイドラインに従います。



デフォルトでは、**WMS** オプションが選択されています。クライアントが起動された後、Wyse Management Suite サービスが自動的に実行されます。
最初の検出で、たとえば Wyse Management Suite サービスがエラーになった場合、次の優先順位、たとえば WDM サービスを検索します。検出が成功するまでこれを継続します。すべての検出がエラーになった場合、一定時間（24 時間）経過後に自動的に再開します。

a **Wyse Management Suite（WMS）で端末を管理**——チェックボックスをオンにして Wyse Management Suite がシンクライアントを検出できるようにします。

b **DNS SRV レコード**——シンクライアントに、DNS サーバから Wyse Management Suite の値を取得させ、Wyse Management Suite サーバへの登録を試行させる場合、このチェックボックスをオンにします。デフォルトではチェックボックスはオンになっています。チェックボックスの選択が取り消された場合、シンクライアントは DNS サーバから Wyse Management Suite の値を取得できません。

DNS サーバに DNS レコードを作成するには、次の情報を使います。

WMS サーバの URL

DNS レコードタイプ：DNS SRV

レコード名：_WMS_MGMT._TCP.<Domain>

戻り値：WDMNG サーバの URL

例：_WMS_MGMT._TCP.WDADEV.com

MQTT サーバの URL

DNS レコードタイプ：DNS SRV

レコード名：_WMS_MQTT._TCP.<Domain>

戻り値：WMS サーバの URL

例：_WMS_MQTT._TCP.WDADEV.com

グループトークン

DNS レコードタイプ：DNS Text

レコード名：_WMS_GROUPTOKEN.<Domain>

戻り値：グループトークン（文字列）

例：_WMS_GROUPTOKEN .WDADEV.com

CA Validation

DNS レコードタイプ：DNS Text

レコード名：_WMS_CAVALIDATION.<Domain>

戻り値：TRUE または FALSE（文字列）

例：_WMS_CAVALIDATION.WDADEV.com

c **グループ登録キー**——Wyse Management Suite 管理者が目的のグループに対して設定したとおりに、**グループ登録キー**を入力します。キーを検証するには**キーの検証**をクリックします。
グループ登録キーは、プライベートの Wyse Management Suite サーバには必要ありません。Wyse Management Suite サーバの詳細情報を入力すると、デバイスを Wyse Management Suite に登録できます。ThinOS は、Wyse Management Suite の隔離テナントに登録します。

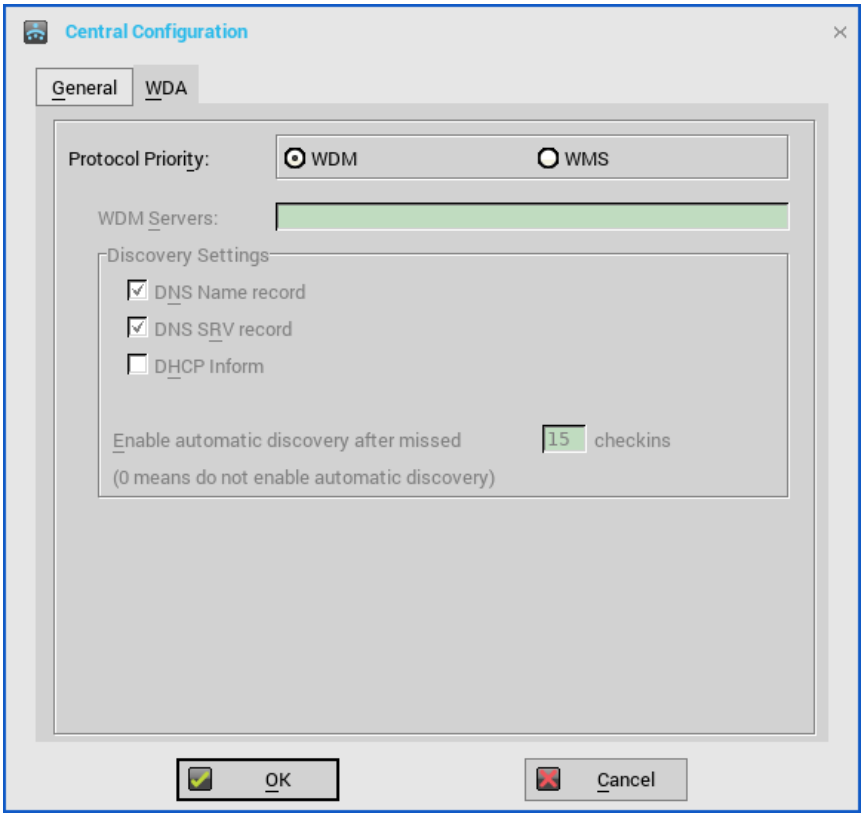
d **WMS 詳細設定の有効化**——このチェックボックスをオンにして、Wyse Management Suite サーバ、MQTT サーバの詳細情報を入力し、CA 検証を有効化します。MQTT サーバオプションは、デフォルトでは無効です。MQTT サーバ値は、ThinOS が Wyse Management Suite に登録されてから追加されます。

メモ：Wyse Management Suite を有効にする場合は、グループ登録キーが入力済みで、Wyse Management Suite の詳細設定が設定済みであることを確認します。

Wyse Management Suite を使用した ThinOS デバイスの管理についての詳細は、www.dell.com/manuals の『Wyse Management Suite バージョン 1.1 管理者ガイド』を参照してください。

3 **OK** をクリックして設定を保存します。

ステータスチェック済みのサービスが、**システム情報**タブに表示されます。
WDM 設定を行うには、次の操作を実施します。



1 **WDM** をクリックして、以下のガイドラインに従います。
2 **WDM サーバ**——WDM を使用する場合、IP アドレスまたはホスト名を入力します。ユーザーの INI プロファイルを使用する場合、場所もユーザープロファイルから指定できます。
3 **DNS ホスト名レコード**——（動的検出）デバイスは DNS ホスト名ルックアップ方式を使用して、WDM サーバを検出します。
4 **DHCP オプションタグ**——（動的検出）デバイスは DHCP Inform を使用して、WDM サーバを検出します。
5 **Check-in 失敗後の自動検出を有効化**——何回チェックインが行われなかったら、自動検出を有効にするのかを選択します。
6 **OK** をクリックして設定を保存します。

Wyse Device Manager オプションは、次の INI パラメータを使用して無効にできます。

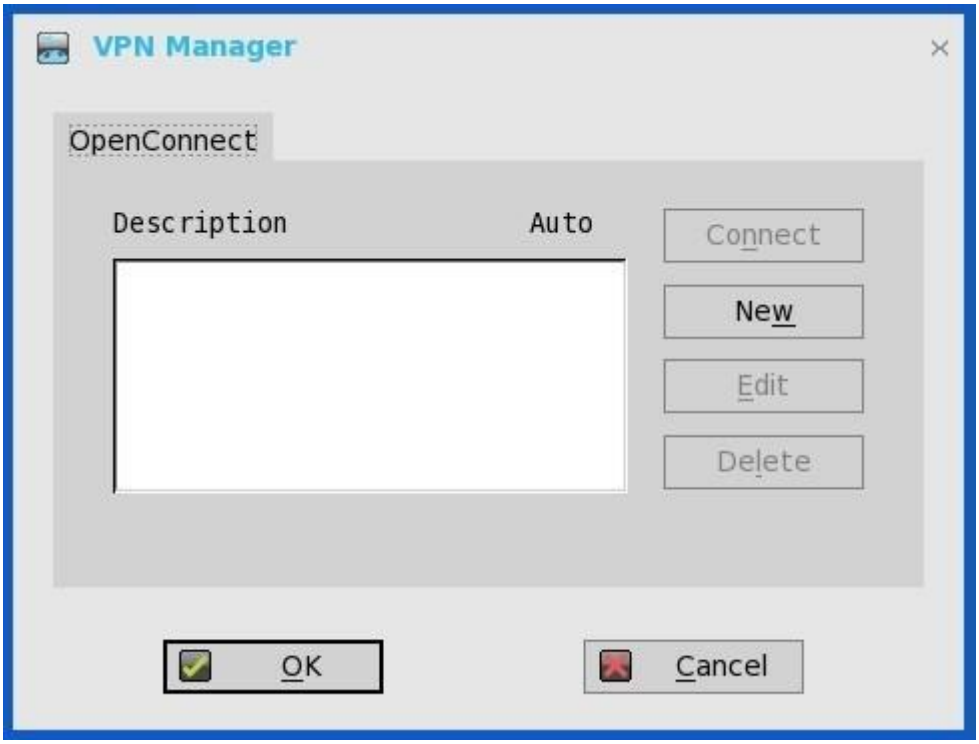
- WMSService=no
- Service=wdm disable=yes
- RapportDisable=yes

VPN マネージャの設定

VPN マネージャ（VPN Manager）は、VPN 接続を管理するために含まれています。仮想プライベートネットワーク（VPN）により、プライベートネットワークをインターネットなどのパブリックネットワーク上に拡張できます。これにより、デバイスが直接プライベートネットワークに接続されているかのように、コンピュータや Wi-Fi 対応デバイスが共有ネットワークまたはパブリックネットワーク上でデータを送受信できます。その際、プライベートネットワークの機能、セキュリティおよび管理ポリシーの利点を活用することができます。

VPN マネージャを設定するには、次のガイドラインに従います。

1 クラシックモードでは、デスクトップメニューで、**システム設定 > WAN 設定**をクリックします。
ゼロモードでは、システム設定パネルに **WAN 設定**タブが表示されます。
2 **WAN 設定**をクリックします。
WAN 設定ダイアログボックスが表示されます。



3 **新規**をクリックして、新しいセッションを作成します。

a セッション名（最大 21 文字）——セッション名を入力します。これは、必須のオプションではありません。フィールドが空白のままの場合は、VPN サーバ名がセッション名として使用されます。

b VPN サーバ（最大 63 文字）——VPN サーバの IP アドレスを入力します。これは、IP アドレスまたはホスト名のいずれかとして定義されます。これは、必須のオプションです。

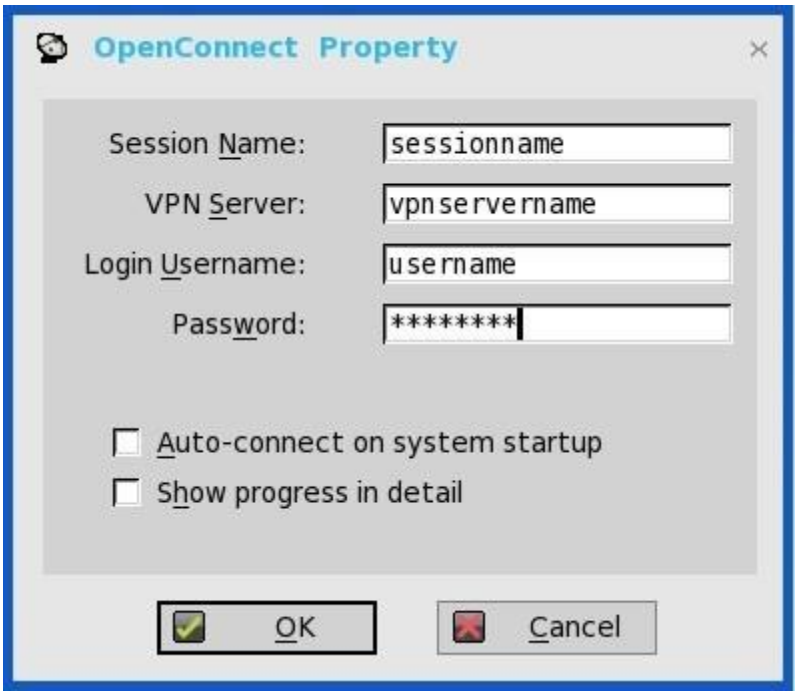
c VPN ユーザ名（最大 31 文字）——ログインユーザー名を入力します。これは、必須のオプションです。

d パスワード（最大 31 文字）——ユーザーのパスワードを入力します。これは、必須のオプションではありません。

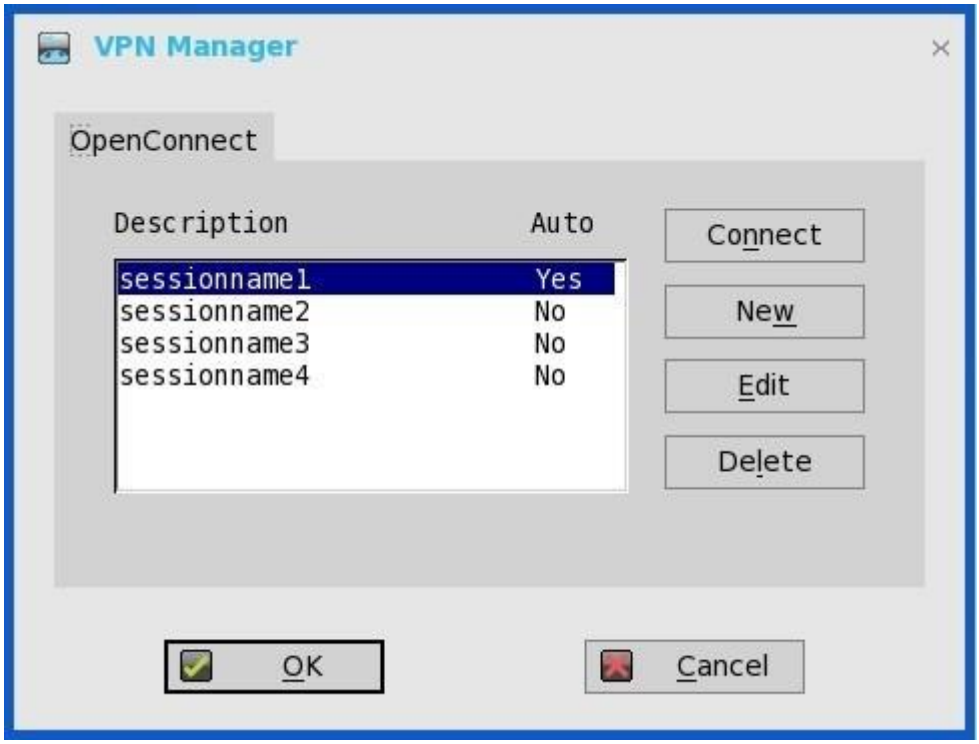
e システムのスタートアップ時に自動接続するチェックボックスをオンにします。

f 進行状況を詳細に表示するチェックボックスをオンにします。

g **OK** をクリックします。



接続が作成されると、Description 列にセッション名が表示され、Auto 列にはユニットのリスタート時に自動接続される接続が示されます。1 つのセッションのみ、自動接続するよう設定できます。



4 **接続**をクリックします。
接続ステータスが表示されます。

コネクションブローカーの設定

Virtual Desktop Infrastructure（VDI）環境では、コネクションブローカーは、ユーザーが使用可能なデスクトップに接続することを許可するソフトウェアエンティティです。コネクションブローカーによって、集中管理されたデスクトップ環境を安全かつ効率的に管理できる VDI 環境が促進されます。

メモ：

- Citrix、VMware、Dell vWorkspace のブローカーで、Linux ホストのデスクトップがサポートされています。
- 複数のブローカーで Windows 10 デスクトップはサポートされています。
  - Windows 10 は、Citrix、VMware、RDS ブローカーでサポートされています。
  - Microsoft RDS から公開された Windows 10 リモートデスクトップは、MMR をサポートしません。VMware Horizon と Citrix Xen から公開された Windows 10 リモートデスクトップは、MMR をサポートしています。
- ICA マルチキャスト機能は、ThinOS 8.4 以降はサポートされていません。ただし、URL のリダイレクトは正常に動作します。

Citrix の設定

Citrix は完全な仮想化ソリューションを提供しており、すべてのアプリケーションとリソースは一元化されたサーバに導入され、リモートデバイスに公開されます。シンクライアントにインストールされた Citrix Receiver クライアントソフトウェアで、ユーザーはアプリケーションの GUI と情報交換できますが、すべてのアプリケーションプロセスは、サーバで実行されます。

このセクションでは、Citrix ブローカー接続を ThinOS デバイスに設定する方法と、ThinOS に設定できるその他の Citrix の機能について説明します。

Citrix ブローカー接続の設定

Citrix ブローカーコネクションを設定するには：

1. デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。
   リモート接続設定ダイアログボックスが表示されます。
2. **ブローカー**タブでは、ドロップダウンリストで Citrix Xen を選択し、次の操作を行います。
   - チェックボックスをオンにし、**StoreFront UI の有効化**を選択します。
   - **ブローカーサーバ**——ブローカーサーバの IP アドレス／ホスト名／FQDN を入力します。
   - **自動接続リスト**——個別のブローカーにログイン後、自動的に起動させたいデスクトップの名前を入力します。複数のデスクトップの入力が可能です。各デスクトップの名前はセミコロンで区切り、大文字と小文字は区別します。
   - チェックボックスをオンにし、ログオン時の自動再接続を有効にします。

     メモ：自動再接続を有効にすると、再接続オプションから選択できます。切断したセッションにのみ接続できるオプション、またはアクティブなセッションと切断したセッションの両方に接続できるオプションのいずれかをクリックします。
   - チェックボックスをオンにし、ボタンメニューで自動再接続を有効にします。

     メモ：自動再接続を有効にすると、再接続オプションから選択できます。切断したセッションにのみ接続できるオプション、またはアクティブなセッションと切断したセッションの両方に接続できるオプションのいずれかをクリックします。
   - **アカウントセルフサービス**——アカウントセルフサービスサーバの IP アドレスを入力します。
   - **XenApp**——デフォルト設定を **XenApp** に設定する場合に、このオプションを使用します。
   - **XenDesktop**——デフォルト設定を **XenDesktop** に設定する場合に、このオプションを使用します。
3. **OK** をクリックして設定を保存します。

Citrix HDX の RealTime Multimedia Engine または RealTime Optimization Pack

HDX RealTime Optimization Pack（RTOP）では、Microsoft Skype for Business を使用して、オーディオビデオ会議と Voice over Internet Protocol（VoIP）企業テレコミュニケーションを実現するスケーラブルなソリューションを提供します。Optimization Pack は、ThinOS デバイスのユーザーの XenDesktop と XenApp 環境をサポートします。HDX RealTime Optimization Pack の詳細については、Citrix ドキュメントを参照してください。

このセクションでは、RealTime Multimedia Engine（RTME）のサポート対象プラットフォーム、RTME パッケージのインストール、Citrix リモートサーバ／デスクトップホストの準備、ThinOS での設定、RTME ステータスチェック、およびトラブルシューティングについて情報を提供します。

はじめに

Citrix HDX RealTime Optimization パックでは、ハイ・デフィニション・オーディオおよびビデオ通話を提供しています。ThinOS がリリースされるたびに、RTME のバージョンは最新バージョンにアップデートされる可能性があり、最新の RTME バージョンは、対応するリリースパッケージの RTME 1.8 バージョンと共存します。ThinOS 8.5 HF は RTME バージョン 2.4 をサポートします。

Citrix RTME 1.8 の機能の詳細については、docs.citrix.com の HDX RealTime Optimization Pack の記事を参照してください。

Citrix RTME 2.x の機能の詳細については、docs.citrix.com の最新の RealTime Optimization Pack の記事を参照してください。

サポート対象環境

- Citrix 環境：XenDesktop および XenApp 5.6/6.5/7.x
- RTME コネクタ 1.8 を備えたデスクトップ（Lync サーバおよびクライアントのバージョン 2010 と 2013、Lync 2013 GUI の Skype for Business クライアントをサポート）
- RTME コネクタ 2.x を備えたデスクトップ（Skype for Business 2015 と Skype for Business 2016 の両方をサポート）
- サポート対象のネットワーク：LAN、WAN（VPN）、ワイヤレスなど
- RTME クライアント間、または RTME クライアントと標準の Lync クライアント間の呼び出しをサポート
- Microsoft Office 365 または Skype for Business Online をサポート詳細については、Citrix ドキュメントを参照してください。

RTME サポート対象プラットフォーム

- Wyse 5010 シンクライアント（ThinOS 搭載）（D10D）、Wyse 5010 シンクライアント（PCoIP 対応）（D10DP）
- Wyse 3030 LT シンクライアント（ThinOS 搭載）、Wyse 3030 LT シンクライアント（PCoIP 対応）
- Wyse 3040 シンクライアント（ThinOS 搭載）、Wyse 3040 シンクライアント（PCoIP 対応）
- Wyse 5060 シンクライアント（ThinOS 搭載）、Wyse 5060 シンクライアント（PCoIP 対応）
- Wyse 5040 AIO シンクライアント（ThinOS 搭載）（5212 AIO）、Wyse 5040 AIO シンクライアント（PCoIP 対応）（5213）
- Wyse 7010 シンクライアント（ThinOS 搭載）（Z10D）

ThinOS での RTME パッケージのインストール

RTME の機能が ThinOS で動作するためには、RTME.i386 パッケージをインストールする必要があります。

RTME.i386 パッケージをインストールするには

1 **RTME.i386.pkg** を¥wnos¥pkg¥ディレクトリにアップロードします。

> **メモ：最新の RTME パッケージのバージョンについては、最新の『Dell Wyse ThinOS リリースノート』を参照してください。**

2 INI の autoload が 0 に設定されていないことを確認する必要があります。
3 シンクライアントをリスタートし、パッケージの自動インストールが完了するまで待機します。
インストールされた RTME パッケージは、システムツールの**パッケージ**ウィンドウに表示されます。

RealTime Multimedia Engine コネクタのセットアップ

このセクションでは、Citrix デスクトップでの Lync または Skype for Business（SFB）のインストールおよび使用方法について説明します。

1 Citrix デスクトップ VDA／サーバに Citrix HDX RealTime Connector をインストールします。HDX RealTime Multimedia Engine（RTME）は、ThinOS にインストールされたパッケージです。HDX RealTime Connector は、リモートサーバと VDA にインストールするか、アップグレードする必要があります。

> **メモ：以下は、RTME 1.8 にのみ適用できます。**
> - 1.7 から 1.8 へのアップグレードオプションについては、docs.citrix.com/en-us/hdx-optimization/1-8/upgrade-1-7-to-1-8.html で説明しています。
> - リモートサーバと VDA 上でファイアウォールの設定が必要です。詳細については、docs.citrix.com/en-us/hdx-optimization/1-8/hdx-realtime-optimization-pack-configure-fire wall.html を参照してください。
> - Citrix の制限により、ThinOS 上の RTME 1.8 の機能は、HDX RealTime Connector 1.8 のみをサポートします。

2 ThinOS ファームウェアをアップデートし、ThinOS クライアントに **RTME.i386.pkg** をインストールします。

> **重要:ThinOS 8.3.1 HF リリース以降、RTME 1.8 および 2.1 がリリースパッケージに共存しており、RTME コネクタの両方のバージョンをサポートしています。ThinOS がリリースされるたびに、RTME は最新バージョンにアップデートされる可能性があり、最新の RTME バージョンは、対応するリリースパッケージの RTME 1.8 バージョンと共存します。**

3 （このステップは RTME 1.8 のみ）Lync Server の ThinOS でドメインネームサーバ（DNS）設定を設定します。

> **メモ：RTME が正しく動作するには、シンクライアントでビデオ／オーディオデバイスの USB リダイレクトが使用できないことを確認する必要があります。**

4 Citrix Desktop にログインし、Lync クライアントまたは Skype for Business（SFB）クライアントにサインインします。
- RTME 1.8 の場合は、RTME アイコンが、Lync クライアントウィンドウの左下隅に表示されます。
- RTME 2.x の場合は、RTME アイコンがタスクバーに表示されます。

Lync アプリケーションまたは Skype for Business アプリケーションを使用して、次のタスクを実行します。

- 音声通話またはビデオ通話の開始
  - 通話先のユーザーの選択
  - IM ウィンドウからの通話
  - 通話先の名前または番号の入力
- 通話への応答
  - 音声通話
  - ビデオ通話
  - 通話に応答するヘッドセットのボタン
- 通話の転送／ミュート／通話の保留
- ビデオの制御：一時停止／終了／ピクチャインピクチャ（PiP）
- ボリュームレベルの設定
- ダイヤルパッドの使用
- 会議通話の開始
- ヘルプと通話の終了
- ビデオ通話ウィンドウの最小化／最大化、または終了
- ネットワークヘルスチェックの実行:
  - RTME 1.8 の場合は、**Ctrl + N** を押して、**Network Health** ウィンドウを開きます。
  - RTME 2.x の場合は、タスクバーの RTME アイコンを右クリックし、**Call Statistics** を選択します。

受信パケット、送信パケット、ビデオフレームレート、ビデオ解像度、オーディオコーデック、ビデオコーデックなどの属性が上記ウィンドウに表示されます。

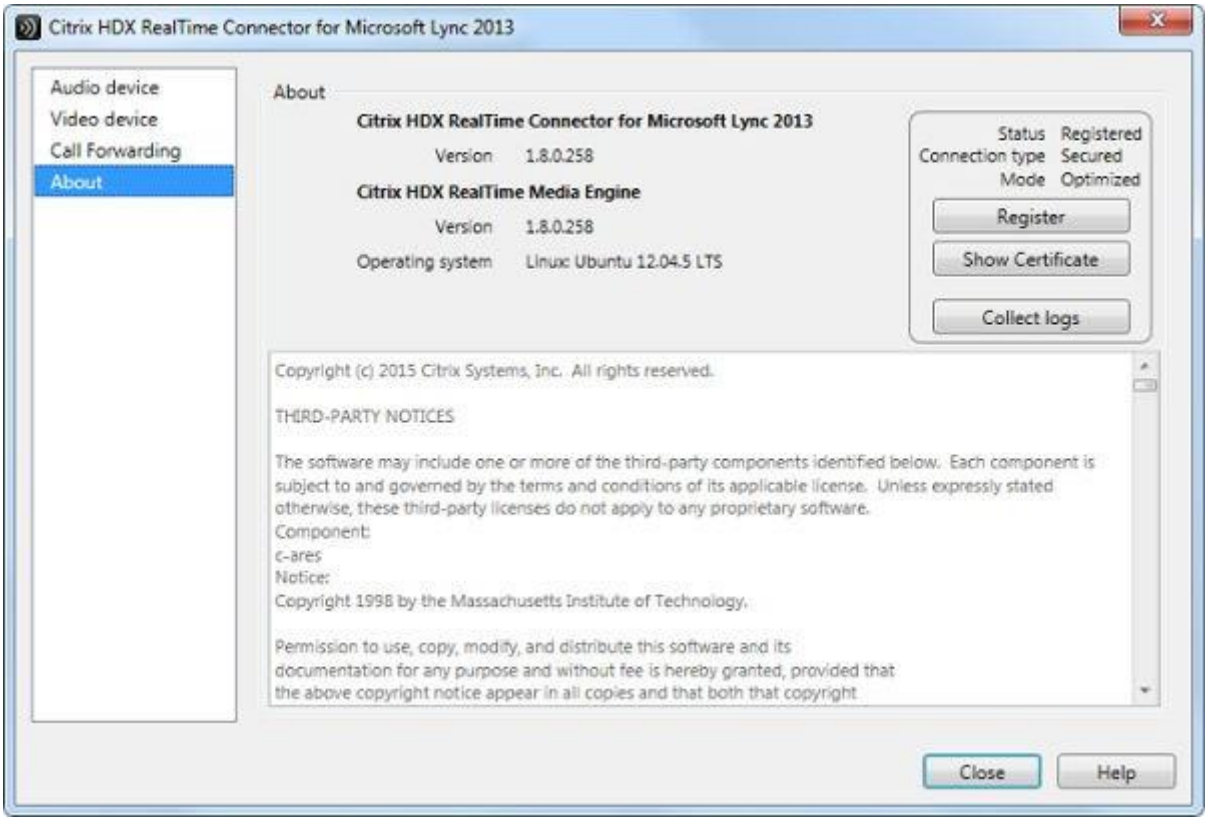
RTME 1.8 ステータスの確認

Citrix HDX RealTime Connector for Microsoft Lync 2013 ダイアログボックスでは、RTME 1.8 ステータスを確認できます。
Citrix HDX RealTime Connector for Microsoft Lync 2013 ダイアログボックスを表示するには：

1 **Citrix HDX RealTime Connector for Microsoft Lync 2013** ダイアログボックスを表示するには、次のいずれかを実行します。

- Lync アプリケーションウィンドウの左下隅にある **RTME** アイコンをクリックし、**Audio Video Settings** をクリックします。
- Lync アプリケーションウィンドウの右上隅にある **Lync menu** アイコンをクリックし、**Tools > Audio Video Settings** をクリックします。

Citrix HDX RealTime Connector for Microsoft Lync 2013 ダイアログボックスが表示されます。



2 **Citrix HDX RealTime Connector for Microsoft Lync 2013** ダイアログボックスの **About** タブをクリックします。
RTME ステータスが、ダイアログボックスの右上のペインに表示されます。RealTime Multimedia Engine が ThinOS クライアントと Citrix Desktop 間で正常に開始されると、RTME ステータスは次のように表示されます。

表 6. RTME ステータス

属性	値
Status	Registered
Connection Type	Secured
Mode	Optimized

Citrix HDX RealTime Connector for Microsoft Lync 2013 のバージョンと **Citrix HDX RealTime Media Engine** のバージョンもダイアログボックスに表示できます。

3 **Audio Device** タブをクリックし、スピーカ、マイク、着信音の設定など、RTME のオーディオ設定を設定します。

ⓘ **メモ：ThinOS 上の RTME オーディオデバイスには、ThinOS のローカルの再生デバイスから 1 つのデバイスのみ表示されます。この RTME オーディオデバイスは、ThinOS のローカルの再生デバイスおよび録音デバイスで設定されたとおりに実際に動作できます。着信音の RTME オーディオデバイスは、ThinOS のローカルの再生デバイスのみ使用できます。これは既知の問題です。**

4 **Video Device** タブをクリックし、RTME ビデオ設定を設定します。ドロップダウンリストから、ビデオ通話に使用する Web カメラを選択します。

5 **Call Forwarding** タブをクリックし、通話転送設定を設定します。
次のオプションを設定できます。

- 通話転送のオフ
- すべての通話を特定の番号に転送
- 同時呼び出し

ⓘ **メモ：一番新しく設定した通話転送設定がダイアログボックスの下のペインに表示されます。**

トラブルシューティングの詳細については、docs.citrix.com/en-us/hdx-optimization/1-8/hdx-realtime-optimization-pack-troubleshooting.html を参照してください。

RTME 1.8 の機能に関する既知の問題

- ThinOS 上の RTME オペレーティングシステムが Linux と表示されます。
- Citrix の既知の制限により、ThinOS 上の RTME 1.8 の機能が、他のバーションの HDX RealTime コネクタと連携しません。
- RTME 通話の間にオーディオデバイスを変更すると音声入力または出力が反応しなくなる可能性があります。
- ビデオ会議の通話では、別のユーザーが話をしていると、画面上のビデオは話をしているユーザーに切り替わりますが、切り替えに数秒かかります。

試験済みデバイス——RTME の試験済みデバイスの詳細については、最新の『Dell Wyse ThinOS リリースノート』を参照してください。

RTME 2.x ステータスの確認

このセクションでは、RTME 2.x の機能と RTME ステータスの検証方法について説明します。

特徴

- Skype For Business のネイティブクライアントのメニューと操作が利用できます。
- 初期化の改善によって DNS の混乱がなくなります。
- コールデリゲーション、応答グループなどさらに多くの通話機能をサポートします。
- RTME 2.1 で導入されたビデオコーデック H.264-UC およびオーディオコーデック SILK をサポートします。
- 呼受付制御のサポート
- 帯域幅ポリシー管理
- DSCP／QoS 設定
- RealTime Connector と RealTime Media Engine の組み合わせが許容範囲である場合に、バージョン不一致への警告を消す機能。

RTME ステータスを検証するには、次の操作を行います。

1 リモートデスクトップに適切なコネクタをインストールします。
2 ThinOS デバイスに適切なパッケージをインストールします。
3 オーディオ／ビデオデバイスに接続します。

ⓘ **メモ：USB リダイレクトはオーディオ／ビデオデバイスに対しては無効にする必要があります。**

4 SFB クライアントを使用してリモートデスクトップに接続します。
5 タスクバーの RTME connector アイコンを確認します。ステータスが **Connected** と表示されます。
6 RTME connector メニューで **About and Settings** オプションを確認します。
7 SFB client メニューでオーディオ／ビデオデバイスを確認します。
8 ビデオ通話または音声通話を開始します。
9 マウスをクリックするか、ヘッドセットのボタンを使って電話に出ます。

10　RTME connector メニューでコール統計（Call Statistics）を確認します。

メモ：RTME 2.2 以降のバージョンでは、さまざまな通話シナリオをサポートします。詳細については、「Citrix ドキュメント」を参照してください。

RTME 2.2 以降のバージョンでは、UVC（USB Video Class）1.1 および 1.5 のカメラのハードウェアエンコーディング／H.264（CAM）がサポートされています。これは限定されたカメラ（Logitech C930e など）にのみ適用されます。

Call Statistics ウィンドウでは、**Sent** カラムの P2P RTME ビデオ通話に対して、**Video Codec = H.264-UC (CAM)**が表示されます。標準の SFB でのグループ通話の場合は、コール統計により **Sent** カラムに、**Video Codec = H.264-UC (CAM)**が表示されます。これによって、Video Codec H.264 (SW)と比べて、ビデオ通話品質／解像度が向上します。たとえば、P2P のビデオ通話の解像度は、480 x 270 から 640 x 360 に上がっています。

既知の問題と制限

- 通話でクライアントから送られるビデオは、通話中の双方機器の性能に左右されます。一方のクライアントから送るビデオの画質が良ければ、通話の相手よりも性能が高いということではありません。
- RTME status ダイアログは、オペレーションシステムを Linux と表示します。
- RTME 通話中にビデオまたはオーディオのデバイスを変更すると、入力または出力で問題が発生します。
- ボリューム：デルは SFB クライアントのオーディオ設定のスピーカのボリュームを、「高」に調整することをお勧めします。SFB クライアントのオーディオのボリュームは、デフォルトでは 40%に設定されています。デフォルトのボリュームは低めです。
- カメラ／ビデオ：RTME の設計で考慮されているため、ローカルカメラの設定が、RTME のビデオ出力に作用したり、影響したりすることはありません。
- Citrix RTME バージョン 2.3 では、アプリケーションのビデオ性能は、CPU の消費を抑えるように設計されています。このため、ビデオの解像度が、バージョン 2.2 と比べると落ちる可能性があります。

Citrix アイコンリフレッシュ

Citrix アプリケーションは、**PNMenu** で **Refresh** をクリックするとリフレッシュされます。

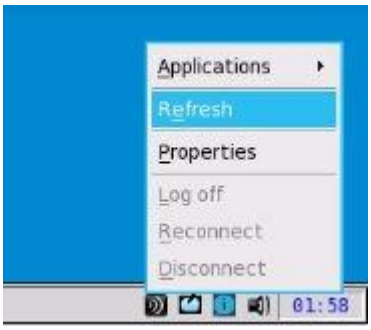
Citrix アプリケーションをリフレッシュする方法は、次の 2 つです。

- 手動リフレッシュ
- INI パラメータを使用した自動リフレッシュ

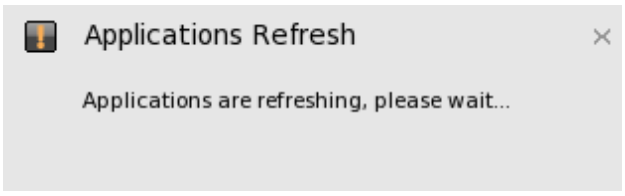
Citrix アプリケーションの手動リフレッシュ

Citrix アプリケーションを手動でリフレッシュするには、次の操作を行います。

1 単独の StoreFront または PNAgent サーバの場合、ブローカーでアプリケーションを変更し、**PNMenu** で**リフレッシュ**をクリックします。



アプリケーションのリフレッシュ中は、次のメッセージが右下のペインに表示されます。

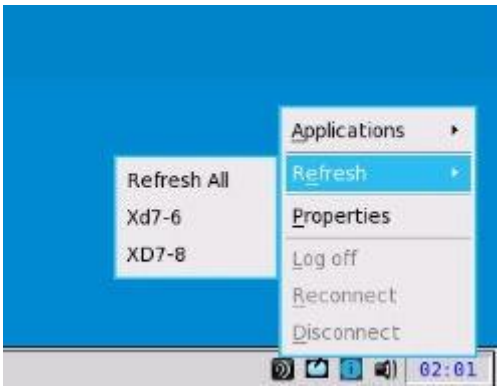


2 セッションバーリスト、接続マネージャリスト、App メニューリストで、アプリケーションがリフレッシュされます。

イベントログウィンドウに次のログが表示されます。

ICA: refresh store “xxx”…” or “ICA: refresh PNAgent”xxx”…

3 マルチファーム（StoreFront または PNAgent サーバ）またはマルチログオン（StoreFront または PNAgent サーバ）の場合、リフレッシュするサーバを 1 つ選択するか、**すべてをリフレッシュ**をクリックしてすべてのサーバをリフレッシュします。



メモ：

アプリケーションをリフレッシュするとき、アプリケーションをオープンまたは編集または削除すると、警告メッセージが表示されます。

4 リフレッシュの範囲には、アプリケーションの削除、追加、複製、無効化、有効化、アイコン／タイトルの変更、デスクトップのオン／オフなどの局面も含まれます。

開始したアクティブなセッションは、アプリケーションのリフレッシュの影響を受けません。

5 リモート接続で**ログイン時に自動再接続を有効にする**が有効になっている場合、アプリケーションのリフレッシュ後に、切断されたセッションの再接続ができます。

INI パラメータを使用した Citrix アプリケーションの自動リフレッシュ

Citrix アプリケーションを自動的にリフレッシュするには、次の INI パラメータを設定します。

SessionConfig=ICA RefreshTimeOut=dd:hh:mm

たとえば、01:01:22 とは、1 日：1 時間：22 分毎に、アプリケーションが自動的にリフレッシュを開始するという意味です。

Citrix アイコンリフレッシュの制限

Citrix アイコンリフレッシュの制限は次のとおりです。

- Citrix アイコンリフレッシュは、クラシックモードと storefront モードのみでサポートされます。
- Virtual Desktop Infrastructure（VDI）モードはサポートされません。

Citrix セッションでのマルチオーディオの使用

ThinOS では、XenDesktop または XenApp バージョン 7.6 以降で、マルチオーディオデバイスの利用をサポートします。セッション中はいつでもオーディオデバイスを接続／切断できますが、動作はローカルデスクトップと同様です。マルチデバイスのサポートで、複数のオーディオデバイスを接続し、特定のアプリケーションに特定のデバイスを選択できます。

Audio Plug N Play ポリシーを、Citrix Remote Desktop Session（RDS）デスクトップで有効にする必要があります。**Audio Plug N Play** ポリシー設定によって、音の録音と再生を行うマルチオーディオデバイスの使用が許可または抑止されます。デフォルトではこの設定は有効です。

メモ：Citrix Virtual Desktop Infrastructure（VDI）デスクトップでは、事前設定は必要ありません。

サポートされるデバイス——USB ヘッドセット、Web カメラ（USB リダイレクトなし）、およびアナログヘッドセットデバイスはサポートされます。

マルチオーディオの有効な動作条件は次のとおりです。

- Citrix HDX の市販のオーディオを使用
  a オーディオデバイスは、**PC Mic and Speaker** を選択します。
  b スピーカまたはマイクを設定します。
  c セカンダリリンガーの場合は、すでに選択済みのデバイスを除いたオーディオデバイスを選択します。
- Citrix RealTime Multimedia Engine（RTME）を使用
  a オーディオデバイスは、**HID headset with PC Mic and Speaker** を選択します。
  b **PC Mic and Speaker** を設定してスピーカまたはマイクを設定します。
  c セカンダリリンガーの場合は、すでに選択済みのデバイスを除いたオーディオデバイスを選択します。

マルチオーディオ設定中は、次のシナリオを考慮する必要があります。

- ThinOS のデフォルトのオーディオは、最新のプラグインオーディオデバイスに設定されています。
- セッションのデフォルトのオーディオは、ThinOS のデフォルトのオーディオに設定されています。ただし、この選択は変更可能です。
- デバイスのプラグを接続および取り外した後は、Skype for Business/Lync クライアントを再起動します。
- ICA RTP オーディオは、マルチオーディオ接続でサポートされています。
- 通話中、デバイスのプラグを抜き差しせず、オーディオデバイスの設定の切替が可能です。
- マルチオーディオは、セッション間で共有できます。

CensorNet MFA 認証での Citrix NetScaler の使用

SMS PASSCODE は、CensorNet MFA ブランドに変更されています。NetScaler Gateway を設定すると、One Time Passcode／Password（OTP）を個人識別番号（PIN）またはパスコードの形で使用できます。このワンタイムパスワードを取得するには、お使いのモバイルデバイスに CensorNet アプリをインストールする必要があります。パスコードまたは PIN を入力すると、認証サーバがワンタイムパスワードを無効にします。同じ PIN またはパスワードは二度と入力できません。ワンタイムパスコードの設定の詳細については、Citrix ドキュメントを参照してください。

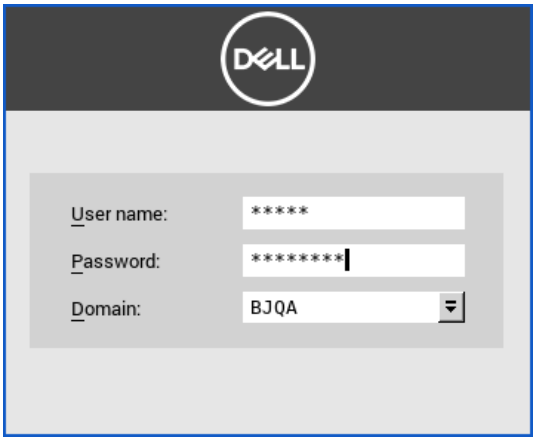
前提条件

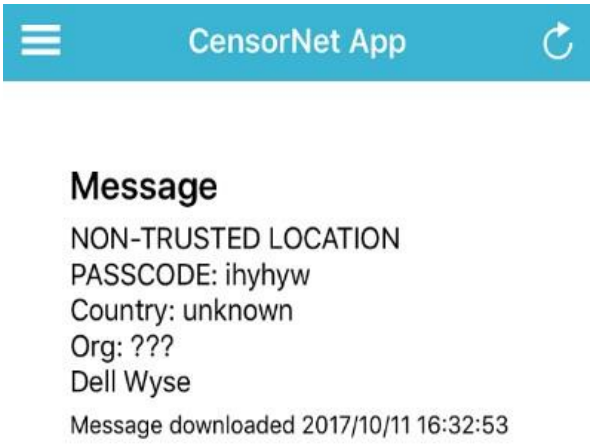
- NetScaler v12.0 以降がお使いのクライアントにインストールされています。
- SMS PASSCODE v9.0 SP1 がインストールされていて、ネットワークの設定がされています。SMS PASSCODE v9.0 のファイルは、download.smspasscode.com/public/6260/SmsPasscode-900sp1 からダウンロードできます。
- Remote Authentication Dial-In User Service（RADIUS）認証ポリシーが設定されていて、NetScaler ゲートウェイサーバに紐付けられています。
- CensorNet アプリがお使いのモバイルデバイスにインストールされ、設定されています。

ThinOS でワンタイムパスワード使用するには、次の操作を実行します。

1 ThinOS にログインし、NetScalar Gateway URL に接続します。
2 資格情報（ユーザーID とパスワード）を入力して Enter を押します。
PASSCODE ダイアログボックスが表示されます。モバイルデバイスの CensorNet App からプッシュ通知でコードを受信しま

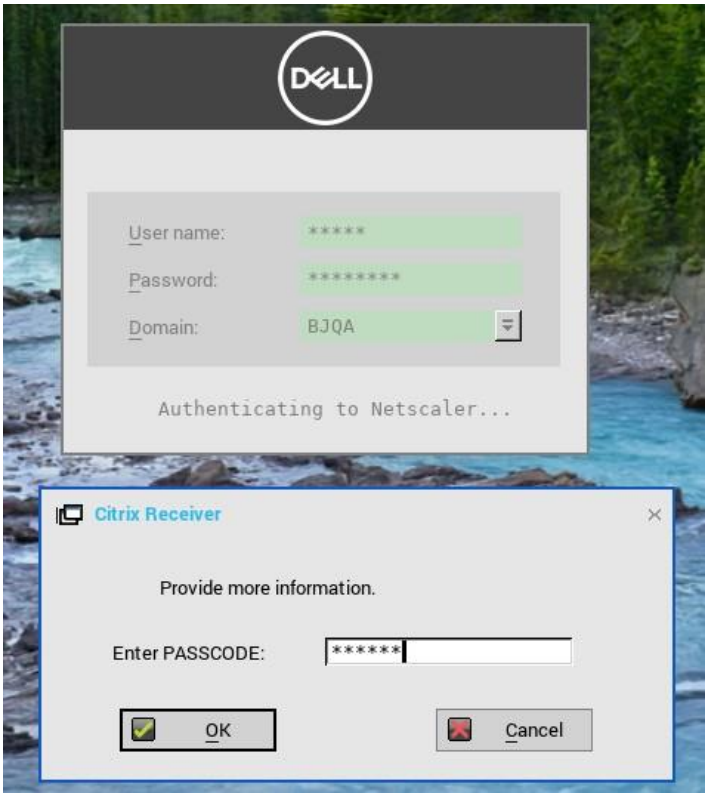
す。





3 **OK** をクリックします。

認証に成功したら、Citrix セッションにログインされます。



ICA 接続の設定

ICA 接続を設定するには：

1 デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。
リモート接続設定ダイアログボックスが表示されます。
2 **ブローカー**タブでは、ドロップダウンリストで**ブローカー選択**を**なし**と選択します。
3 **ICA** 接続プロトコルをクリックし、**接続設定の編集**をクリックします。
Default ICA ダイアログボックスが表示されます。

> **メモ：Default ICA は常に公開されたアプリケーションへの直接接続に使用され、StoreFront または PNAgent には使用されません。**

4 **接続**タブをクリックします。
ICA 接続を設定するには、次の操作を行います。

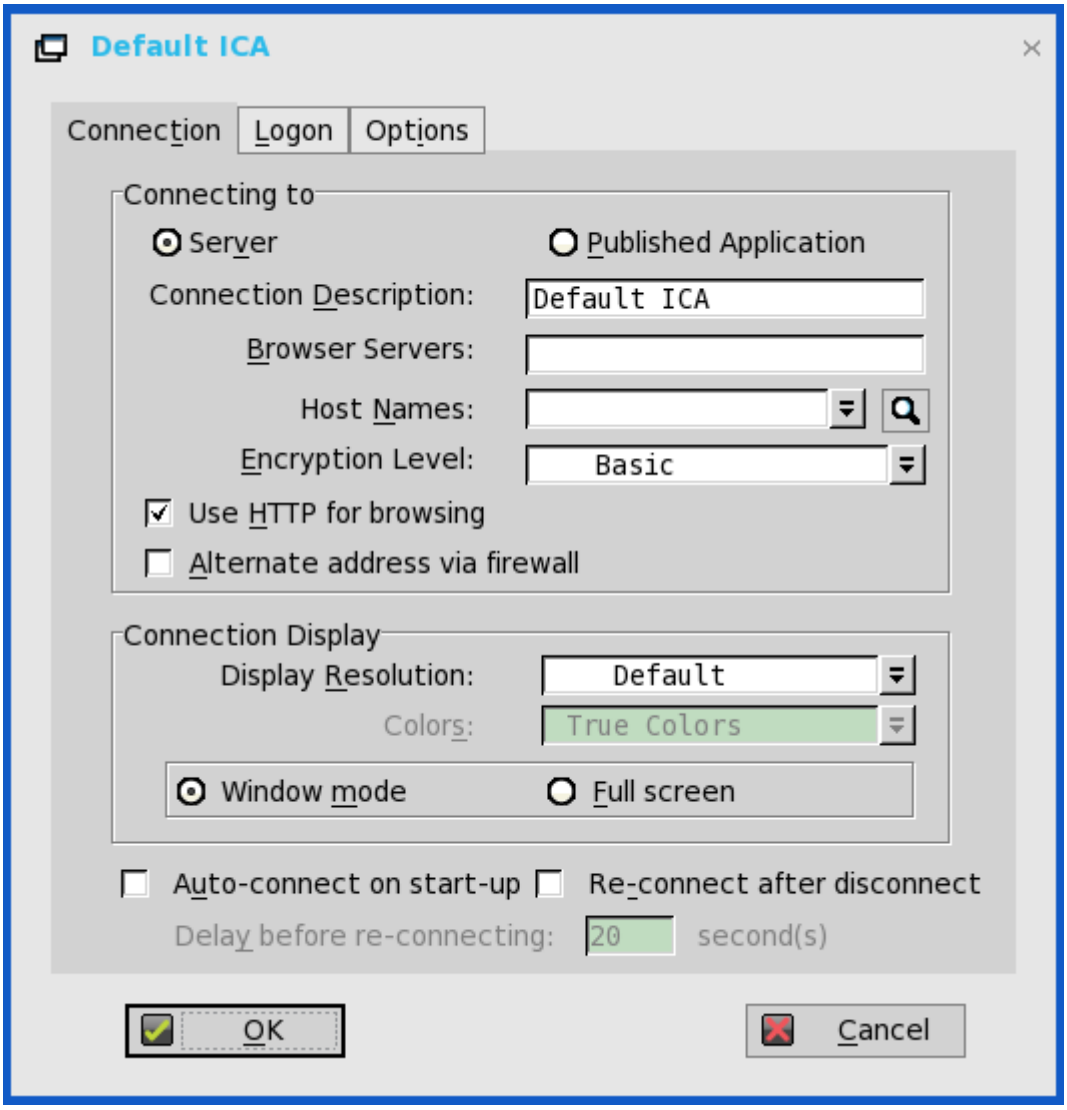


図 5.　デフォルト ICA

a　**サーバ**または**公開アプリケーション**——設定を適用する接続のタイプを選択します。

b　**接続の説明**——接続リストに表示するわかりやすい名前を入力します（最大 38 文字）。

c　**ブラウザサーバ**——マスターブラウザリストがある ICA サーバか、マスターブラウザリストがある別のサーバを参照できる ICA サーバの IP アドレスまたは DNS 登録名を（カンマまたはセミコロンで）区切ったリストにして入力します。
マスターブラウザリストは、（サーバ間のネゴシエーションで選択される）いずれかの ICA サーバ上の閲覧プログラムによって自動的に生成されます。このリストは、ホスト名ボックスまたは IP ボックスに表示される情報を提供するために使用されます。このリストがシンクライアントと同じネットワークセグメントに配置されている ICA サーバにある場合、入力は不要です。サーバに接続する場合や、サーバ名か IP にそのサーバの IP アドレスが含まれている場合も、入力は不要です。

d　**ホスト名またはアプリケーション名**（このタイトルは Server オプションまたは Published Application オプションの選択によって変わります）——サーバホスト名か IP アドレスをセミコロンまたはカンマで区切ってリストにして入力するか、ICA マスターブラウザから取得した ICA サーバまたは公開アプリケーションのリストから選択できます。ボックスの横にある**ブラウズ**を使用しても、希望する選択ができます。
サーバの区切りリストを入力した場合は、シンクライアントは前のサーバへの接続に失敗すると、リスト上の次のサーバに対して接続しようとします。リストを使用して選択した接続が失敗すると、シンクライアントはリスト上の次のサーバに対して接続しようとします。

メモ：ホスト名は、3 つのメカニズムのいずれかを使用して解決できます。ICA マスターブラウザ、DNS、WINS のいずれかです。マスターブラウザは、公開アプリケーションに対して DNS で手動入力を行っていない場合、公開アプリケーションを解決できる唯一のメカニズムです。DNS は、ネットワークコントロールパネルのデフォルトドメイン名を使用して、FQDN を作成しようとしますが、デフォルトを使用しない名前の解決も試みます。

e **暗号化レベル**——シンクライアントと ICA サーバ間の通信のセキュリティレベルを選択できます。

基本設定（デフォルトオプション）が最低のセキュリティレベルです。Basic では、高レベルの暗号化よりも必要な処理が少ないため、デバイスと ICA サーバ間で高速な通信ができます。

メモ：選択した暗号化は、シンクライアントと ICA サーバ間の通信のセキュリティに対してのみ適用されます。この設定は、ICA サーバ上の各アプリケーションのセキュリティ設定とは別のものです。たとえば、Web でのほとんどの金融取引には、シンクライアントで 128 ビット暗号化が必要です。シンクライアントの暗号化も 128 ビットに設定していないと、取引情報には、より低いレベルのセキュリティが適用されてしまう可能性があります。

f **HTTP を使用する**——オンにすると、デフォルトでシンクライアントは閲覧に HTTP を使用します。

g **代替アドレスを使用する**——オンにすると、シンクライアントは ICA マスターブラウザから返された代替 IP アドレスを使用して、ファイアウォールを通過します。接続がアクティブになるときに Windows のログオンで使用されます。

h **解像度**——この接続の画面解像度を選択します。

公開アプリケーションオプションを選択している場合、解像度の**シームレス**オプションを選択できます。

色——ICA セッションの表示色を選択できます。High Colors（16 bits）または True **Colors** が選択されていて、ICA サーバがその表示色をサポートしていない場合、シンクライアントは表示色を 256 Colors [8 – bits]などの低い値に調整します。

i **ウィンドウモード**および**全画面モード**——アプリケーションとデスクトップの最初の表示を、ウィンドウ化された画面にするか、フルスクリーンにするかを選択します。

j **起動時に自動接続**——オンにすると、起動時にセッションが自動接続されます。

k **切断後に再接続**——オンにすると、操作者以外によって切断された後で、シンクライアントをセッションに自動で再接続します。オンにすると、待機間隔は**再接続前に遅延**ボックスに設定した間隔（1〜3600 秒で入力）か、ユーザープロファイルに設定した Yes の場合の間隔（20 秒）または秒単位の間隔です。この接続の記述が INI ファイルにない場合や、スタンドアロンユーザーがいる場合、単に省略されている場合は、デフォルトは 20 秒です。

5 **ログオン**タブをクリックし、次のガイドラインに従います。

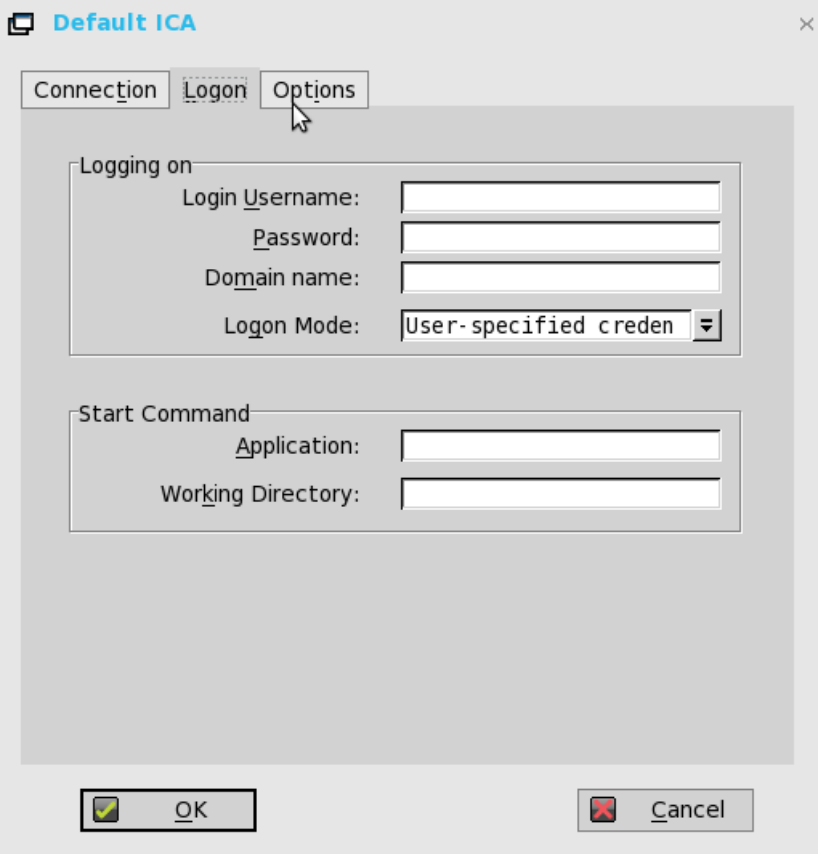


図 6.　デフォルト ICA——ログオン

a　**ログオン設定**——ユーザ名、パスワード、ドメイン名、およびログオンモードに入力します。
ユーザ名、パスワードおよびドメイン名ボックスに入力されていない場合は、接続時に ICA サーバログイン画面に情報を手動で入力できます。

- ユーザ名——最大 31 文字まで入力できます。
- **パスワード**——最大 19 文字まで入力できます。
- **ドメイン名**——最大 31 文字まで入力できます。
- **ログオンモード**——**指定ユーザ**、**スマートカード**、または**ローカルユーザ**を選択します。

b　**接続時に実行する領域**——サーバ接続オプションのみ——この領域は、公開アプリケーションオプションに対しては無効です。
アプリケーション（最大 127 文字）と**作業ディレクトリ**（最大 63 文字）——関連付けられた作業ディレクトリなど、接続時に自動的にサーバ上で開始する初期化文字列と引数を入力します。

6　**オプション**タブをクリックし、次のガイドラインに従います。

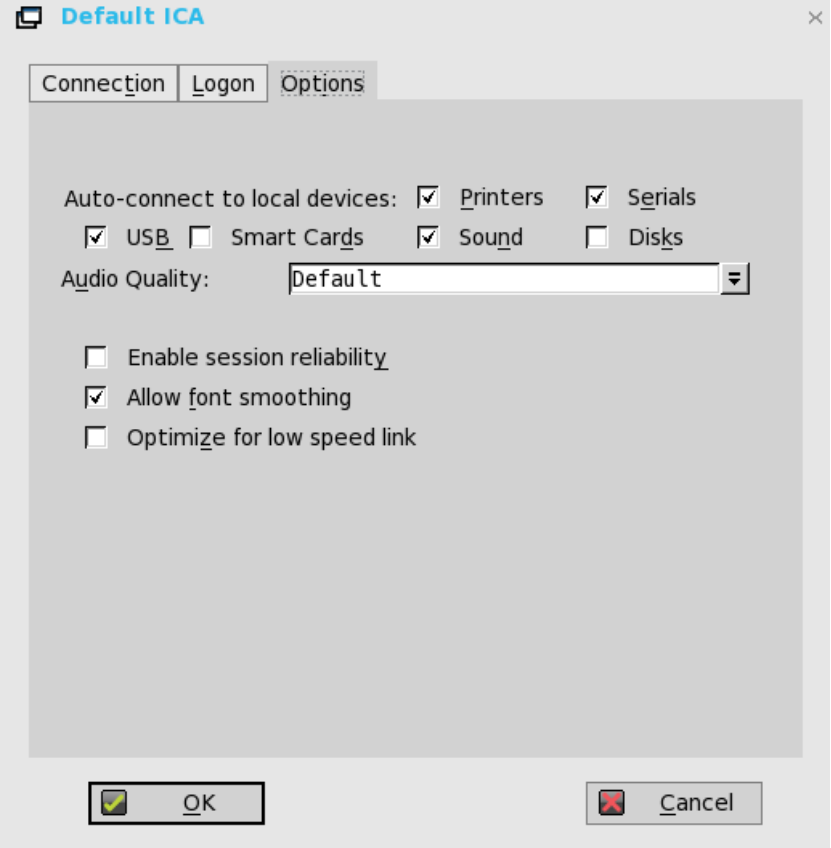


図 7.　デフォルト ICA——オプション

a　**ローカルデバイスに自動接続**——任意のオプション（プリンタ、シリアル、USB、スマートカード、およびディスク）を選択し、シンクライアントがこれらのデバイスに自動的に接続するようにします。

b　フォントスムージング——オンにすると、フォントスムージング（滑らかな文字）を有効にします。

c　**低速回線に最適化**——オンにすると、音声品質を下げたり、プロトコル専用のキャッシュサイズを減らしたりするなど、低速接続に最適化できます。WAN リンクをまたぐ接続やダイアルアップを使用する接続を対象としています。

d　**セッション画面の保持を有効化**——有効にすると、セッションの信頼性を高めて、ユーザーが一時的にサーバとの接続を失っても、接続の回復時に再認証する必要がなくなります。X 秒後にユーザーの接続タイムアウトが発生するのではなく、セッションはサーバ上で維持され、接続が回復するとクライアントが利用できるようになります。セッションの信頼性が最も重視されるのは、ワイヤレスデバイスを使用する場合です。

Citrix セッションでマルチモニタをサポート

ThinOS は、XenDesktop／XenApp 7.6 以降のバージョンでは、ICA デスクトップマルチモニタをサポートします。

前提条件：

- 1 つまたは複数の 4K 解像度モニタをサポートするには、**MaxVideoMemoryBytes** REG_DWORD の値を大きくします。詳細については、support.citrix.com の Citrix ドキュメントを参照してください。
- 色深度を増やして解像度を上げるには、表示メモリ制限を大きくします。詳細については、citrix.com の Citrix ドキュメントを参照してください。

ユーザーのシナリオ：

1　複数のモニタを ThinOS デバイスに接続します。
2　**ディスプレイ**ダイアログボックスで、**ミラーモード**を無効にし、ディスプレイレイアウトを設定します。
3　ICA デスクトップをフルスクリーンで立ち上げます。

表 7.　ディスプレイの詳細

プラットフォーム	ディスプレイの最大解像度	システムディスプレイの最大数	
		標準または RDS デスクトップ——Windows 10/2012 R2/2016	HDX 3D Pro デスクトップ——Windows 10（GRID K1/K2 GPU 搭載）
Wyse 5070 Extended シンクライアント	1920×1080	6	4
	2560 x 1440	6	4
	3840 x 2160	6	GRID K1/K2 vGPU のプロファイル制限のため、サポートされません。
Wyse 5070 シンクライアント——Pentium Processor	1920×1080	3	3
	2560 x 1440	3	3
	3840 x 2160	3	GRID K1/K2 vGPU のプロファイル制限のため、サポートされません。
Wyse 5070 シンクライアント——Celeron Processor	1920×1080	2	2
	2560 x 1440	2	2
	3840 x 2160	2	GRID K1/K2 vGPU のプロファイル制限のため、サポートされません。

制限

- Wyse 5070 Extended シンクライアントの標準または RDS デスクトップ（Windows10/2012 R2/2016）については、4K モニタを最大 4 台とし、残りは解像度が 1920 x 1080 のモニタを使用することを、デルはお勧めします。
- vGPU または GPU Passthrough を使用する HDX 3D Pro デスクトップについては、サポートされる解像度とモニタの数は、NVIDIA の GRID サポートマトリックスに基づいています。

メモ：Citrix の正式なマルチモニタのサポートの詳細については、support.citrix.com の Citrix ドキュメントを参照してください。

ICA Self Service のパスワードリセット

セキュリティに関する質問の登録を完了すると、パスワードのリセットまたはアカウントのロック解除が可能となります。

サポート対象環境

- XenDesktop 7.11 以降のバージョン
- Storefront サーバ 3.7 以降のバージョンをサポート
- Self-Service Password Reset Server 1.0 以降のバージョン

サポート対象プラットフォーム——すべてのプラットフォームがサポート対象

制限

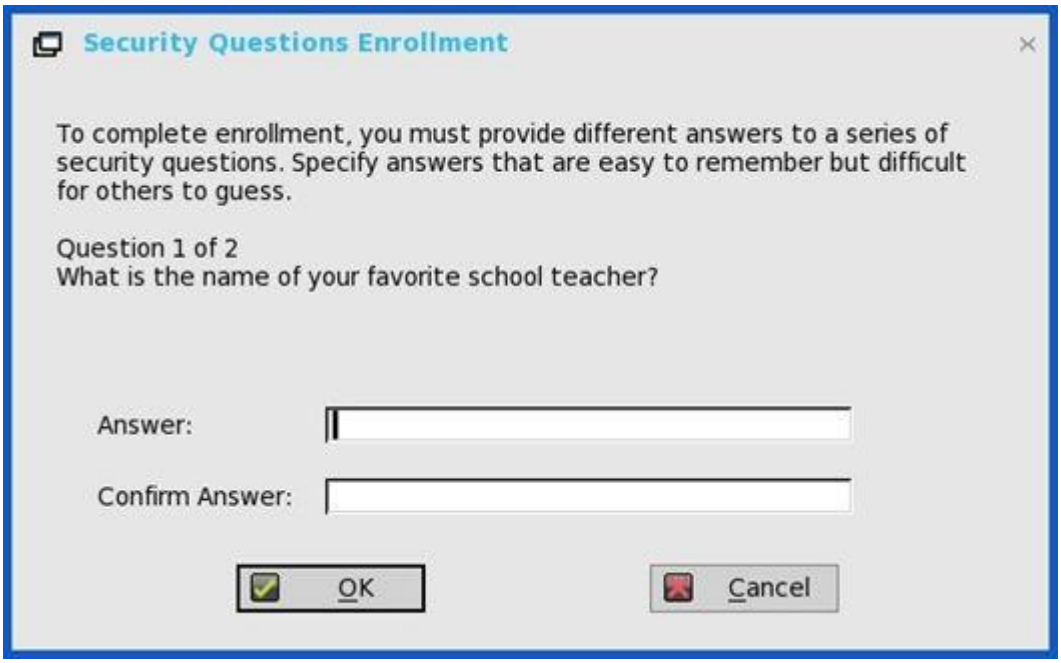
- storefront サーバのみサポート
- Legacy Account Self-Service（ThinOS リモート接続設定で設定された Account Self-Service Server が必要）は、この storefront のバージョンには依存しません。storefront のバージョンは、Legacy Account Self-Service を対象とします。
- セキュリティに関する質問の登録は、Virtual Desktop Infrastructure（VDI）モードではサポートされません。

パスワードのリセットやアカウントのロック解除の前に

パスワードのリセットやアカウントのロック解除の前に、セキュリティに関する質問を登録する必要があります。セキュリティに関する質問への回答を登録するには、次の操作を行います。

1 **PNMenu** で、**Manage Security Questions** オプション（クラシックおよび StoreFront のみ）をクリックします。**Security Questions Enrollment** ウィンドウが表示されます。

2 セキュリティに関する質問に対して、適切な回答を入力します。



3 セキュリティに関する質問を登録するには、**OK** をクリックします。

アカウントセルフサービスを使用する

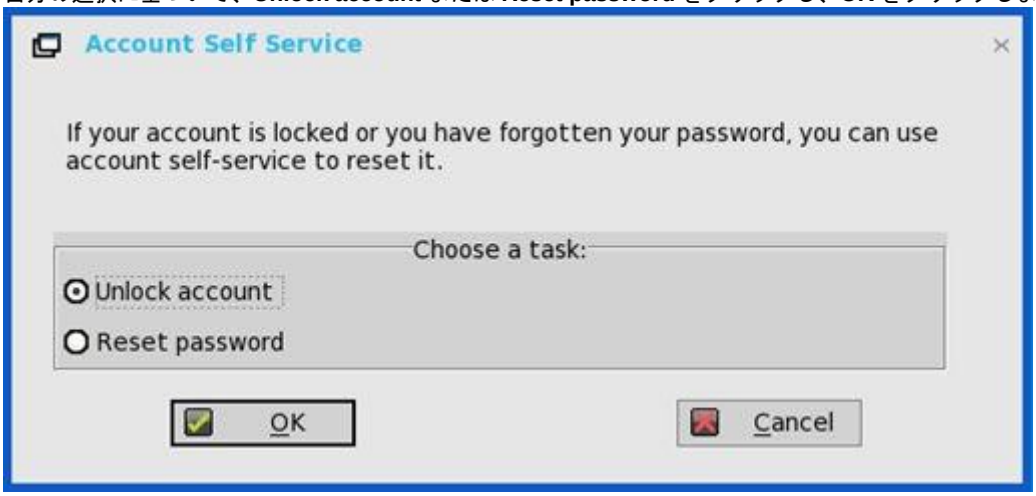
セキュリティに関する質問の登録が完了した後は、セルフサービスパスワードリセットを有効にして ThinOS を StoreFront サーバに接続すると、サインオンウィンドウに**アカウントセルフサービス**アイコンが表示されます。

メモ：サインオンウィンドウで 5 回以上パスワードの入力を間違えると、クライアントは自動的にアカウントロック解除プロセスに入ります。

1 **アカウントセルフサービス**アイコンをクリックし、アカウントのロックを解除するか、パスワードのリセットをします。

メモ：アカウントロックの解除またはパスワードのリセットを使用する前に、ユーザーのセキュリティに関する質問を登録する必要があります。

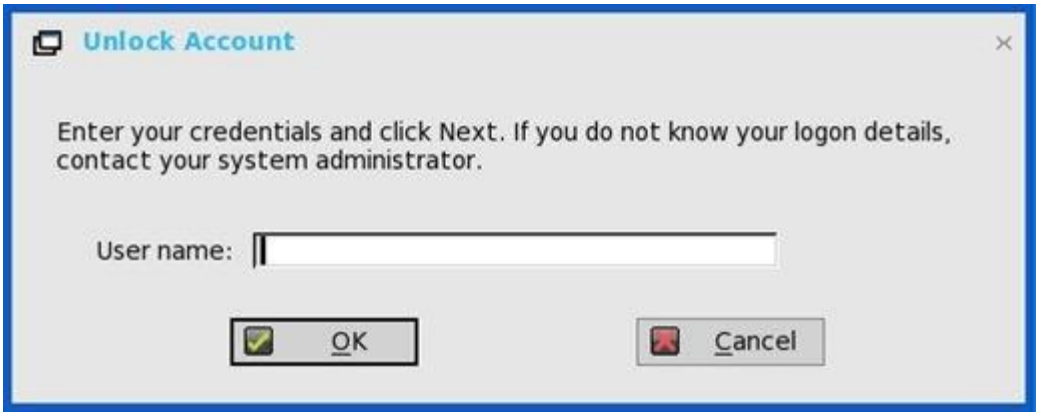
2 自分の選択に基づいて、**Unlock account** または **Reset password** をクリックし、**OK** をクリックします。



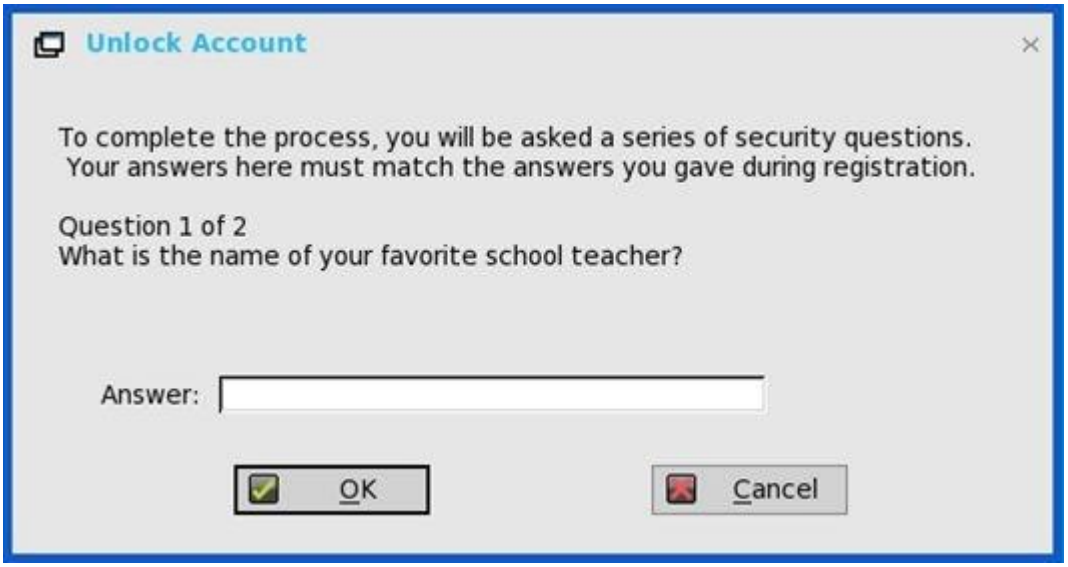
アカウントロックの解除

セキュリティに関する質問を登録した後、アカウントロックを解除するには、次の操作を行います。

1 **Account Self-Service** ウィンドウで、タスク（Unlock account）を選択します。
2 ユーザー名を入力します。
Unlock Account ダイアログボックスが表示されます。

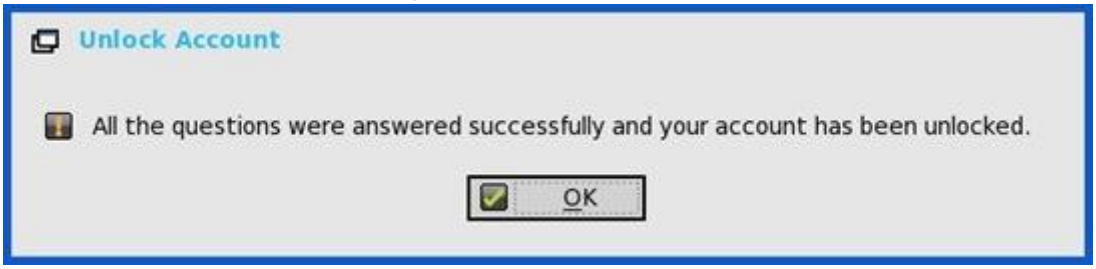


3 セキュリティに関する質問に登録された回答を入力します。



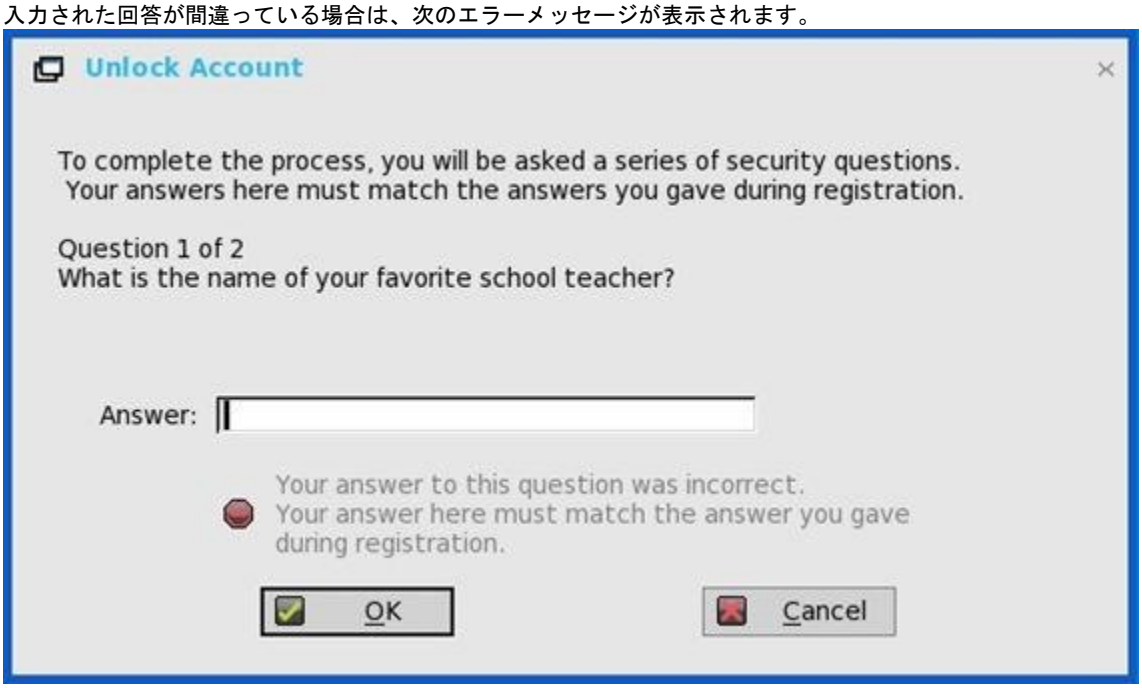
入力された回答が登録された回答と一致すると、**Unlock Account** ダイアログボックスが表示されます。

4 **OK** をクリックしてアカウントロックを解除します。

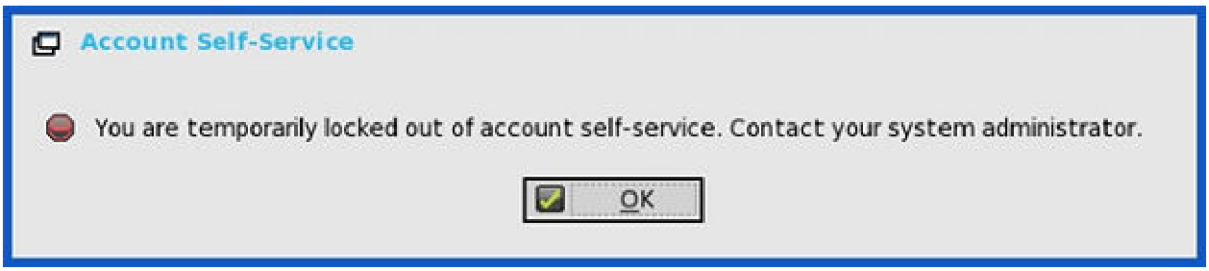


メモ：

- 入力された回答が間違っている場合は、次のエラーメッセージが表示されます。



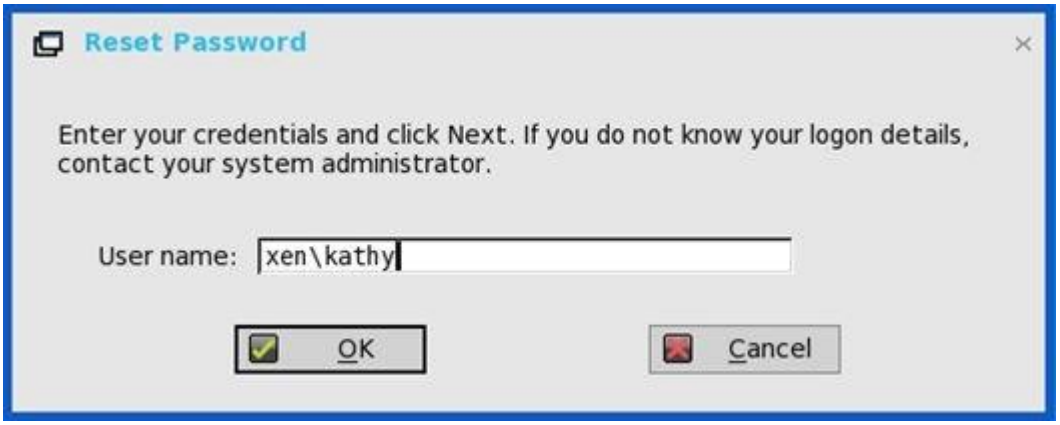
- 4 回以上間違った回答を入力した場合、アカウントロックの解除またはパスワードのリセットはできず、次のエラーメッセージが表示されます。



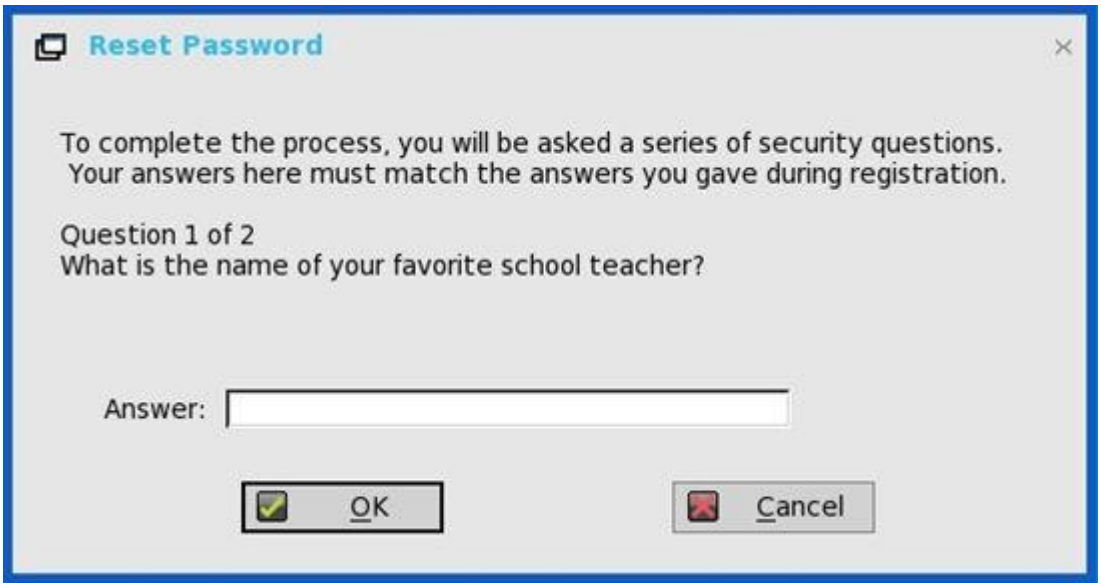
パスワードのリセット

セキュリティに関する質問を登録した後、パスワードをリセットするには、次の操作を行います。

1 **Account Self-Service** ウィンドウで、タスク（Reset password）を選択します。
2 ユーザー名を入力します。
Reset Password ダイアログボックスが表示されます。



3 セキュリティに関する質問に登録された回答を入力します。



入力された回答が登録された回答と一致すると、**Reset Password** ダイアログボックスが表示されます。

4 新しいパスワードを入力し、確認フィールドに同じパスワードを入力します。

5 **OK** をクリックしてパスワードを変更します。

間違った回答を入力すると、パスワードはリセットできず、エラーメッセージが表示されます。

QUMU または ICA Multimedia URL Redirection

QUMU は、ICA Multimedia URL Redirection を利用します。この機能を動作させるには、ブラウザのプラグインをインストールする必要があります。

ThinOS の初期のリリースでは、ICA Multimedia URL Redirection は部分的にサポートされていました。ThinOS 8.4 リリース以降、ICA マルチメディア URL リダイレクトのパフォーマンスを向上させるため、いくつかの改善が行われています。

サポート対象プロトコル：

- RTPS HLS
- HTTP

QUMU Multimedia URL Redirection の確認： ビデオを再生中に画面のブラウザを移動したり、ブラウザをスクロールしたりすると、ビデオウィンドウで映像の遅延や抜けが目立ちます。こうした動きはビデオがリダイレクトされることによるものです。

HTML5 Video Redirection

HTML5 Video Redirection によって、XenApp および XenDesktop サーバが、HTML5 マルチメディアのウェブコンテンツをユーザーに提供する方法が制御、最適化されます。XenApp および XenDesktop 7.12 から、この機能は内部のウェブページにのみ使用可能です。HTML5 マルチメディアコンテンツが利用できるウェブページ（たとえば、内部のトレーニングサイトのビデオ）に、JavaScript を追加する必要があります。

次のサーバポリシーを有効にする必要があります。

- Windows Media リダイレクト——このオプションはデフォルトで有効になっています。
- HTML5 ビデオリダイレクト——このオプションはデフォルトで無効になっています。

HTML5 Video Redirection を確認——ビデオを再生中に画面のブラウザを移動したり、ブラウザをスクロールしたりすると、ビデオウィンドウで映像の遅延や抜けが目立ちます。こうした動きはビデオがリダイレクトされることによるものです。

RAVE MMR の ThinOS イベントログも表示されます。

参考資料

- Citrix サンプルビデオ——www.citrix.com/virtualization/hdx/html5-redirect.html。
- ICA Multimedia ポリシー設定——www.docs.citrix.com/en-us/xenapp-and-xendesktop/7-12/policies/reference/ica-policy-settings/multimedia-policy-settings.html。

ICA SuperCodec

ICA SuperCodec は、ThinOS ICA クライアント側で統合された H.264 デコーダです。サーバは、セッションイメージを H.264 ストリームに変換し、クライアント側に送信します。クライアントは、SuperCodec によって H.264 ストリームをデコードし、イメージを画面に表示します。この機能により、特に HDX 3D Pro デスクトップでのユーザーエクスペリエンスが向上します。

サポート対象環境

XenDesktop／XenApp 7.5 以降のバージョン

前提条件

XenApp/XenDesktop バージョン 7.9 以降では、**Use video codec for compression** のデフォルト設定は **Use when preferred** です。ThinOS デバイスの性能を最大にするために、デルは **Use video codec for compression** ポリシーを **For the entire screen** に設定することをお勧めします。これとは別に、このポリシーを **Do not use video codec** に設定する方法もあります。これによって ThinOS は、帯域幅を節約し CPU オーバヘッドを削減する **ThinWire Plus** を使用できるようになります。

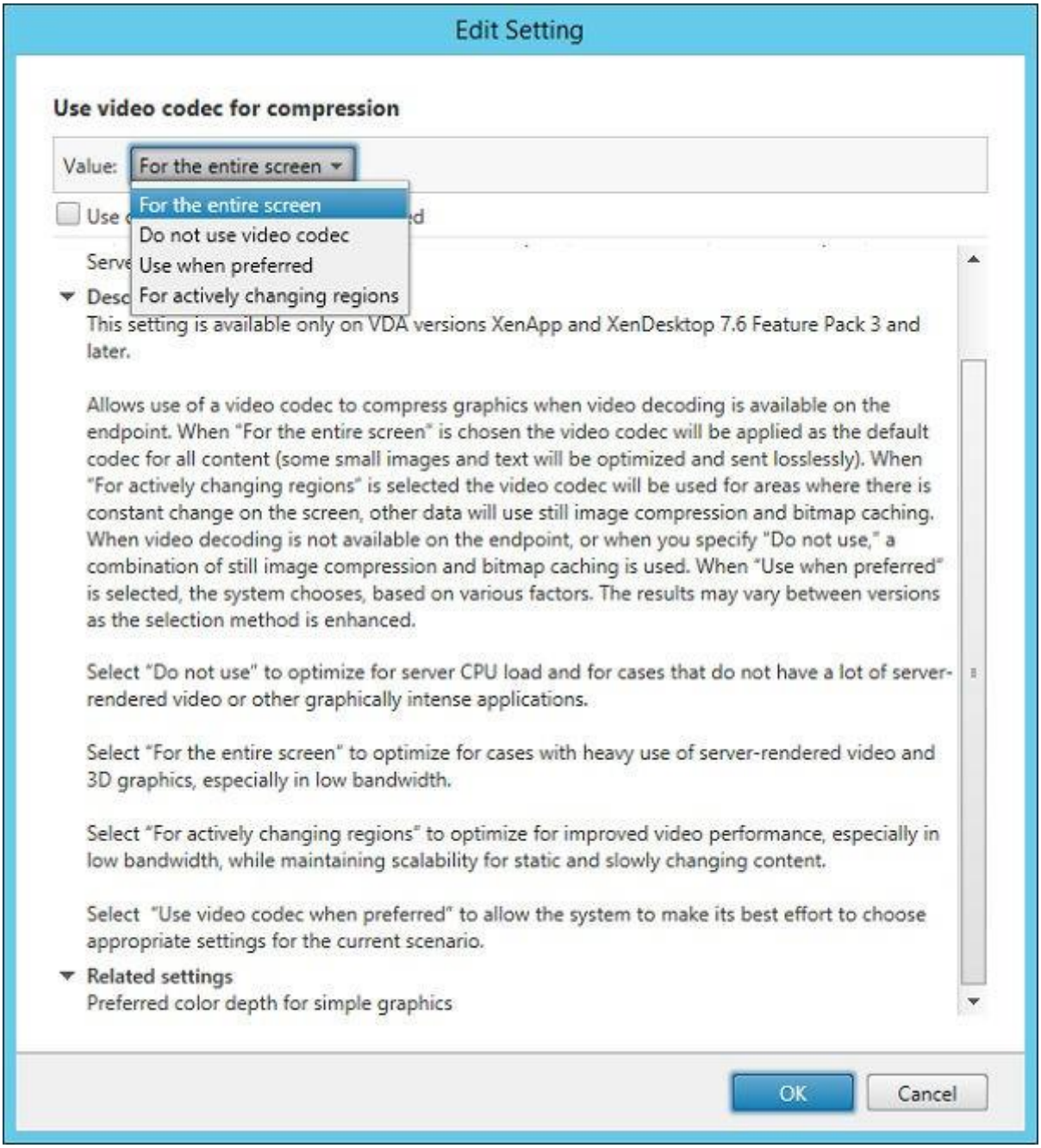


図 8.　圧縮設定にビデオコーデックを使用

- **ThinWire Plus**——**Do not use video codec** オプションに相当
- **Fullscreen H.264**——**For the entire screen** オプションに相当
- **Selective H.264**——**For actively changing** リージョンに相当

ICA 接続の動作ステータスを確認

- ICA SuperCodec は常に無制限に有効です。
- ThinOS イベントログには、「ICA:SuperCodec enabled」と表示されます。

メモ：ICA 接続には、INI パラメータはありません。
Use video codec for compression ポリシーを **Do not use video codec** に設定すると、ICA SuperCodec は無効となり、ThinOS はどのようなログも出力しません。

匿名ログオン

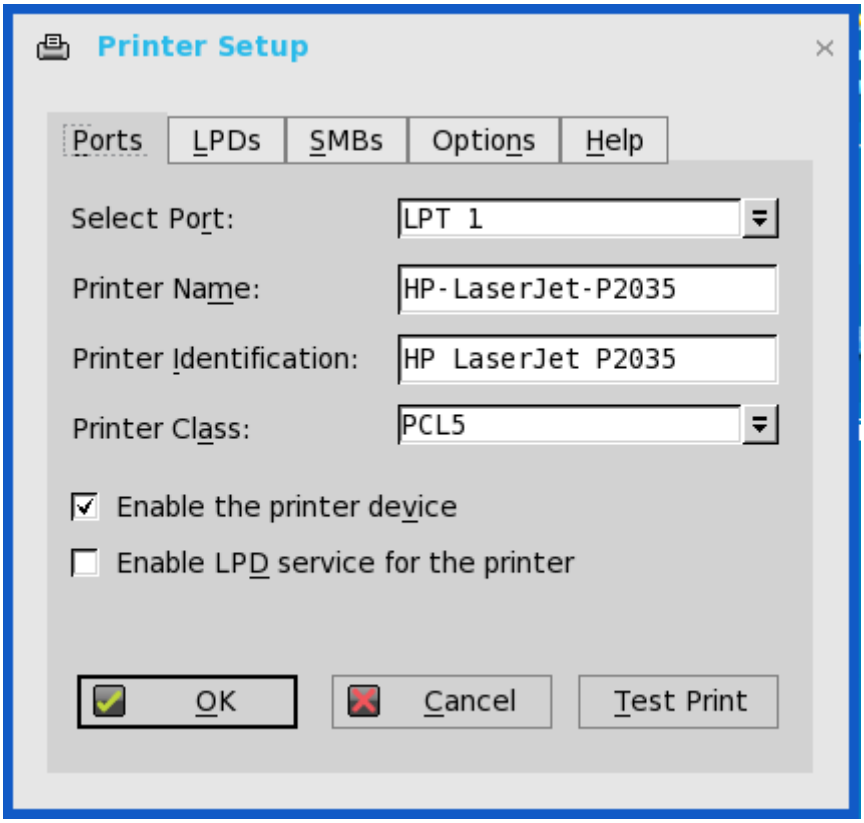
匿名ログオン——この機能では、認証されていないストアが設定された Storefront サーバに、ユーザーが Active Directory（AD）ユーザー資格情報を使用しないでログオンできます。この機能によって、AD アカウントではなく、認証されていないユーザーがアプリケーションにアクセスできます。

ⓘ **メモ：Storefront サーバのレガシーモードでは、匿名ログオンはサポートされていません。**

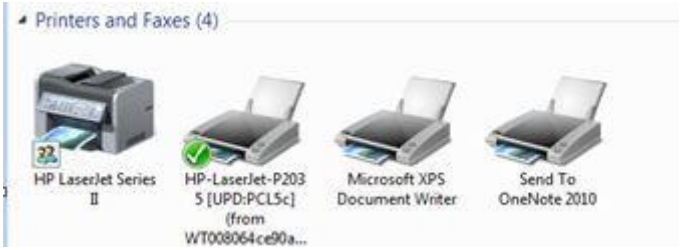
Citrix UPD プリンタの設定

Citrix ユニバーサルプリンタドライバ（Citrix UPD）を使用すると、新しいプリンタドライバをデータセンターに統合することなく、クライアントに接続されたすべてのプリンタを仮想デスクトップやアプリケーションセッションからでも使用できます。Citrix UPD は、Citrix ユニバーサルプリンタの基盤です。Citrix ユニバーサルプリンタは、Citrix UPD を使用し、クライアントで定義されている特定のプリンタに関連付けられていない、自動作成のプリンタオブジェクトです。
ThinOS での Citrix UPD の使用方法を設定するには

1 プリンタを ThinOS クライアントに接続します。
2 デスクトップメニューで**システム設定**をクリックし、**Printer** をクリックします。
プリンタ設定ダイアログボックスが表示されます。



3 **プリンタ名**ボックスにプリンタの名前を入力します。
4 **プリンタ ID** ボックスに任意のプリンタ識別情報の文字列を入力します。
5 ドロップダウンリストからプリンタクラスのタイプを選択します。チェックボックスをオンにして**プリンタデバイス**を有効にしてから **OK** をクリックします。
6 XenDesktop または XenApp アプリケーション接続を始動します。
7 デスクトップまたはアプリケーションで Devices and Printers を開き、デフォルトでプリンタが UPD プリンタとしてマップされていることを確認します。HP-LaserJet-P2035 [UPD:PCL5c]を使用して、プリントジョブを実行できます。



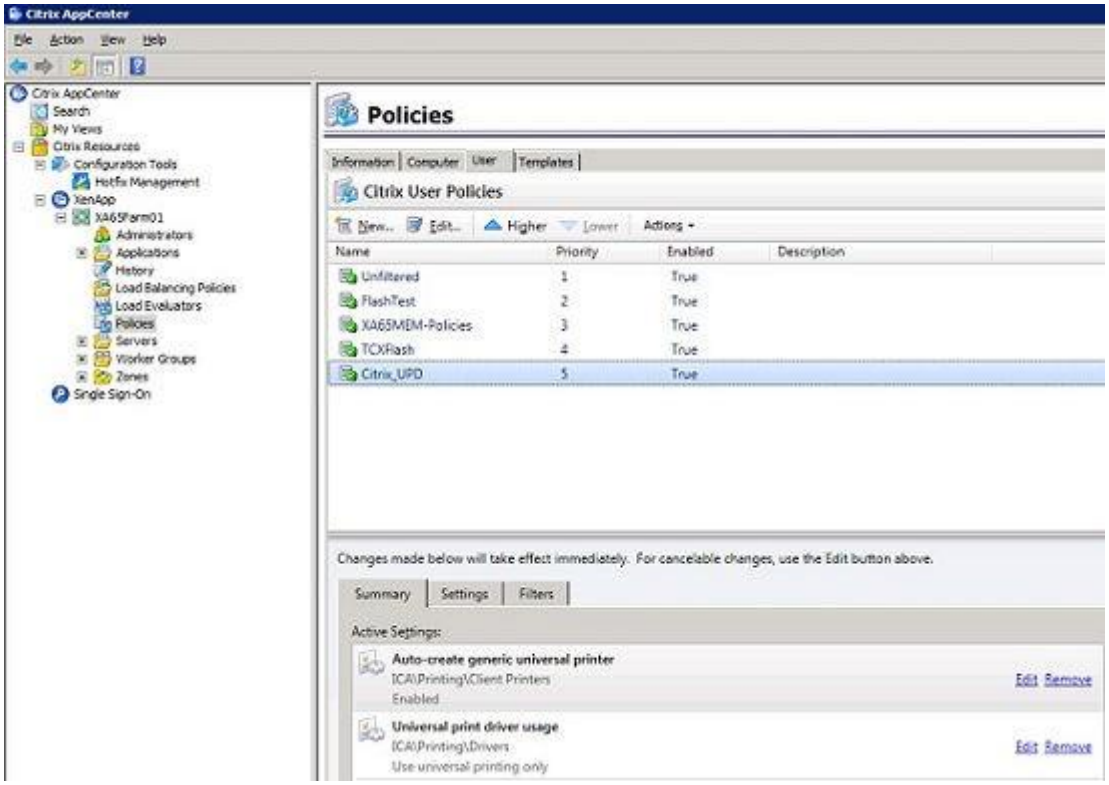
サーバでの Citrix UPD 設定

a　プリンタポリシーを有効にするには、次のガイドラインに従います。

1　XenApp 6.5 でプリンタポリシーを有効にするには、DDC Server に移動し、**Start > Citrix AppCenter** をクリックします。

2　**Citrix Resources > XenApp > Policies > User > Settings > Printing > Client Printers** をクリックし、**Auto-create generic universal printer** を有効にします。

3　**Printing > Drivers** をクリックし、使用可能なドロップダウンメニューで **Universal print driver usage** を **Use universal printing only** に設定します。

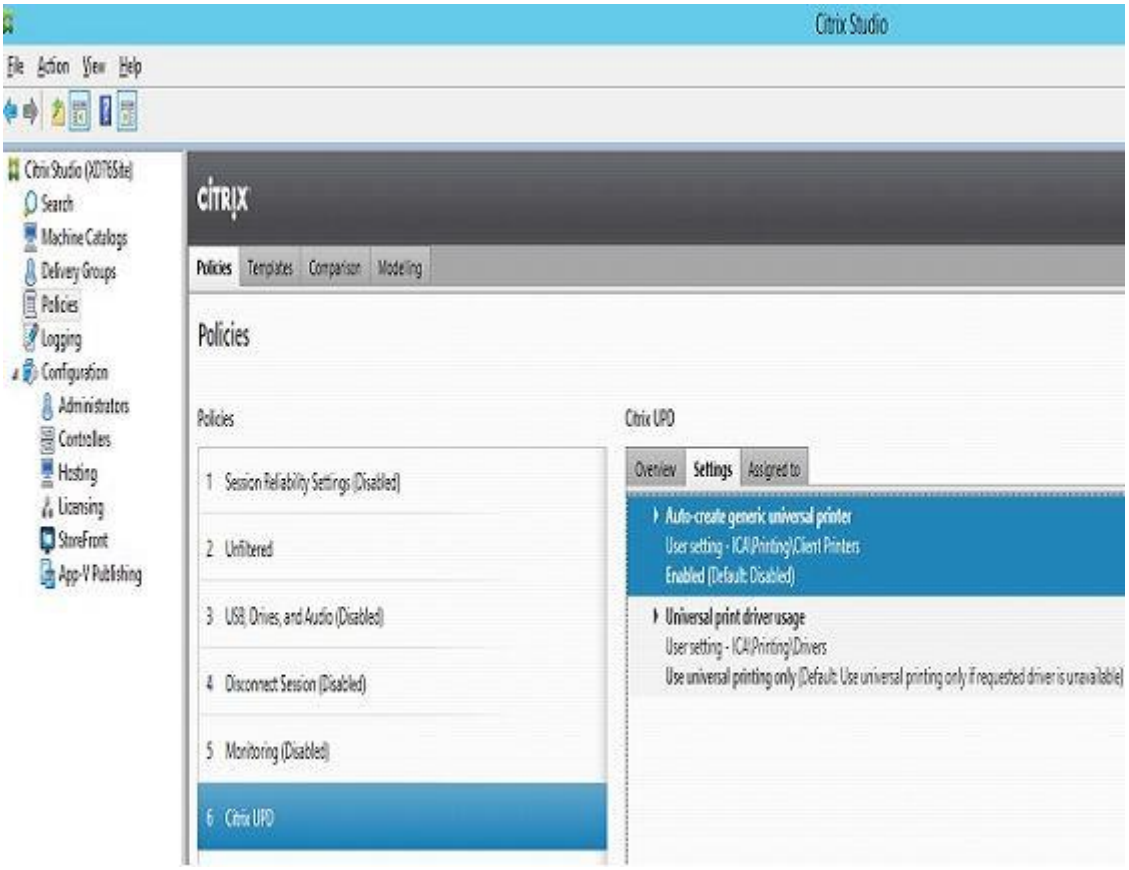


4 XenApp/XenDesktop 7.5 以降のバージョンで、プリンタポリシーを有効にするには、次の操作を行います。

a Citrix DDC Server に移動します。

1 **Citrix studio > policies** をクリックし、ポリシーを追加します。**Auto-create generic universal printer** オプションを有効にします。

2 ドロップダウンメニューで **Universal print driver usage** を **Use universal printing only** に設定します。



b レジストリを確認し、同じドライバがインストールされていることを確認します。

1 接続するサーバまたはデスクトップのレジストリのドライバを確認します。サーバまたはデスクトップのレジストリに ps、pcl5、pcl4 の各ドライバがあり、同じドライバがサーバまたはデスクトップにインストールされている必要があります。

2 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\UniversalPrintDrivers\に移動します。ThinOS では、EMF と XPS をサポートしていません。

> **メモ：次の表のサポート対象のドライバは、ThinOS で使用される Citrix UPD のサポート対象のドライバの一つです。推奨されるドライバの一つがここに例として挙げられています。**

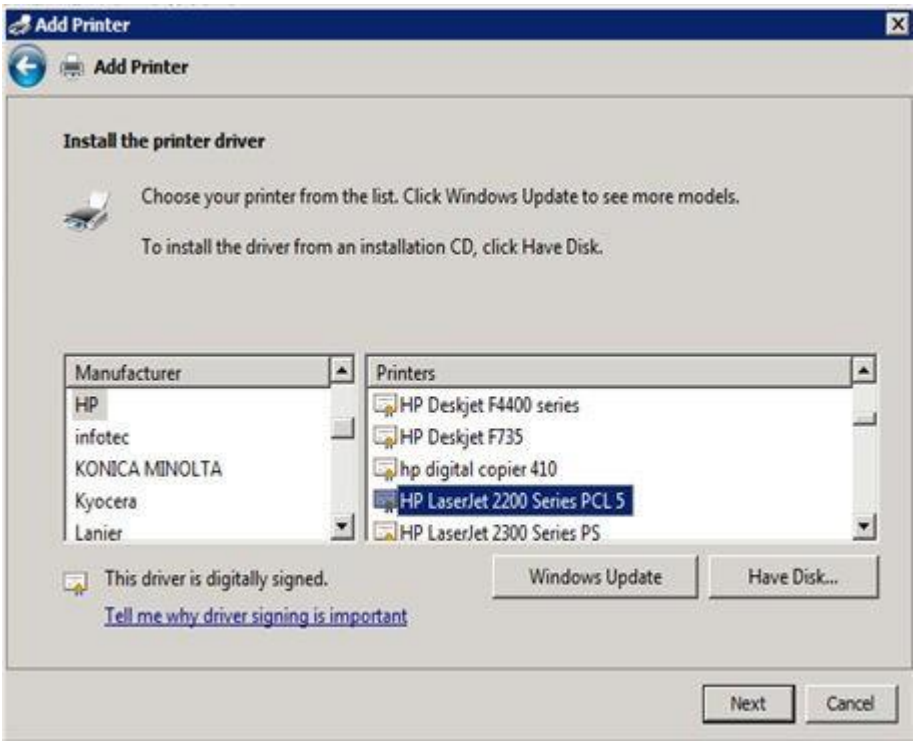
次の表に、サポート対象のドライバを示します。

表 8. サポート対象のドライバ

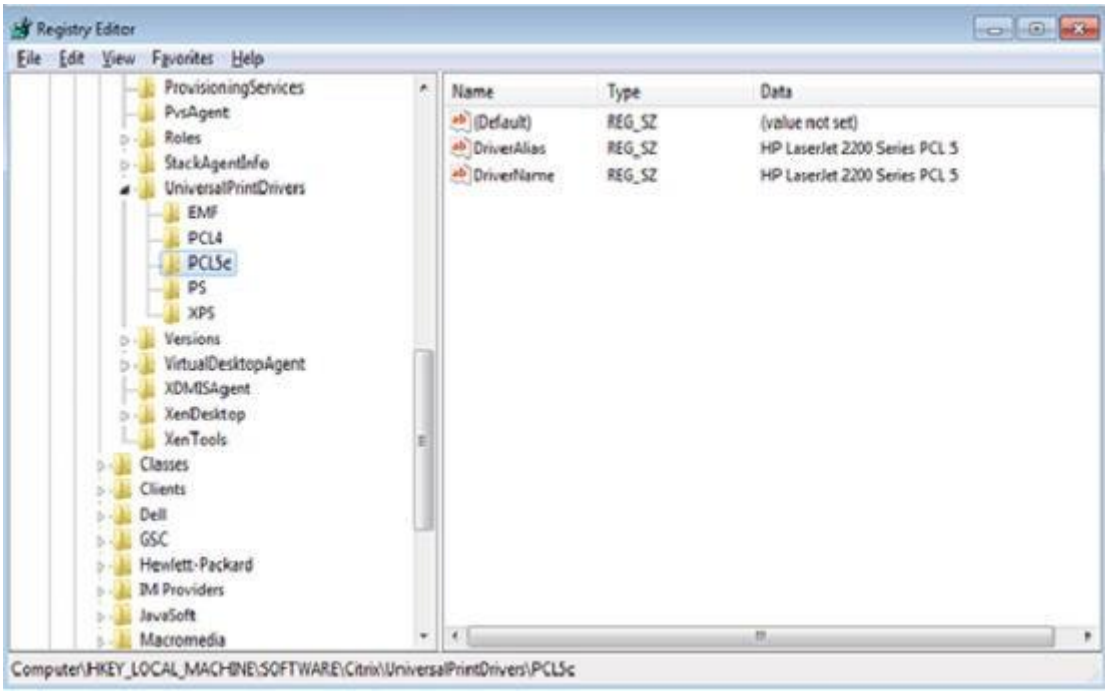
プリンタクラス	プリンタ ドライバ
PS	HP Color LaserJet 2800 Series PS
PCL5	HP LaserJet 2200 Series PCL 5
PCL4	HP LaserJet Series II

c 接続するサーバまたはデスクトップにこれらのドライバがない場合は、次の手順に従います。

1 例として、XenApp A6.5 + 2008 R2 で、サーバに PCL ドライバを追加します。**Device and Printers > Select any printer > Click Printer server properties > Driver** タブに移動し、**HP LaserJet 2200 Series PCL 5 driver** を追加します。



2 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\UniversalPrintDrivers\PCL5c\の下にある DriverAlias および DriverName を **HP LaserJet 2200 Series PCL 5** に変更します。



Flash リダイレクト

Flash リダイレクトソリューションは、Flash コンテンツを ThinOS クライアントにオフロードして、ローカルで Flash の再生のレンダリングとデコードを行います。このオフロードは、Citrix HDX Flash リダイレクトによって実行されます。ローカルレンダリングおよびデコード処理は、ThinOS 上で、ローカルで実行されるカスタマイズした Flash Player とその他のマルチメディア処理によって行われます。

サポート対象環境——XenApp 6.5 以降のバージョンおよび XenDesktop 7.0 以降のバーションを使用した Citrix 接続のみをサポートします。

必要なパッケージ

この機能が動作するには、ユーザーは FR.i386.pkg パッケージをインストールする必要があります。

パッケージのインストール

必要なパッケージをインストールするには、ここで説明するステップに従います。

1 パッケージを¥wnos¥pkg¥ディレクトリにアップロードします。
2 INI の autoload が 0 に設定されていないことを確認します。wnos.ini に「INI AutoLoad=1 AddPkg=FR」を設定します。
3 クライアントをリスタートしてファイルサーバを読み取り、パッケージの自動インストールが完了するまで待機します。
インストールされた**パッケージ**は、システムツールダイアログボックスの**パッケージ**タブに表示されます。
4 **Flash リダイレクトのサーバ設定**
   a Flash Player のバージョン間の差異を無視できるよう、ユーザーはデスクトップで FlashPlayerVersionComparisonMask および ClientFlashPlayerVersionMinimum のレジストリキーを追加する必要があります。
   XenApp 6.5 の場合は、IE ブラウザのバージョン間の差異を無視できるよう、IEBrowserMaximumMajorVersion レジストリキーが必要です。

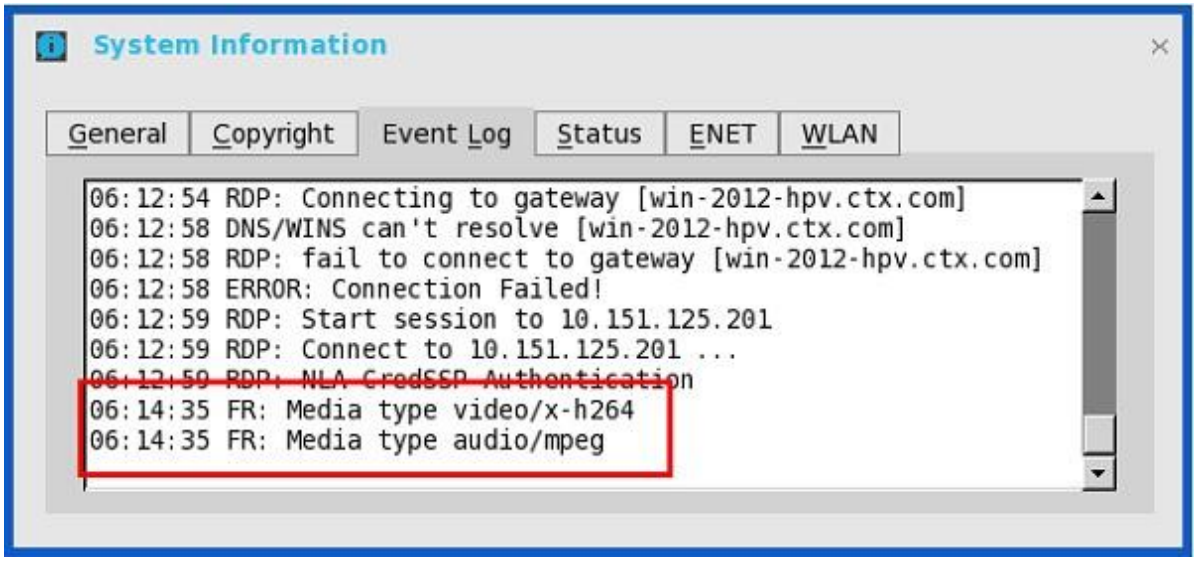
   詳細については、docs.citrix.com/en-us/xenapp-and-xendesktop/7-9/hdx/flash-redirection.html を参照してください。

   XenDesktop 7.9 から、HDX FR を動作させるために、レジストリにさらにエントリーを追加する必要があります。こうしたエントリーの追加の詳細については、Citrix の技術マニュアルを参照してください。
5 **Flash リダイレクトのクライアント設定**
デフォルトでは、クライアント設定は必要ありません。新しい INI パラメータが HDX FR クライアント設定をサポートするために追加され、サーバ側のコンテンツの取得などに使用できます。新しく追加された INI パラメータは、次のとおりです。

```
SessionConfig=ICA\
HDXFlashUseFlashRemoting=Never | Always（デフォルト）\
HDXFlashEnableServerSideContentFetching=Disabled（デフォルト）| Enabled \
```

正常に動作しているかどうかの確認方法

a Flash ビデオを右クリックして、Flash Player のバージョンを確認します。ThinOS クライアント側のカスタマイズされたプレーヤーのバージョンが表示されます。バージョンは 11.1.102.59 です。Flash Player のバージョンがこれとは異なる場合は、サーバでのレンダリングが正しく行われません。
b Flash の再生中に、**システム情報**ダイアログボックスに HDX FR に関する ThinOS のイベントログが表示されます。
   1 FR:Media type video/x-264
   2 FR:Media type audio/mpeg



Citrix HDX Flash リダイレクトとポリシー設定の基本操作の詳細については、Citrix ドキュメントを参照してください。

既知の問題

a Flash ビデオは、通常のセキュリティ設定の Internet Explorer ブラウザで再生してください。

b Flash ビデオはロード後、初期のサイズが保持されます。たとえば、ブラウザのサイズを変更してもビデオコンテンツのサイズは変更されません。

c 英語フォントのみがサポートされます。たとえば、他の言語の字幕は適切に表示されません。

d Linux または Windows クライアントの HDX FR で動作可能なビデオで再生します。msn.com、espn.com、movies.yahoo.com、dell.com など、Citrix HDX FR ソリューションで動作しないことが確認されているビデオや Web サイトが複数あります。Flash ビデオでは、HDX FR ソリューションを使用して、これらの Web サイトをロードできません。これらの一部は、一定期間動作しています。たとえば、dell.com のビデオは、今年の 2 月と 3 月には正常に動作していましたが、その後動作しなくなりました。この結果は、ユーザーの所在地（米国／欧州／アジア）によっても異なる場合があります。そのため、Linux または Windows 上の HDX FR で、目的のビデオの動作を確認してから、ThinOS で使用することをお勧めします。

e ThinOS 上のこのソリューションは、Citrix HDX FR Linux バージョンに基づいています。問題の発生時には、Linux クライアントと比較することをお勧めします。

f YouTube.com のビデオを再生すると、問題が発生する場合があります。たとえば、ユーザーがブラウザに URL をコピーして貼り付けて再度アクセスしないと、ビデオが表示できないことがあります。この現象が発生した場合は、Linux クライアントと比較することをお勧めします。

VMware の設定

VMware 仮想化によって、1 つの物理マシンで複数の仮想マシンを稼働させることができます。VMware Horizon Client は、View Connection Server とシンクライアントオペレーティングシステムの通信をする、ローカルにインストールされたソフトウェアアプリケーションです。これによって、一元的に管理された仮想デスクトップにシンクライアントからアクセスできます。

このセクションでは、VMware ブローカー接続を ThinOS デバイスに設定する方法と、ThinOS に設定できるその他の VMware の機能について説明します。

VMware ブローカー接続の設定

VMware ブローカーセットアップを設定するには :

1 デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。
リモート接続設定ダイアログボックスが表示されます。

2 **ブローカー**タブでは、ドロップダウンリストで **VMware view** を選択し、次の操作を行います。

- **ブローカーサーバ**——ブローカーサーバの IP アドレス／ホスト名／FQDN を入力します。
- **自動接続リスト**——個別のブローカーにログイン後、自動的に起動させたいデスクトップの名前を入力します。複数のデスクトップの入力が可能です。各デスクトップの名前はセミコロンで区切り、大文字と小文字は区別します。
- **セキュリティモード**——次のオプションから望ましいセキュリティモードを選択します。
  - **警告**——警告では、自己署名証明書付きの FQDN アドレスを必要とします。証明書なしで継続しようとすると、対応する警告メッセージがユーザーに表示されます。
  - **完全**——完全では、ドメイン証明書付きの FQDN アドレスを必要とします。
  - **無効**——無効では、証明書の有無にかかわらず、FQDN／IP アドレスを許可します。
  - **既定**——システムセキュリティモード設定に従います。
- **接続プロトコル**——ドロップダウンリストで、プロトコル接続のタイプを選択します。このオプションは、デフォルトではデフォルトプロトコルのみに設定されています。

  メモ : PCoIP 専用接続プロトコルは、PCoIP クライアントにのみ使用可能です。Horizon パッケージをインストールしていない場合は、Blast 専用プロトコルオプション（Blast only protocol option）は選択できません。PCoIP プロトコルは、PCoIP セッションには必須です。Horizon パッケージは、Blast セッションには必須です。

  次のオプションを使用できます。

  – **デフォルト　プロトコルのみ**——ブローカーの各プールに、VMware View Admin コンソールで設定した通りのデフォルトプロトコルのデスクトップを表示するには、このプロトコル接続を選択します。デスクトッププールで、デフォルトプロトコルを View Admin コンソールで **RDP** と設定した場合、ユーザーがそのデバイスにサインインすると、デスクトップの RDP 接続だけが ThinOS に表示されます。

- **選択可能な組み合わせ全て**——デスクトッププールで、ユーザーのプロトコル選択の許可を **yes** と設定した場合、すべての使用可能な接続のデスクトップを表示するには、このプロトコル接続を選択します。デスクトップでデフォルトプロトコルを **PCoIP** と設定し、ユーザーのプロトコル選択の許可を **no** と設定した場合は、ThinOS は PCoIP 接続のデスクトップのみ表示します。
- **RDP のみ**——RDP 接続のデスクトップのみ表示するには、このプロトコル接続を選択します。デスクトッププールで、デフォルトプロトコルを View Admin コンソールで **PCoIP**、ユーザーのプロトコル選択の許可を **no** と設定した場合、ユーザーがそのデバイスにサインインすると、このデスクトップは ThinOS に表示されません。
- **PCoIP のみ**—このオプションは、PCoIP が使用可能なクライアントにのみ利用できます。ブローカーの各プールに、PCoIP 接続のデスクトップのみ表示するには、このプロトコル接続を選択します。デスクトッププールで、デフォルトプロトコルを View Admin コンソールで **RDP**、ユーザーのプロトコル選択の許可を **no** と設定した場合、ユーザーがそのデバイスにサインインすると、このデスクトップは ThinOS に表示されません。
- **Blast のみ**——VMware Blast 表示プロトコルは、リモートアプリケーションに使用できます。また、RDS ホストの仮想マシンか共有セッションデスクトップを使用するリモートデスクトップにも使用できます。Blast プロトコルのデスクトップを表示するには、このプロトコル接続を選択します。

- **未認証のアクセスを使った匿名のログイン**——VMware セッションにリモートアプリケーションを使って匿名でログインするには、このチェックボックスをオンにします。

3 **OK** をクリックして設定を保存します。

VMware Horizon View ブローカーとデスクトップの使用

VMware Horizon View Broker timeout——VMware Horizon View Broker timeout では、安全なトンネルが有効な場合は、ユーザーはブローカーから強制的にサインオフされなくなります。

ThinOS の以前のバージョンでは、ブローカーがタイムアウトすると、ユーザーセッションは切断され、ユーザーがブローカーからログアウトされます。ThinOS 8.2 リリース以降、ThinOS によって、ユーザーセッションがブローカーから切断されても、ユーザーは強制的にログアウトされません。これは、ユーザーはブローカーデスクトップの他にローカル接続を使用し、ブローカーのタイムアウトに達したときにこれらの接続がアクティブになっているためです。

PCoIP セッションの NUM／CAP キーボードステータスは、シンクライアントではなくセッションと同期——これはセッション開始のみに利用できます。PCoIP セッションの NUM/CAP ステータスは、リモートセッションからクライアントに同期されますが、RDP/ICA は、ステータスをローカルからリモートセッションに同期します。

例：

1 現在の PCoIP セッションでキーボードの NUM キーをオフに設定します。
2 セッションを切断します。
3 クライアントキーボードの NUM キーをオンに設定します。
4 PCoIP セッションに再接続します。
5 セッションおよびクライアントの両方でキーボードの NUM ステータスがオフに更新されます。

RDS desktop through PCoIP/Blast——PCoIP/Blast を使用可能な ThinOS クライアントを使用し、ブローカーの PCoIP/Blast プロトコルを介して、リモートデスクトップサービス（RDS）デスクトップを表示したり、RDS デスクトップに接続したりすることができます。VMware Horizon View 6.0 以降のバージョンでは、RDS デスクトップは、サーバの構成によって、RDP、PCoIP、Blast のいずれかの接続を使用できます。

メモ：Horizon アプリケーションは、PCoIP および Blast の両方でサポートされます。RDP はサポートされません。

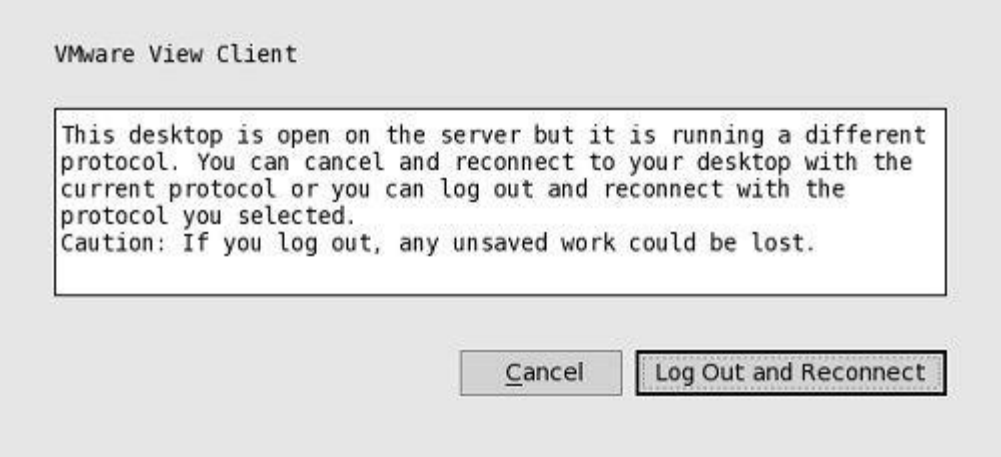
このリリースには、**RDS desktop protocol switch message** ダイアログボックスが備わっています。次に示すのは、一般的なユーザーシナリオです。

1 プロトコルを介して、RDS デスクトップに接続します。ここでは例として RDP を使用します。
2 デスクトップから切断します。
3 別のプロトコルを介して、同じ RDS デスクトップに接続します。ここでは例として PCoIP を使用します。
メッセージのダイアログボックスが表示され、オプションを選択して続行できます。

次のオプションを使用できます。

- **Cancel**——PCoIP 接続を終了し、もう一度 RDP でデスクトップに接続できます。
- **Log Out and Reconnect**——PCoIP を介してデスクトップに接続することができ、RDP を介した以前のセッションはログア

ウトされます。

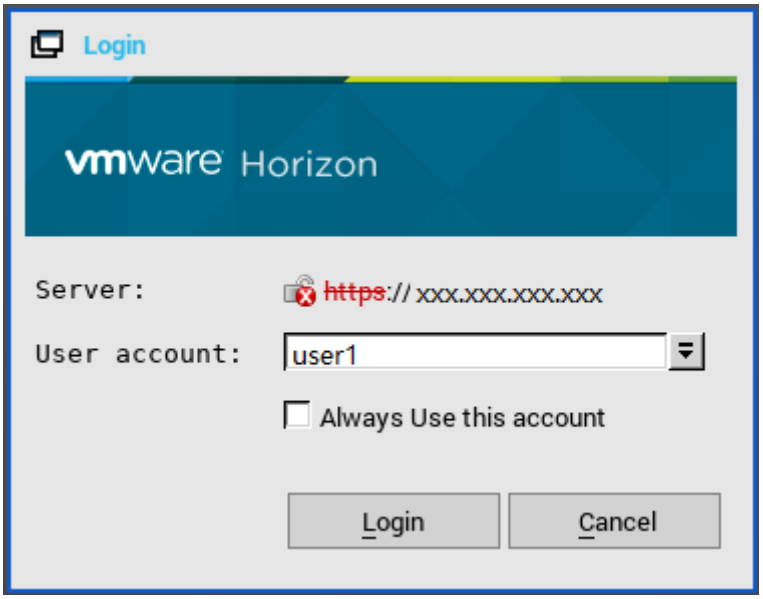


USB redirection RDS desktop through PCoIP/Blast——この機能はサポートされます。

Using unauthenticated access——VMware セッションにリモートアプリケーションを使って匿名でログインできます。

非認証オプションを使用するには、次の操作を行います。

1 AD サーバで、2 人の匿名ユーザー（たとえば、anonymous1、anonymous2）を作成します。
2 View Admin ウェブポータルにログインします。
3 **Users and Groups > Unauthenticated Access** と進んで、View 接続マネージャに新しい 2 人の匿名ユーザーを追加します。
4 **View Configurations > Select Servers > Connection Servers** と進んで、今お使いのコネクションサーバを選択します。
5 **Edit > Authentication** タブを順にクリックし、**Enabled for unauthenticated access** チェックボックスをオンにします。デフォルトの非認証ユーザーにはどのユーザーも選択しません。
6 **Application Pools** に進んで、Virtual Machine にインストールしたアプリケーションをいくつか選択し、匿名 1 と匿名 2 のユーザーに対しそのアプリケーションの使用権を付与します。
7 VMware View の **ThinOS ブローカー**ダイアログボックスで、**未認証のアクセスを使った匿名のログイン**チェックボックスをオンにします。
8 シンクライアントをリスタートします。
次のダイアログボックスが表示されます。



9 指定したログインアカウントを使用するために、**Always use this account** チェックボックスをオンにします。このログインアカウントを他のユーザーに変更することはできません。

Hide Server URL——サーバ URL は、Horizon View ブローカーUI で非表示にすることができます。次の方法のいずれかを使って、この設定を行うことができます。

- **View Connection Server ウェブポータルを使用する**
  a View Connection Server ウェブポータルにログインします。
  b **View Configuration > Global Settings > Edit** と順に進んで、**Hide server information in client user interface** チェックボックスをオンにし、**Hide domain list in client user interface** チェックボックスをオフにします。
  c **OK** をクリックします。
  d VMware Horizon ブローカーにログインします。
  サーバ URL は非表示で、ドメインリストは表示されます。
- **INI パラメータを使用する**
  INI パラメータ「ConnectionBroker=vmware DisableShowServer=yes」を使用します。

Hide Domain List——ドメインリストは、Horizon View ブローカーログオン UI で非表示にすることができます。この設定を行うには、次の操作を行います。

1 View Connection Server ウェブポータルにログインします。
2 **View Configuration > Global Settings > Edit** と順に進んで、**Hide domain list in client user interface** チェックボックスをオンにし、**Hide server information in client user interface** チェックボックスをオフにします。
3 **OK** をクリックします。
4 VMware Horizon ブローカーにログインします。
ドメインリストは非表示で、サーバ URL は表示されます。

VMware Real Time Audio-Video（RTAV）のサポート

Real-Time Audio-Video 機能を使って、リモートデスクトップで Skype などのオンライン会議アプリケーションを起動します。この機能を使用すると、シンクライアントに接続されたオーディオ、ビデオの両方のデバイスを、リモートデスクトップで VoIP に利用できます。

VMware Real Time Audio-Video のサポートの詳細については、pubs.vmware.com/horizon-62-view/topic/com.vmware.horizon-view.desktops.doc/GUID-D6FD6AD1-D326-4387-A6F0-152C7D844AA0.html を参照してください。

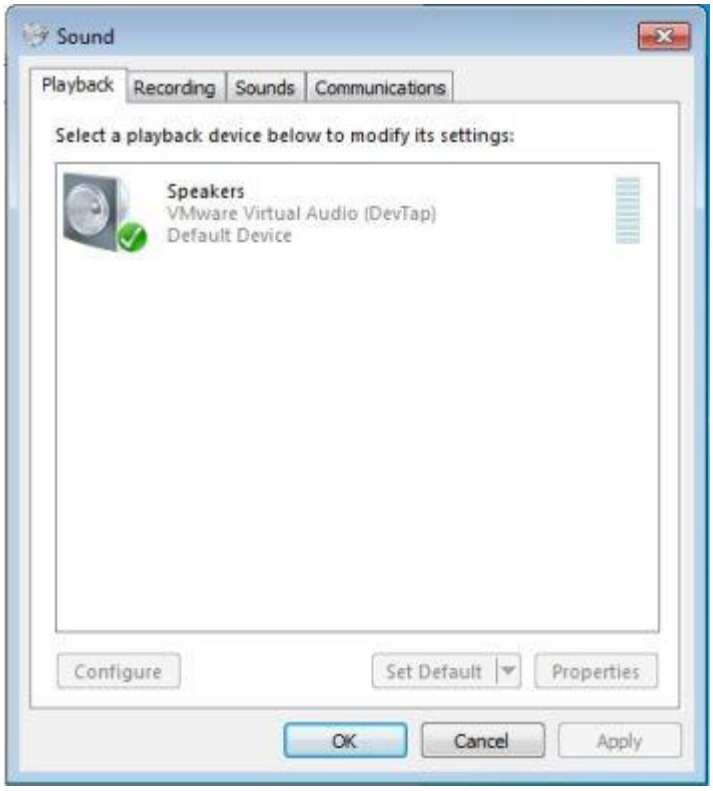
メモ：ThinOS の追加の設定はありません。RTAV ビデオでは、お使いのデバイスに RTME パッケージをインストールする必要があります。

VMware Real Time Audio-Video を確認するには、次の操作を行います。

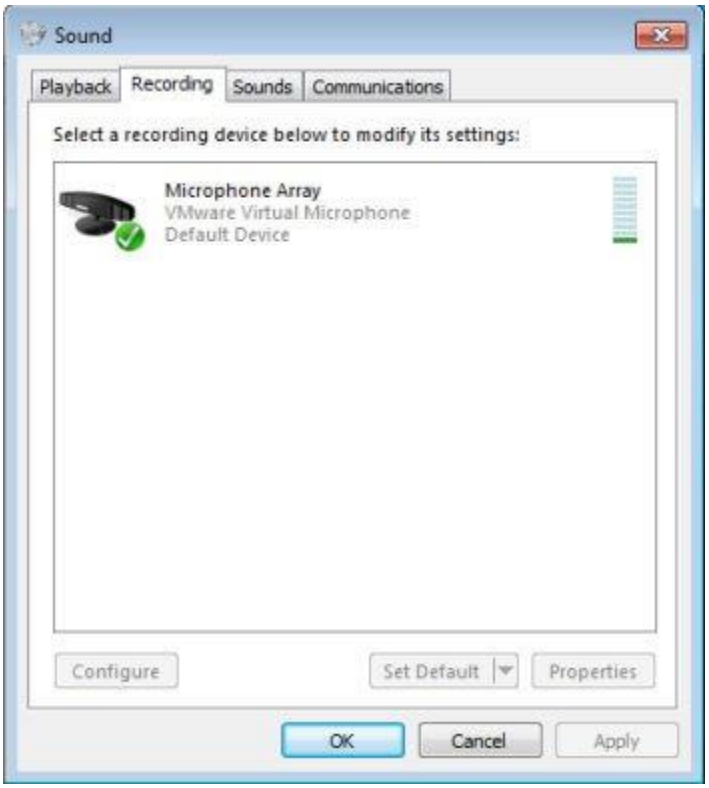
1 オーディオおよびビデオデバイスを接続した VMware PCoIP または Blast デスクトップに接続します。

メモ：USB リダイレクトはオーディオ／ビデオデバイスに対しては無効にする必要があります。

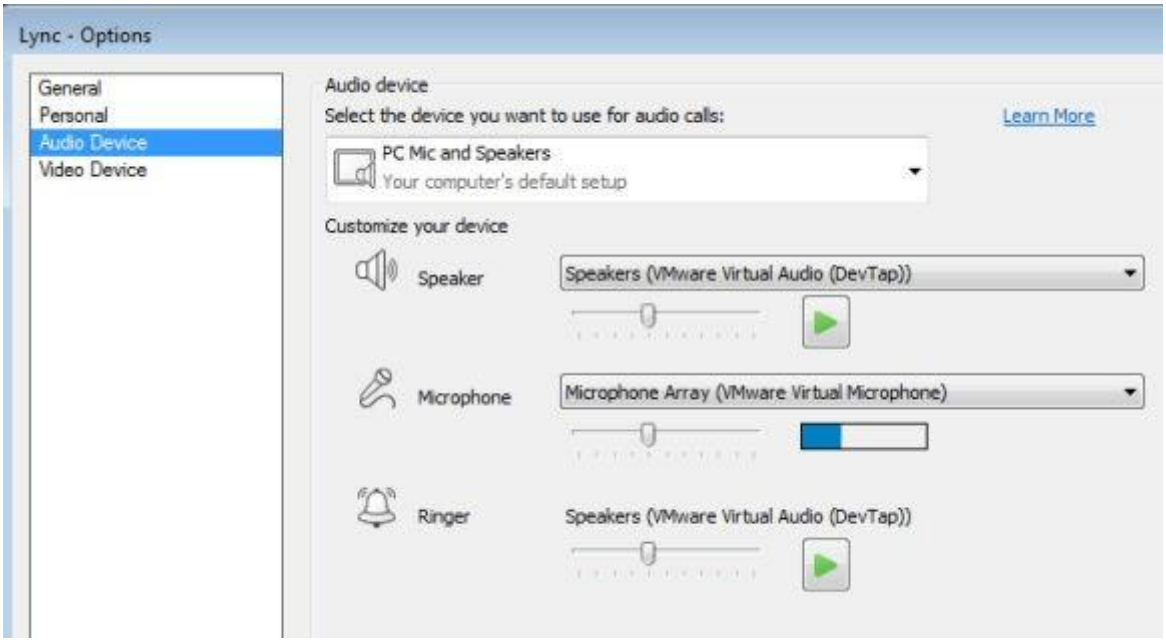
2 VMware の仮想オーディオを使用してシステムのオーディオ再生を確認します。



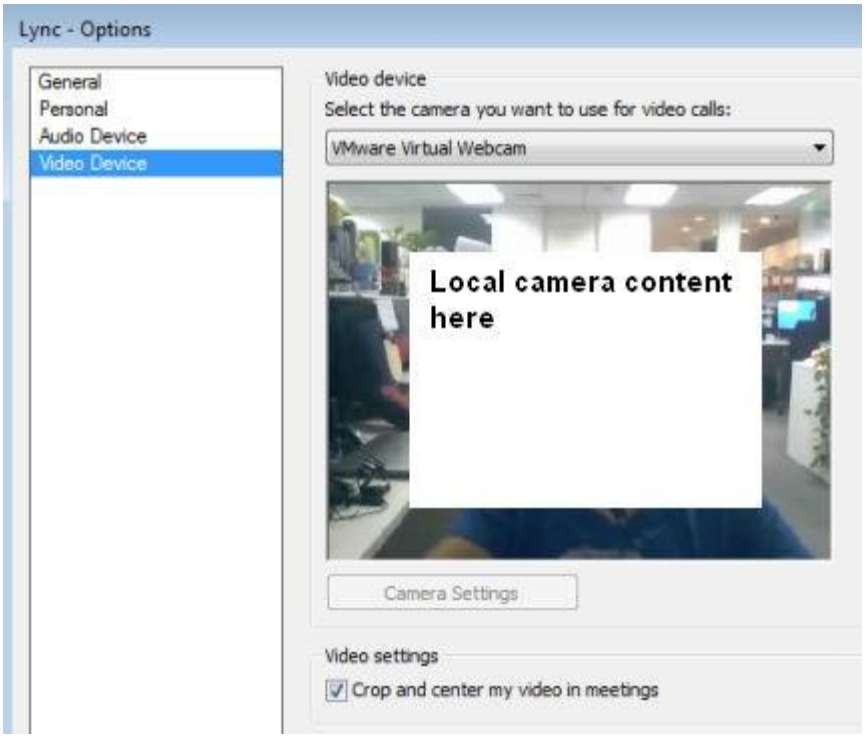
3 VMware の仮想マイクを使用してシステムのオーディオ録音を確認します。



4 VoIP アプリケーションのオーディオ設定を確認します。



5 VMware の仮想 Web カメラを使用して VoIP アプリケーションのビデオ設定を確認します。



6 音声通話またはビデオ通話を開始します。

依存関係と既知の問題

- 依存関係:RTAV ビデオには、RTME.i386.pkg をインストールする必要があります。
- ローカルのオーディオデバイスの応答ボタンは、HDX RTME ではサポートされていますが、RTAV ではサポートされていません。
- RTAV は RDS デスクトップをサポートしません（たとえば、VMware の場合は 2008 R2/2012 R2）。
- PCoIP および Blast プロトコルのみをサポートします。RDP プロトコルは VMware の場合はサポートされません。
- Web カメラ環境設定はサポートされていません。たとえば、ローカルの周辺機器設定の **Camera** タブに表示される第 1 Web カメラが、常に使用されます。
- カメラ／ビデオ：ハイ・デフィニション・ビデオは、RTAV の制限のためサポートされていません。アプリケーションの設計で考慮されているため、ローカルカメラの設定は RTAV に影響しません。デルはユーザーに、ローカルカメラの設定を変更しないことをお勧めします。

VMware Blast のサポート

VMware Blast 表示プロトコルは、リモートアプリケーションに使用できます。また、RDS ホストの仮想マシンか共有セッションデスクトップを使用するリモートデスクトップにも使用できます。Blast プロトコルのデスクトップを表示するには、このプロトコル接続を選択します。

メモ：接続アイコンにポインタを合わせると、対応する接続プロトコルがツールチップに表示されます。これは RDSH アプリケーション用に設計されています。ThinOS 8.4 リリース以降、PCoIP と Blast の両方のプロトコルに、RDSH アプリケーションがサポートされています。これら 2 つのプロトコルは、同じアプリケーションアイコンを共有しているので、プロトコルを見分けるには、接続アイコンにポインタを合わせる必要があります。

ThinOS の Blast 機能マトリックス

表 9. Blast 機能マトリックス

Blast 機能	ThinOS のサポート	コメント／既知の問題
H.264 オフロード	サポート	該当なし
VDI デスクトップ	サポート	該当なし
RDSH デスクトップ	サポート	該当なし
RDSH アプリケーション	サポート	Application ウィンドウはシームレスモードをサポートしません。たとえば、VMware の制限により、アプリケーションはすべて 1 つのウィンドウで開始します。
		RDSH アプリケーションは、PCoIP プロトコルを同じ制限でサポートします。
ユニファイドコミュニケーション	未サポート	サードパーティのプラグインは、予定されていません。
MS VDI プラグイン	未サポート	該当なし
RTAV	サポート	該当なし
Windows Media MMR	未サポート	該当なし
Flash URL マルチキャスト	未サポート	該当なし
プリンタリダイレクト	サポート	プリンタリダイレクト、および仮想プリントでのプリンタマッピングをサポートします。
スマートカードリダイレクト	サポート	該当なし
スキャナーリダイレクト	未サポート	該当なし
シリアルポートリダイレクト	未サポート	該当なし
USB リダイレクト——VDI/RDSH	サポート	デフォルトでは有効になっています。
クライアントドライブリダイレクト	未サポート	該当なし
Linux デスクトップ	サポート	該当なし

Blast 機能	ThinOS のサポート	コメント／既知の問題
Copy Paste テキスト	サポート	VMware Horizon のサーバとクライアントの設定とドキュメントを参照してください。
VPN 接続	サポート	該当なし
AES 128/256	サポート	ThinOS AES の設計に関する記事を参照してください。
デュアルディスプレイ／4K／32 ビット	サポート	VMware Blast のサポートに関する情報を参照してください。たとえば、前提条件は仮想マシンビデオ RAM です。
ClearType フォントのサポート	サポート	ThinOS は TrueType フォントをサポートします。
3D ディスプレイ	サポート	VMware Blast のサポートに関する情報を参照してください。
ネットワーク切断から Blast の復旧	サポート	Horizon View Agent 7.0.1 を必要とします。

VMware Horizon Blast の詳細については、VMware ドキュメントを参照してください。

ThinOS の Blast Virtual Printing（仮想印刷機能）の詳細については、「Blast Virtual Printing（仮想印刷機能）」を参照してください。

VMware Blast セッションでのマルチモニタのサポート

ThinOS はマルチモニタディスプレイをサポートし、各モニタでは仮想マシンが稼働します。
前提条件: VMware Blast パッケージを最新のバージョンにアップデートします。詳細については、最新の『Dell Wyse ThinOS リリースノート』を参照してください。
ユーザーのシナリオ：

1 マルチモニタを ThinOS デバイスに接続します。
2 システム設定のディスプレイダイアログボックスで、ミラーモードを無効にし、ディスプレイレイアウトを設定します。
3 フルスクリーンの VMware Horizon Blast セッションを開始します。

- **ディスプレイの数**——仮想マシンには、マルチモニタをサポートするための十分なビデオメモリを必要とします。十分な RAM を搭載したモニタを最大 4 台使用できます。

表 10. ディスプレイレイアウトマトリックス

解像度	1920×1080					2560 x 1440				
ディスプレイの数	2	3	4	5	6	2	3	4	5	6
水平	はい	はい	はい	該当なし	該当なし	はい	はい	はい	該当なし	該当なし
垂直	はい	はい	はい	該当なし	該当なし	はい	はい	はい	該当なし	該当なし
グリッド	はい	はい	はい	該当なし	該当なし	はい	はい	はい	該当なし	該当なし

- **4K ディスプレイ**——VMware Blast 表示プロトコルでは、リモートデスクトップで 4K（3840 x 2160）の画面解像度をサポートしています。サポートされる 4K ディスプレイの数は、デスクトップの仮想マシンのハードウェアバージョンと Windows バージョンに依存します。

表 11. 4K ディスプレイのサポート

ハードウェアバージョン	Windows バージョン	サポートされる 4K ディスプレイの数
10（ESXi 5.5.x 互換）	7、8、8.x、および 10	1
11（ESXi 6.0 互換）	7（3D レンダリング機能と Windows Aero が無効）	3
11	7（3D レンダリング機能が無効）	1

ハードウェアバージョン	Windows バージョン	サポートされる 4K ディスプレイの数
11	8、8.x、および 10	1

- **3D レンダリング**——接続したデスクトップに 3D グラフィックスのレンダリングを設定できます。3D レンダリング機能を使用するには、最大 1920 x 1200 の解像度のモニタを最大 2 台使用します。4K（3840 x 2160）の解像度については、モニタは 1 台だけサポートされます。
- **Blast H.264**——次の表には、VMware Blast 表示プロトコルを使用する VMware Horizon セッションの H.264 デコーダのパフォーマンスが記載されています。

表 12. Blast H.264 デコード

VMware の画面解像度 Horizon Blast セッション	VMware Horizon の Blast H.264 デコード Blast セッション	要約
セッションの表示幅は 1920 ピクセル以下です。	Blast H.264 デコードは常に有効です。	H.264 デコーダ設定が GUI または INI オプションを使って無効化されていても、Horizon クライアントは Blast H.264 デコードを使用します。
セッションの表示幅は 1920 ピクセルを超えます。	Blast H.264 デコードはデフォルトでは無効です。ThinOS GUI を使用するか、INI パラメータをデプロイすることにより、Blast H.264 デコードを有効にできます。	Horizon クライアントは、デフォルトでは Blast H.264 デコードを使用しません。Blast H.264 デコーダ設定が ThinOS で有効である場合、Horizon クライアントは H.264 デコードを使用します。H.264 を有効にすると セッションのパフォーマンスが低下する場合があります。

PCoIP セッションでのマルチモニタのサポート

ThinOS はマルチモニタディスプレイをサポートし、各モニタでは仮想マシンが稼働します。
ユーザーのシナリオ：

1 マルチモニタを ThinOS デバイスに接続します。
2 システム設定のディスプレイダイアログボックスで、**ミラーモード**を無効にし、ディスプレイレイアウトを設定します。
3 フルスクリーンの PCoIP セッションを開始します。

- **ディスプレイの数**——仮想マシンには、3 台または 4 台のマルチモニタをサポートするための十分なビデオメモリを必要とします。VMware vSphere のデフォルトのビデオメモリは、2 台のモニタしかサポートしません。
  – 解像度が最大 2560 x 1600 のスパンモードで、1 セッション最大 4 台のモニタをサポートします。
  – 解像度が最大 3840 x 2160 のスパンモードで、1 セッション最大 2 台のモニタをサポートします。

  垂直に積み重ねられるモニタの数は、最大 2 台です。3 台以上のモニタを使用する場合、モニタは同じモードとし、画面解像度も同じにする必要があります。たとえば、モニタが 3 台の場合、3 台のモニタはすべて、ポートレートモードかランドスケープモードのいずれかにする必要があり、同じ画面解像度を使用する必要があります。
- **ディスプレイレイアウト**——モニタのディスプレイレイアウトは、上下または左右に位置合わせをする必要があります。位置合わせが不適切であると、表示がおかしくなります。
- **3D レンダリング**——接続したデスクトップに 3D グラフィックスのレンダリングを設定できます。3D レンダリング機能を使用するには、最大 1920 x 1200 の解像度のモニタを最大 2 台使用します。

表 13. マルチスクリーンサポートのマトリックス

PCoIP Multi モニタサポート																
Wyse 5070 Extended シンクライアント																
ディスプレイレイアウト	解像度	1920×1200					2560 x 1440					3840 x 2160				
	ディスプレイの数	2	3	4	5	6	2	3	4	5	6	2	3	4	5	6

PCoIP Multi モニタサポート																
Wyse 5070 Extended シンクライアント																
	水平	はい	はい	はい	該当なし	該当なし	はい	はい	はい	該当なし	該当なし	はい	該当なし	該当なし	該当なし	該当なし
	垂直	はい	はい	はい	該当なし	該当なし	はい	はい	はい	該当なし	該当なし	はい	該当なし	該当なし	該当なし	該当なし
	グリッド	該当なし	はい	はい	該当なし	該当なし	該当なし	はい	はい	該当なし	該当なし	該当なし	該当なし	該当なし	該当なし	該当なし
ディスプレイレイアウト	解像度	1920×1200					2560 x 1440					3840 x 2160				
	ディスプレイの数	2	3	4	5	6	2	3	4	5	6	2	3	4	5	6
	水平	はい	はい	該当なし	該当なし	該当なし	はい	はい	該当なし	該当なし	該当なし	はい	該当なし	該当なし	該当なし	該当なし
	垂直	はい	はい	該当なし	該当なし	該当なし	はい	はい	該当なし	該当なし	該当なし	はい	該当なし	該当なし	該当なし	該当なし
Wyse 5070 シンクライアント——Celeron																
ディスプレイレイアウト	解像度	1920×1200					2560 x 1440					3840 x 2160				
	ディスプレイの数	2	3	4	5	6	2	3	4	5	6	2	3	4	5	6
	水平	はい	該当なし	該当なし	該当なし	該当なし	はい	該当なし	該当なし	該当なし	該当なし	はい	該当なし	該当なし	該当なし	該当なし
	垂直	はい	該当なし	該当なし	該当なし	該当なし	はい	該当なし	該当なし	該当なし	該当なし	はい	該当なし	該当なし	該当なし	該当なし

Blast Virtual Printing（仮想印刷機能）

VMware Blast の仮想印刷機能によって、リモートデスクトップにプリンタドライバを追加インストールしなくても、Blast デスクトップからローカルプリンタまたはネットワークプリンタが使用できます。ThinOS でローカルに設定された各プリンタについては、プリンタを VMware Blast デスクトップにマップする必要があります。ThinOS Blast プリンタマッピングは、VMware Blast 仮想印刷機能に相当します。

お使いのプリンタをマップするには、次の操作を行います。

メモ：LPT プリンタは、プリンタマッピングのシナリオを説明する一例です。ThinOS のプリンタマッピングは、LPD プリンタおよび SMB プリンタに対する LPT と同様の働きをします。

1 VMware View ブローカーを搭載し、**ブローカー**タブで設定した ThinOS クライアントの電源をオンにします。**接続プロトコル**ドロップダウンリストで、接続プロトコルを**利用可能な組み合わせ全て**と設定します。

2 接続マネージャの**接続設定全般 > 前セッション共通**に順に進み、**プリンタデバイスを除外項目の**チェックボックスをオンにしておきます。このオプションはデフォルトでオンになっています。

3 USB プリンタのプラグを ThinOS クライアント端末に差し込みます。

4 **システム設定 > プリンタ**に進みます。
プリンタ設定ダイアログボックスが表示されます。

5 **プリンタ設定**ダイアログボックスで次の操作を行います。

   a **ポートの選択**ドロップダウンリストで **LPT 1** を選択します。

   b プリンタ名とプリンタ ID を正しく入力します。

   c **プリンタデバイスを有効にする**チェックボックスをオンにします。

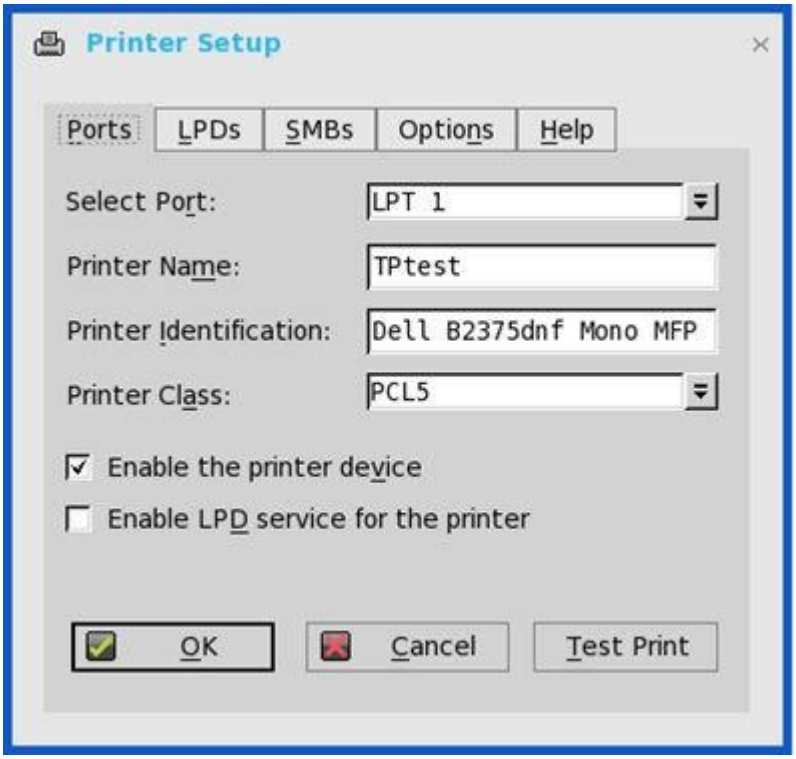


図 9.　　プリンタ設定

d　**Ok** をクリックし設定を保存します。

6　**オプション**タブをクリックし、次の操作を行います。

a　**LPT1: <プリンタ名>**をデフォルトプリンタとして設定します。

> **メモ：.print クライアントを有効にするの「チェックボックスはオンにしません。**

b　**Ok** をクリックし設定を保存します。

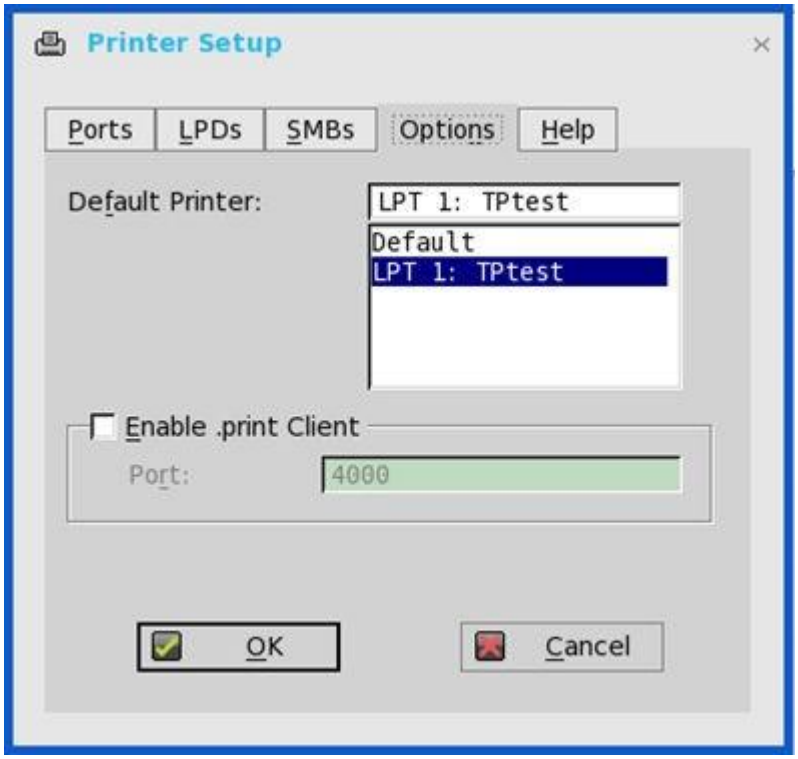


図 10.　オプション

7　VMware Blast セッションに接続します。**Control Panel > Devices and Printers** に進みます。ThinOS でローカルに設定されたプリンタは、このセッションにマップされます。

マップされたプリンタのドライバは TP PS Driver で、ポートは TPVM ポートです。

仮想プリンタによって、ThinOS ローカルプリンタは、そのセッションでプリンタドライバをインストールしなくても、VMware Blast セッションにマップされます。

Teradici SDK のサポート

PCoIP Client Software Development Kit（SDK）は、PCoIP クライアントのビルドやカスタマイズに利用できる一連のライブラリとバイナリです。

ThinOS は、Teradici SDK バージョン 2.9 をサポートします。

ユーザーのシナリオ：

- Teradici SDK の初期のバージョンの動作:セッション間で USB ディスクの出力先を切り替えることができました。たとえば、USB ディスクを差し込んで、デスクトップ 1 と 2 に接続します。USB ディスクの出力先はデスクトップ 1 です。デスクトップ 1 を切断すると、USB ディスクはデスクトップ 2 に出力先を変更します。
- Teradici SDK バージョン 2.9 の動作:デスクトップ 1 を切断しても、USB ディスクはデスクトップ 2 に出力先を変更しません。出力先を変更するには、USB ディスクを抜いて、再度差し込む必要があります。

Microsoft リモートデスクトップの設定

Microsoft リモートデスクトップのアプリケーションによって、インターネット接続を使用して、リモートデバイスのデータとリソースにアクセスし、管理することができます。

このセクションでは、リモートデスクトップブローカー接続を ThinOS デバイスに設定する方法と、ThinOS に設定できるその他のリモートデスクトップの機能について説明します。

Microsoft リモートデスクトップブローカー接続の設定

Microsoft リモートデスクトップのブローカー設定を設定するには：

1 デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。
リモート接続設定ダイアログボックスが表示されます。
2 **ブローカー**タブでは、ドロップダウンリストで Microsoft を選択し、次の操作を行います。

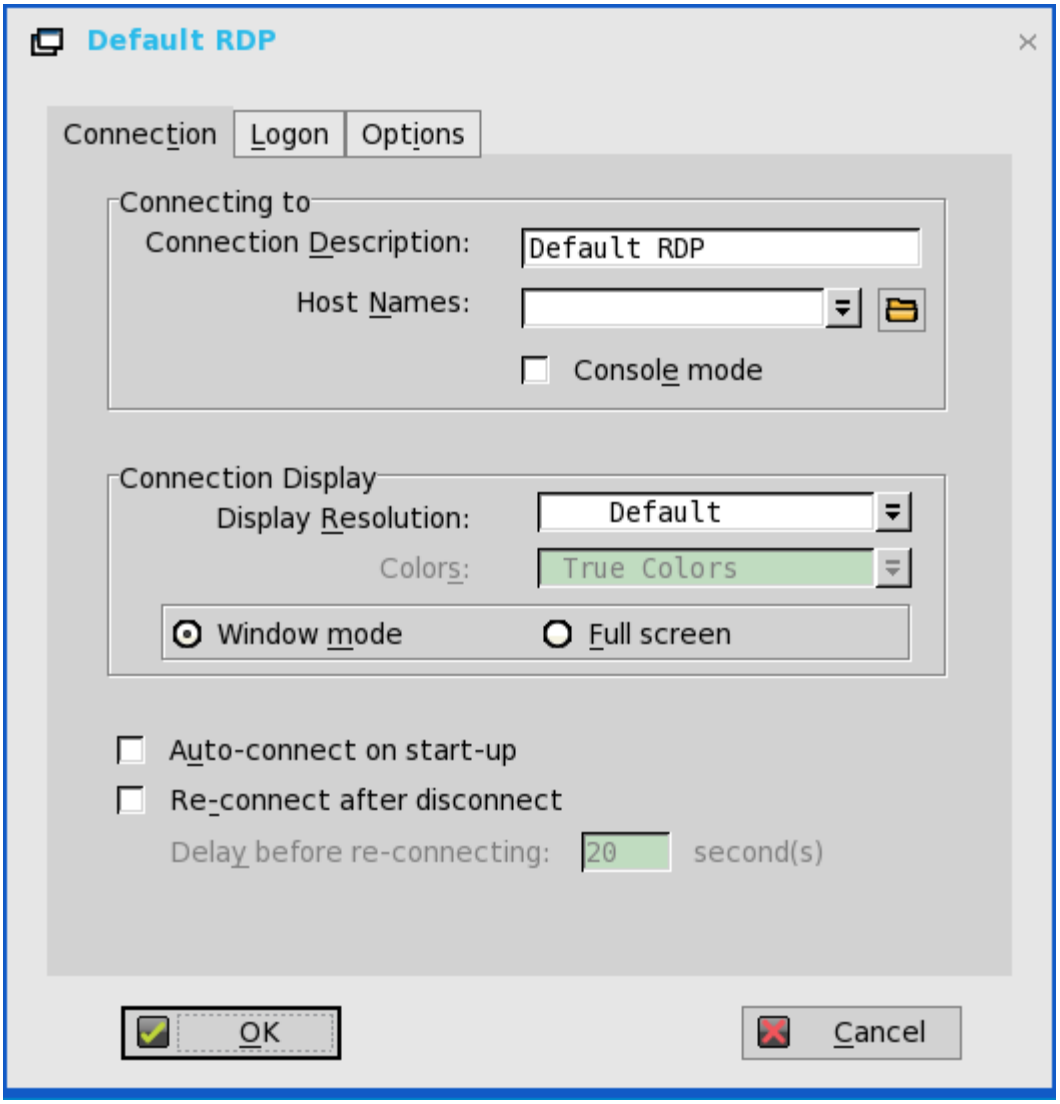
- **ブローカーサーバ**——ブローカーサーバの IP アドレス／ホスト名／FQDN を入力します。
- **自動接続リスト**——個別のブローカーにログイン後、自動的に起動させたいデスクトップの名前を入力します。複数のデスクトップの入力が可能です。各デスクトップの名前はセミコロンで区切り、大文字と小文字は区別します。

3 **OK** をクリックして設定を保存します。

RDP 接続の設定

リモート接続設定で選択した RDP 接続オプションを設定するには

1 デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。
リモート接続設定ダイアログボックスが表示されます。
2 **ブローカー**タブでは、ドロップダウンリストで**ブローカータイプ**を**なし**と選択します。
3 通信プロトコル選択にて **RDP** をクリックし、**接続設定の編集**をクリックします。
Default RDP ダイアログボックスが表示されます。
4 **接続**タブをクリックし、次のガイドラインに従います。



a **接続の説明**——接続リストに表示するわかりやすい名前を入力します（最大 38 文字）。

b **ホスト名**——リストを使用して有効な DNS サーバ名またはシンクライアントが接続するサーバの IP アドレスを選択します。ボックスの横にある **Browse アイコン**を使用しても、希望する選択ができます。たとえば、ローカルネットワーク上の WTS サーバのリストから選択できます。

> ⓘ **メモ：サーバ名は、2 つのメカニズム（DNS と WINS）のいずれかを使用して解決できます。DNS は、ネットワークコントロールパネルのデフォルトドメイン名を使用して、FQDN を作成しようとしますが、デフォルトを使用しない名前の解決も試みます。**

c **コンソール接続**——オンにすると、Windows コンソールモードで RDP 接続を設定します。

d **解像度**——この接続の画面解像度を選択します。

色—

RDP セッションの表示色を選択できます。High Colors（16 bits）または True **Colors**（32 bits）が選択されていて、RDP サーバがその表示色をサポートしていない場合、シンクライアントは表示色を 256 Colors（8 bits）などの低い値に調整します。ハードウェアがサポートしている場合、最大は 32 ビットです。

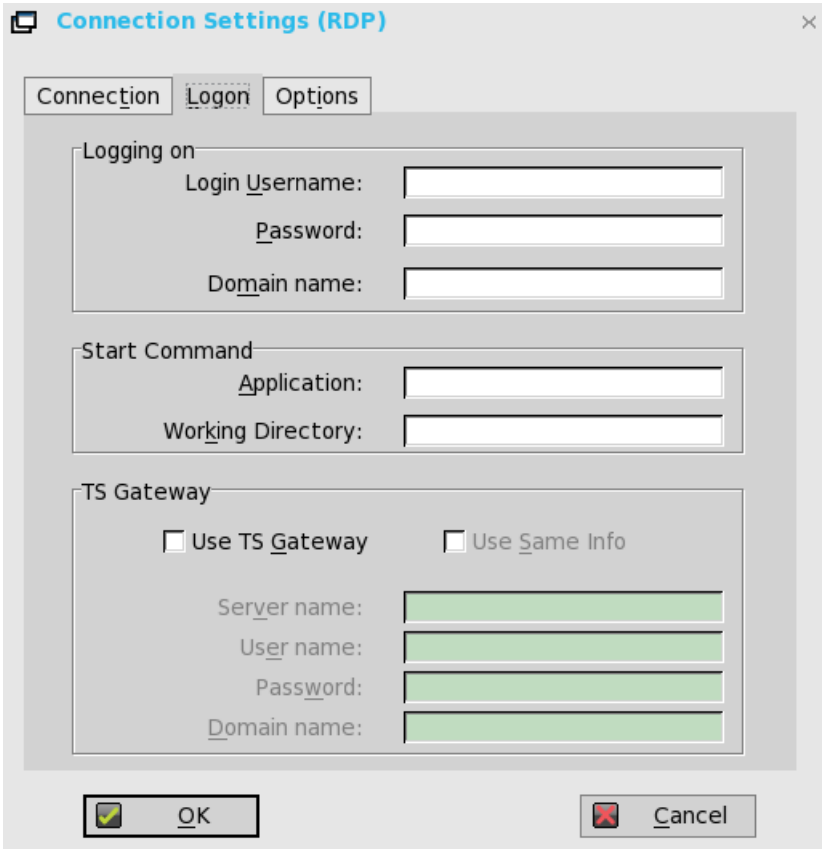
e **ウィンドウモード**または**全画面モード**——セッションの最初の表示を、ウィンドウモードにするか、フルスクリーンモードにするかを選択します。

f **起動時に自動接続**——オンにすると、起動時にセッションが自動接続されます。

g **切断後に再接続**——オンにすると、操作者以外によって切断された後で、シンクライアントをセッションに自動で再接続します。オンにすると、待機間隔は**再接続前に遅延**ボックスに設定した間隔（1～3600 秒で入力）か、ユーザープロファイルに設定した Yes の場合の間隔（20 秒）または秒単位の間隔です。この接続の記述が INI ファイルにない場合や、スタンドアロンユーザーがいる場合、単に省略されている場合は、デフォルトは 20 秒です。

オプションは、接続の設定（**RDP**）ダイアログボックスの**接続**タブでリセットできます。そのためには、Reset VM コマンドボタンをクリックします。このコマンドボタンは、ダイアログボックスの右上に表示されます。このボタンは、VDM ブローカー接続でのみ表示されます。

5 **ログオン**タブをクリックし、次のガイドラインに従います。



a **ログオン設定**——Login Username、Password、および Domain name に入力します。これらのボックスに入力されていない場合は、接続時に RDP サーバログイン画面に情報を手動で入力できます。次のガイドラインに従います。

- **ユーザ名**——最大 31 文字まで入力できます。
- **パスワード**——最大 19 文字まで入力できます。
- **ドメイン名**——最大 31 文字まで入力できます。

b **アプリケーション**（最大 127 文字）と**作業ディレクトリ**（最大 63 文字）——関連付けられた作業ディレクトリなど、接続時に自動的にサーバ上で開始する初期化文字列と引数を入力します。

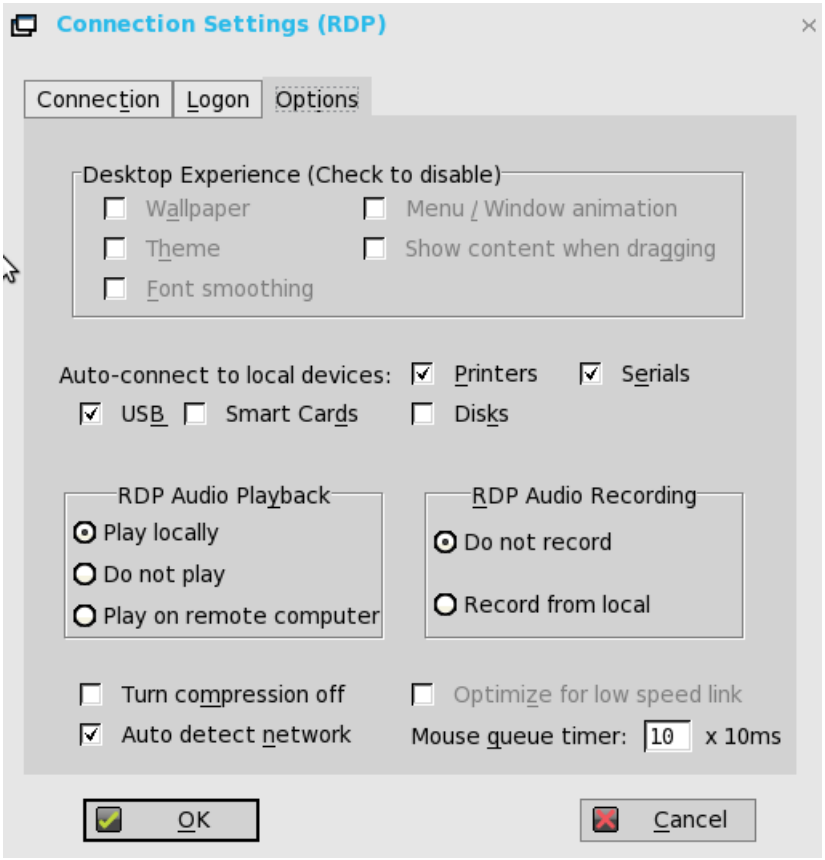
c **TS Gateway 利用**——接続時にターミナルサービスゲートウェイ（TS ゲートウェイ）を使用可能にします。必要に応じて、TS ゲートウェイサーバの IP アドレスまたは URL をサーバボックスに入力します。**同じ認証情報を利用の項目**を有効にするか（サーバの資格情報がユーザ、パスワードおよびドメインフィールドのリモートデスクトップの資格情報（ホストリモートコンピュータの資格情報）と同じ場合）、**同じ認証情報を利用の項目**を無効にして、必要に応じて TS ゲートウェイサーバのサーバ、ユーザ、パスワードおよびドメイン名を入力することができます。

> **メモ：TS ゲートウェイサーバはゲートウェイの一種で、権限のあるユーザーがインターネット接続を使用して任意のコンピュータから企業ネットワーク上のリモートコンピュータに接続できるようにします。TS ゲートウェイサーバを使用すると、仮想プライベートネットワーク（VPN）接続を設定しなくても、インターネットから企業ネットワークへのリモートデスクトップ接続が可能となります。TS ゲートウェイサーバを指定する必要性については、ネットワーク管理者に問い合わせてください。**

- **ユーザ**——接続のユーザー名を入力します。
- **パスワード**——パスワードを入力します。
- **ドメイン**——ドメイン名を入力します。

> **メモ：ユーザ、パスワードおよびドメインフィールドはオプションです。これらのフィールドのいずれかを空白にすると、インタラクティブなログインが必要となり、ユーザはログイン時に情報を入力する必要があります。**

6 **オプション**タブをクリックし、次のガイドラインに従います。



a **壁紙**——オンにすると、デスクトップの壁紙を無効にします。

b アニメーション表示——オンにすると、メニューまたはウィンドウのアニメーションを無効にします。

c **テーマ**——オンにすると、デスクトップのテーマを無効にします。

d **ウィンドウ内容のドラック**——デフォルトでは、ウィンドウのタイトルバーをつかんで移動すると、ウィンドウの内容も一緒に移動します。これをオンにすると、ウィンドウの内容の表示を無効にし、ドラッグしている間はウィンドウをドロップするまで、ウィンドウの輪郭だけが移動します。このオプションは処理能力の消費を抑えるため、役立ちます。

e **フォントスムージング**——ベクトルテキストをビットマップに変換して、見やすくします。

f **ローカルデバイスに自動接続**——任意のオプション（プリンタ、シリアル、USB、スマートカード、およびディスク）を選択し、シンクライアントがこれらのデバイスに自動的に接続するようにします。

> ⓘ **メモ：USB——シンクライアント上でローカル接続されている USB デバイスを Microsoft Windows ターミナルサーバにリダイレクトします。ユーザーがターミナルサーバに接続すると、シンクライアント上でローカル接続された USB デバイスにアクセスできます。**

g **RDP オーディオ再生**——ローカルで再生、再生しないおよびリモートコンピュータという音声再生オプションを選択します。

h **RDP オーディオ録音**——録音しないおよびローカルデバイスから録音という音声録音オプションを選択します。

i **圧縮を無効化**——オンにすると、圧縮をオフにします（高速接続が対象です）。

j **低速回線に最適化**——オンにすると、音声品質を下げたり、プロトコル専用のキャッシュサイズを減らしたりするなど、低速接続に最適化できます。WAN リンクをまたぐ接続やダイアルアップを使用する接続を対象としています。

k **回線速度自動検出**——オンにすると、自動検出ネットワーク機能がオンになります。デフォルトではこの機能が有効です。この機能は、デフォルトで低速回線に最適化オプションと Desktop Experience のオプションを無効にします。

l **マウスキュー**——ICA または RDP セッションにおけるマウスイベントのデフォルトのキュータイマーを指定します（1/100 秒単位です）。この機能を使用すると、ネットワークの帯域幅を調整できます。

7 **OK** をクリックして設定を保存します。

RDP プロトコルの機能

Remote Desktop Protocol（RDP）は、Microsoft によって開発されたネットワーク通信プロトコルで、仮想デスクトップとアプリケーションへのリモートアクセスを可能にするものです。このセクションでは、RDP プロトコルで接続する ThinOS の機能について説明します。

RDP セッションでのマルチモニタのサポート

ThinOS はマルチモニタディスプレイをサポートし、各モニタには RDP デスクトップを起動します。
ユーザーのシナリオ：

1 複数のモニタを ThinOS デバイスに接続します。
2 **システム設定のディスプレイの**ダイアログボックスで、**ミラーモード**を無効にし、ディスプレイレイアウトを設定します。
3 RDP デスクトップをフルスクリーンで立ち上げます。

次の表に記載されているすべてのデータは、RemoteFX/vGPU が有効に設定されていない仮想マシンに基づいたものです。

表 14. RDP 表示能力マトリックス

デスティネーションエンドポイント	モニタあたりの最大解像度[Enable Force Span]	最大表示サポート[Span Monitors]
Windows 7 SP1	4096（幅）x 2048（高さ）	4096（幅）x 2048（高さ）
Windows 8.1	8192 x 8192	6 x 4K
Windows Server 2012 R2	8192 x 8192	6 x 4K
Windows 10	8192 x 8192	6 x 4K
Windows Server 2016	8192 x 8192	6 x 4K

RDP H.264

ThinOS バージョン 8.5.1 では、H.264 と H.264-AVC444 のログは非表示で、**イベントログ**タブには表示されません。

次の表には RDP H.264 の機能マトリックスが記載されています。

表 15. RDP H.264 機能マトリックス

RDP セッション	Microsoft ブローカー2012 R2	Microsoft ブローカー2016	H.264 有効の場合の解像度
Windows 8.1/ 2012 R2	H.264 を使用	H.264 を使用	>= 576 x 576 および <= 2048 x 1280
Windows 10/ 2016	H.264 は不使用	H.264-AVC444 を使用	>= 576 x 576 および <= 3840 x 2160

次の表には RDP H.264 のデコードマトリックスが記載されています。次の表に記載されているすべてのデータは、RemoteFX/vGPU が有効に設定されていない仮想マシンに基づいたものです。

表 16. RDP H.264 デコードマトリックス（Wyse 5070 シンクライアント）

ユニットタイプ	GPU	セッション	Windows 10/Windows Server 2016		Windows 8.1/Windows Server 2012 R2	
		ディスプレイ解像度	H.264-AVC444	デコード	H.264	デコード
Wyse 5070 Extended シンクライアント	AMD	3840 x 2160	有効	ソフトウェア	無効	
		2560 x 1440	有効	ソフトウェア	無効	
		2048 x 1280	有効	ソフトウェア	有効	ハードウェア
		1920×1200	有効	ソフトウェア	有効	ハードウェア
	Intel	3840 x 2160	有効	ソフトウェア	無効	
		2560 x 1440	有効	ソフトウェア	無効	
		2048 x 1280	有効	ソフトウェア	有効	ハードウェア
		1920×1200	有効	ソフトウェア	有効	ハードウェア
Wyse 5070 シンクライアント—Celeron Processor Wyse 5070 シンクライアント—Pentium Processor	Intel	3840 x 2160	有効	ソフトウェア	無効	
		2560 x 1440	有効	ソフトウェア	無効	
		2048 x 1280	有効	ソフトウェア	有効	ハードウェア
		1920×1200	有効	ソフトウェア	有効	ハードウェア

メモ：

- Windows 10/Window Server 2016 は、H.264-AVC444 を有効にするために、Microsoft RDS 2016 ブローカーで提供される必要があります。
- H.264 のログと H.264-AVC444 のログは非表示で、**イベントログ**タブには表示されません。

既知の問題

- アクティブなセッションのミラーモードで、解像度を 2048 x 1280 以上に変更すると、接続された RDP セッション（Windows 8/Windows 2012 R2）が強制終了し、エラーメッセージ「**RDP:サーバ側のグラフィックサブシステムはエラー状態で、グラフィックスのエンコードを継続できません**」が表示されます。これは、H.264 コーデックにサポートされている解像度を超えるような解像度の変更をすると、セッションはミラーモードでは再接続できないためです。

  回避策——解像度変更後、手動でセッションを再接続する必要があります。

- デフォルトで有効な VOR を使用した RDP セッションでは（Windows 8.1 x86）、フルスクリーンでセッションに接続し、それを 5 台以上の 4K モニタに拡大します。このシナリオでは、ビデオを再生すると、エラーログ「**RDP:サーバ側のグラフィックサブシステムはエラー状態で、グラフィックスのエンコードを継続できません**」を出力して、セッションが自動的に切断される場合があります。これは VOR/x-264 が、サーバのリソースより多くの RAM などのリソースを必要するからです。

  回避策——モニタの数を減らしたり、解像度を下げたり、さらに多くの RAM を搭載した 64-ビットオペレーティングシステムに切り替えることが可能です。

RDP 10 セッションの H.264 AVC444 の設定

前提条件：

- シンクライアントは、ThinOS バージョン 8.5 以降で稼働させる必要があります。
- Windows 10 または Windows Server 2016 は、Microsoft RDS 2016 ブローカーまたは最新の VMware View ブローカで作成する必要があります。

RDP 10 セッションの H.264 AVC444 を設定するには：

1 Windows セッションのホストで、**gpedit.msc** を実行します。
2 Local Group Policy Editor を開始します。
3 **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment** の順に進み、次のポリシーを有効にします。

- リモートデスクトップ接続の H.264/AVC 444 Graphics モードの優先順位を決めます。
- リモートデスクトップ接続の H.264/AVC ハードウェアエンコードを設定します。

4 cmd.exe を開始して gpupdate /force を実行するか、サーバを再起動します。

RDP セッションの VOR コーデック

RDP セッションでビデオを再生しているときは（Windows 8.1、Windows 2012 R2、Windows 10 および Windows 2016）、VOR コーデックが使用されます。次のログが**イベントログ**タブに表示されます。

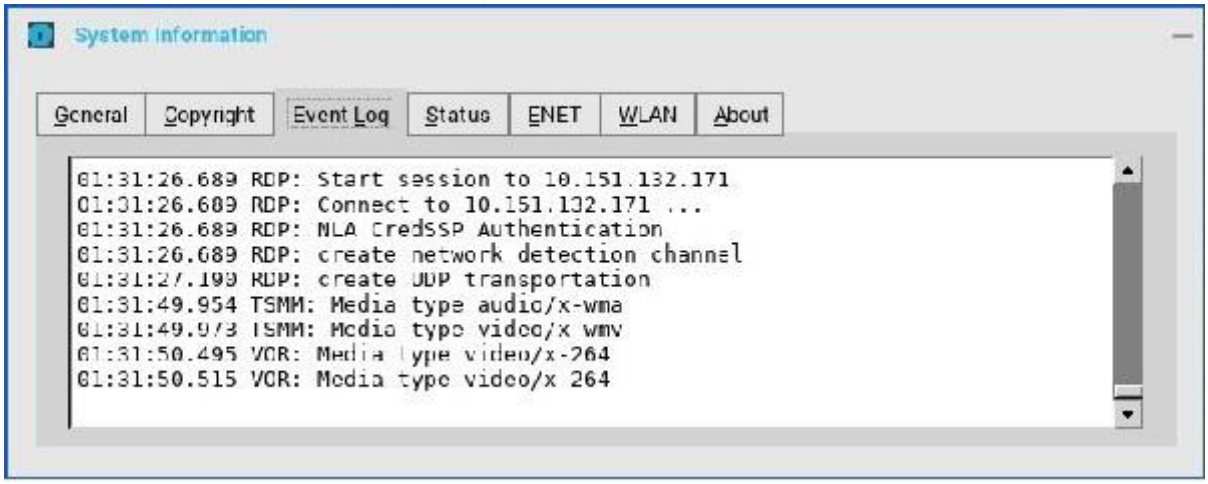


図 11.　イベントログタブ

メモ：

- 依存関係 1——RDP GFX ステータス、H.264 および VOR は、GFX が有効の場合のみ機能します。
- 依存関係 2——VOR は動的です。このため、ビデオの解像度が変化（拡大／縮小）すると、VOR の有効化／無効化が動的に変化します。
- 依存関係 3——H.264 の有効化は、接続開始時に、そのセッションで利用可能な最大解像度によって決定されます。
- Microsoft ブローカー2016 および Windows 10/2016 のセッションでは、H.264-AVC444 が有効であると、VOR は使用されません。H.264- AVC444 を無効にすると、VOR が使用されます。

RDP セッション（RDP 8.1 以降）では、VOR、H.264 および H.264-AVC444 はデフォルトで有効です。これらのパラメータを無効にするには、次の ini パラメータを使用します。SessionConfig-RDP EnalbeGFX=yes EnableVOR=no EnableRDPh264=no.

Microsoft ブローカーの TS Gateway

ユーザーのシナリオ：

1 TS Gateway が設定された Microsoft ブローカーにログインします。
2 公開済みのコレクションを起動します。
TS Gateway 接続が確立されます。

次の表には、Windows サーバでサポートされている TS Gateway のバージョンが記載されています。

表 17.　サポート対象の TS Gateway バージョン

サーバのオペレーティングシステム	TS Gateway II	TS Gateway III	WebSocket
Windows 2008 R2	サポートする	サポートしない	サポートしない
Windows 2012 R2	サポートする	サポートする	サポートしない

サーバのオペレーティングシステム	TS Gateway II	TS Gateway III	WebSocket
Windows 2016	サポートする	サポートする	サポートする

メモ：

- TS Gateway II または III の接続の設定では、Terminal Server (TS) Gateway サーバとシンクライアントの間は、半二重通信を 2 本使用します。
- WebSocket 接続では、セッション接続の設定で、TS Gateway とシンクライアントの間は、二重通信を使用します。
- TS Gateway II および TS Gateway III は、Windows Server 2016 と下位互換性があります。つまり、WebSocket 接続が失敗した場合や、TS Gateway サーバまたはシンクライアントのバージョンで WebSocket をサポートしない場合は、TS Gateway II または TS Gateway III が使用されます。

次のスクリーンショットには、TS Gateway II 接続の設定ログが表示されています。

図 12.　イベントログタブ

次のスクリーンショットには、TS Gateway III 接続の設定ログが表示されています。

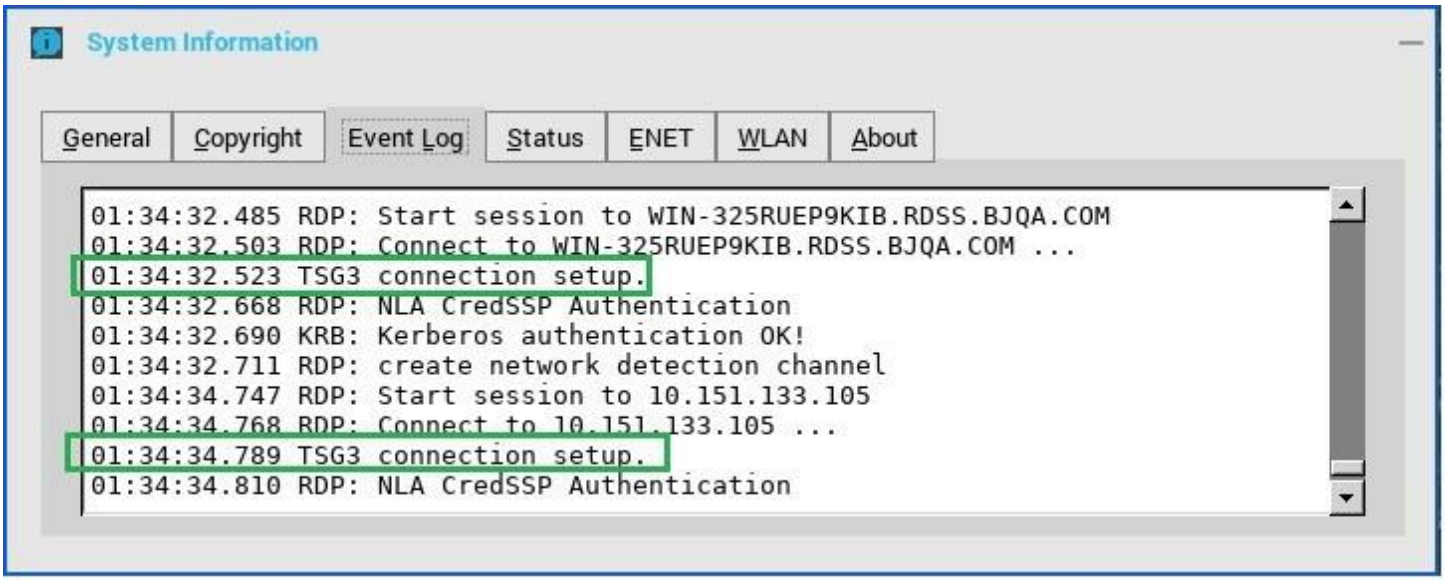


図 13.　イベントログタブ

メモ：WebSocket 接続のログは非表示で、イベントログタブには表示されません。

Dell vWorkspace の設定

Workspace Virtualization では、アプリケーションまたはデスクトップのカタログを、1 つの完全な仮想ワークスペースとして提供します。これはコンピュータのワークスペース全体を分離し一元化するものです。vWorkspace は、複数の仮想プラットフォームから仮想ワークスペースを提供することで、場所やプラットフォームに依存しない柔軟なアクセスを実現します。

このセクションでは、Dell vWorkspace ブローカー接続を ThinOS デバイスに設定する方法について説明します。

Dell vWorkspace ブローカー接続の設定

vWorkspace ブローカー設定を設定するには：

1 デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。
リモート接続設定ダイアログボックスが表示されます。
2 **ブローカー**タブでは、ドロップダウンリストで **Dell vWorkspace** を選択し、次の操作を行います。

- **ブローカーサーバ**——ブローカーサーバの IP アドレス／ホスト名／FQDN を入力します。
- **自動接続リスト**——個別のブローカーにログイン後、自動的に起動させたいデスクトップの名前を入力します。複数のデスクトップの設定が可能です。各デスクトップの名前はセミコロンで区切り、大文字と小文字は区別します。
- チェックボックスをオンにし、vWorkspace Gateway を有効にします。
- **vWorkspace Gateway**——vWorkspace Gateway の IP アドレスを入力します。

3 **OK** をクリックして設定を保存します。

Amazon Web Services または WorkSpaces の設定

Amazon WorkSpace は、リモートアプリケーションに簡単にアクセスできるクラウドベースの仮想デスクトップです。

Amazon WorkSpaces 接続は、ThinOS 8.3 以降のバージョンで稼働している PCoIP クライアントにのみ適用できます。

このセクションでは、Amazon WorkSpaces（AWS）接続を ThinOS デバイスに設定する方法と、ThinOS に設定できるその他の Amazon WorkSpace の機能について説明します。

Amazon WorkSpaces ブローカー接続の設定

Amazon WorkSpaces 接続は、PCoIP クライアントにのみ適用できます。Amazon WorkSpaces（AWS）ブローカー設定を設定するには：

1 デスクトップメニューで**システム設定**をクリックし、**リモート接続設定**をクリックします。
リモート接続設定ダイアログボックスが表示されます。
2 **ブローカー**タブでは、ドロップダウンリストで **Amazon WorksSpaces** を選択し、次の操作を行います。

- **ブローカーサーバ**——ブローカーサーバの IP アドレス／ホスト名／FQDN を入力します。
- **自動接続リスト**——個別のブローカーにログイン後、自動的に起動させたいデスクトップの名前を入力します。複数のデスクトップの設定が可能です。各デスクトップの名前はセミコロンで区切り、大文字と小文字は区別します。
- **セキュリティモード**——次のオプションから望ましいセキュリティモードを選択します。
  - **警告**——警告は、PCM にインストールされたドメイン証明書の FQDN アドレスを必要とします。証明書がクライアントにインストールされていない場合、継続しようとすると対応する警告メッセージがユーザーに表示されます。
  - **完全**——完全は、PCM にインストールされたドメイン証明書付きの FQDN アドレスとクライアントにインストールされた証明書を必要とします。
  - **無効**——無効は、証明書の有無にかかわらず、FQDN／IP アドレスを許可します。
  - **既定**——システムセキュリティモード設定に従います。

- **接続プロトコル**——ドロップダウンリストは AWS ブローカーには無効です。このオプションは、デフォルトでは PCoIP のみに設定されています。

3 **OK** をクリックして設定を保存します。

AWS WorkSpaces および AWS EC2 PCM for AWS WorkSpaces の導入の詳細については、www.teradici.com/web-help/Connecting_ZC_AWS_HTML5/TER1408002_Connecting_ZC_AWS.htm#03_DeployPCM.htm%3FTocPath%3D3 を参照してください。

「Broker Server address = PCM の URI（https://<FQDN または IP アドレス>）」の設定の詳細については、www.teradici.com/web-help/Connecting_ZC_AWS_HTML5/TER1408002_Connecting_ZC_AWS.htm#05_Connect.htm%3FTocPath %3D5 を参照してください。

Amazon Web Services または WorkSpaces の既知の問題

- **Ctrl + Alt** のキーを組み合わせて押すと、AWS デスクトップの古いエージェントの場合、ユーザーの AWS セッションが断続的に切断します。この問題を解決するには、デスクトップを再起動してエージェントを最新に更新します。
- 各ユーザーは、1 つの WorkSpaces のデスクトップに割り当てられています。このため、どのユーザー名でログオンしても 1 つのデスクトップに戻り、セッションは自動的に接続します。デスクトップとの接続が切れると、ユーザーはログオン画面に戻ります。

ローカル設定の設定

次を使用して、シンクライアントで、使用可能なシンクライアント設定を設定できます。ユーザーの権限レベルによっては、一部のダイアログボックスが使用できない場合があります。

- ローカル設定メニュー
- リセット機能

メモ：シンクライアント設定を設定する際にダイアログボックスを使用することは推奨していませんが、これらのダイアログボックスは、一時的にデフォルトの一元設定をオーバーライドする場合や一元設定を設定できない（小規模な環境）場合に備えて用意されています。一般的には、一元設定を使用してアップデートと目的のデフォルト設定を、使用環境内のすべてのサポート対象シンクライアントに自動的にプッシュすることをお勧めします。「一元設定：アップデートと設定の自動化」を参照してください。

ローカル設定メニュー

ローカル設定メニューでは、次の操作を行うことができます。

- システム環境の設定
- ディスプレイ設定の設定
- 周辺機器設定の設定
- プリンタ設定の設定

ローカル設定メニューにアクセスするには

- **ゼロデスクトップ**——ゼロツールバーで**システム設定**アイコンをクリックします。管理者は、**ログイン**ダイアログボックスで**管理者モード**ボタンをクリックすることもできます。
- **クラシックデスクトップ**——ユーザー名をクリックし、**システム設定**を選択します。

メモ：ユーザ名は、ログインしているユーザで、タスクバーの左下ペインに表示されています。

システム環境の設定

システム設定のダイアログボックスを使用して、スクリーンセーバー、時刻／日付、カスタム情報設定など、個人の環境設定を選択します。

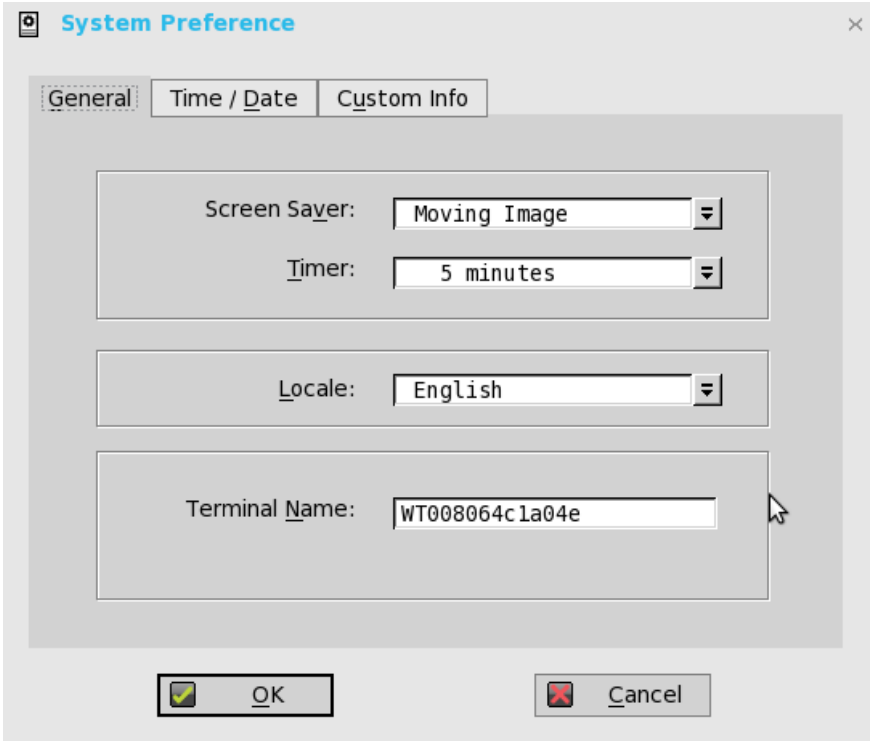
次のオプションを使用して、システム環境を設定します。

- システム環境の全般設定
- 時刻と日付の設定
- カスタム情報の設定

システム環境の全般設定

システム環境の全般設定を行うには

1 デスクトップメニューで**システム設定**をクリックし、**システム設定**をクリックします。
システム設定ダイアログボックスが表示されます。
2 **全般**タブをクリックし、次のガイドラインに従います。



a **スクリーンセーバ**——スクリーンセーバーの種類を選択できます。デフォルトは、**モニタ信号を切る**です。
他に利用可能なスクリーンセーバーとして、**フライングバブル、ムービングイメージ、画像を表示、**および **None** があります。

b **待ち時間**——スクリーンセーバーがアクティブになるまでの時間を選択します。**スクリーンセーバ無効、1 分、3 分、5 分、10 分**（デフォルト）、**15 分**または **30 分**のいずれかを選択します。
指定した時間、シンクライアントがアイドル状態のままになると、スクリーンセーバが起動します。

c **ロケール**——ユーザーのログイン操作の際に有効にする言語を、Japanese、または **English**（デフォルト）のいずれかから選択します。

d **端末名**——シンクライアントの名前を入力できます。デフォルトは、14 文字の文字列で、WT という文字の後にシンクライアントの Ethernet MAC アドレスが続きます。
一部の DHCP サーバでは、DHCP マネージャの画面でこの値を使用して IP アドレスのリースを識別します。

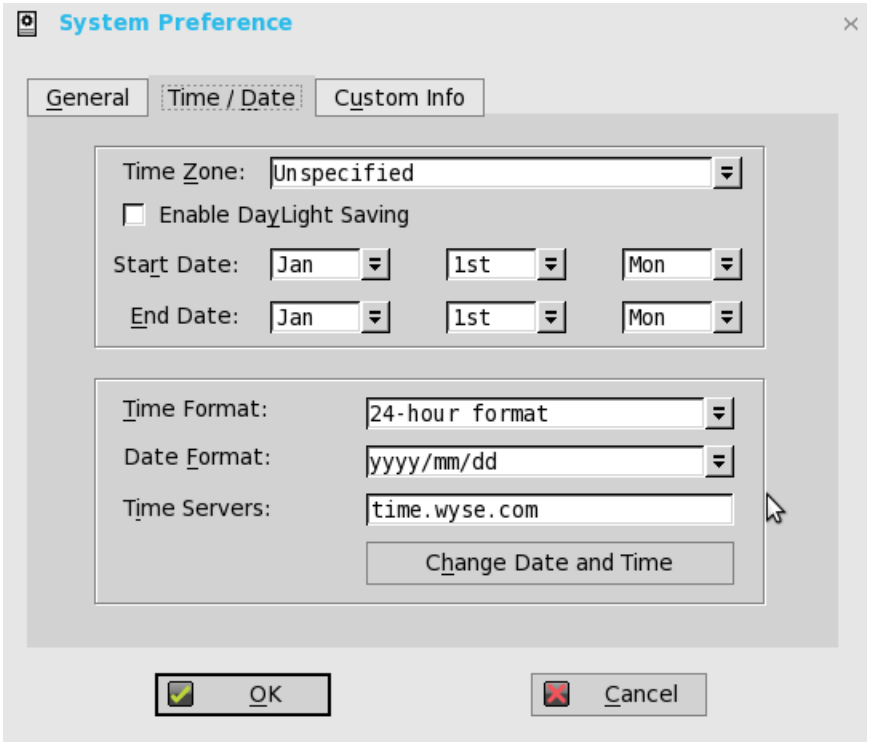
3 **OK** をクリックして設定を保存します。

時刻と日付の設定

時刻と日付の設定を設定するには：

1 デスクトップメニューで**システム設定**をクリックし、**システム設定**をクリックします。
システム設定ダイアログボックスが表示されます。

2 **時間/日付**タブをクリックし、次のガイドラインに従います。



a **タイムゾーン**——ドロップダウンリストから、シンクライアントが稼働するタイムゾーンを選択します。デフォルト値は**未指定**です。

b **夏時間を有効にする**——夏時間の設定を有効にできます。選択する場合は、**開始**ボックスと**終了**ボックスを適切に夏時間の開始期間（月／週／日）と終了期間（月／週／日）を定義します。
次のガイドラインに従って、開始日と終了日を入力します。

- **月**——1 年の **1 月**から **12 月**までの月を選択します。
- **週**——月の **1** から **4** までの週を選択します。最終週は月の最終週を表します。
- **曜日**——週の**月曜日**から日曜日までの曜日を指定します。

c **時刻表示形式**——12 時間または 24 時間形式を選択できます。**デフォルトは 24 時間形式です。**

d **日付表示形式**——yyyy/mm/dd（年／月／日）または dd/mm/yyyy（日／月／年）の日付形式を選択できます。
デフォルトは **yyyy/mm/dd** です。

e **時刻サーバ**——オプションのタイムサーバの TCP ポート番号とともに、IP アドレスまたはホスト名を表示するリストです。
オプションのポート番号を使用して各エントリーを指定する場合は、Name または IP:port の形式にします。ここで、port はオプションです。指定しない場合は、ポート 80 が使用されます。ユーザープロファイルを使用している場合、場所はユーザープロファイルを介して提供できます。タイムサーバは、タイムゾーンと夏時間の情報の設定に基づいて、シンクライアントに時刻を提供します。DHCP を使用している場合は、場所は DHCP を介して提供できます。

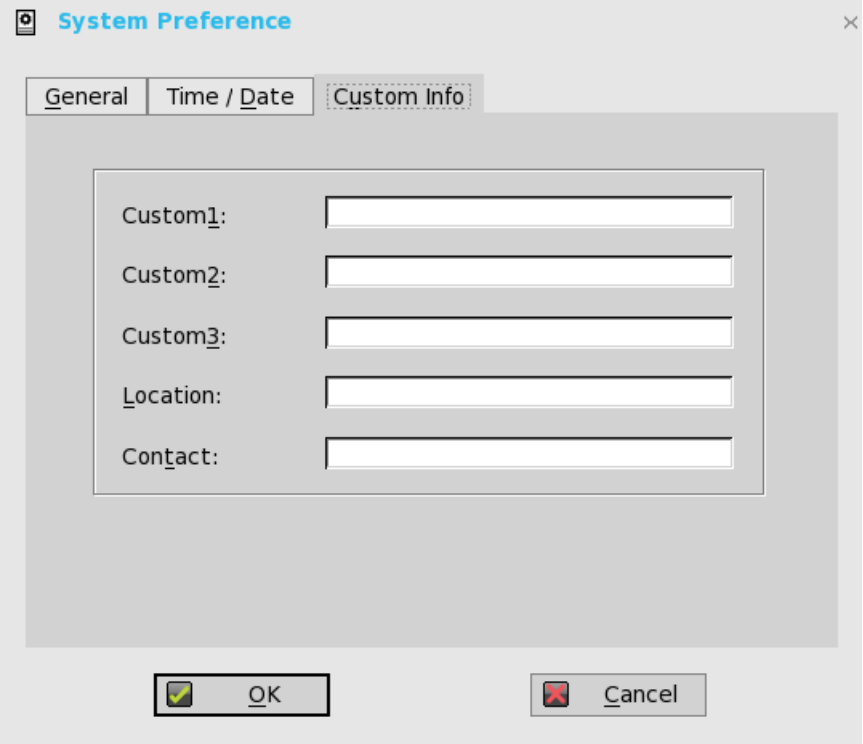
f **日付と時刻の変更**——外部からのサーバへのアクセスの対策を必要とする安全な環境のために、日付と時刻を変更できます。HTTPS を介してファイルサーバに接続する場合、SSL や認証の確認のために、適切な時刻をシンクライアントで定義する必要があります。

3 **OK** をクリックして設定を保存します。

カスタム情報の設定

カスタム情報タブを使用して、WMS/WDM ソフトウェアで使用する設定文字列を入力します。設定文字列には、場所、ユーザー、管理者などの情報を含めることができます。
カスタム情報を設定するには

1 デスクトップメニューで**システム設定**をクリックし、**システム設定**をクリックします。
システム設定ダイアログボックスが表示されます。
2 **カスタム情報**タブをクリックして、WDM ソフトウェアで使用する設定文字列を入力します。設定文字列には、場所、ユーザー、管理者などの情報を含めることができます。**OK** をクリックすると、ダイアログボックスに入力するカスタムフィールド情報が Windows レジストリに転送されます。これでこの情報は、WDM クライアントマネージャで使用できます。シンクライアントソフトウェアのリモート管理とアップグレードで、カスタムフィールドを使用する方法および WDM を使用する方法の詳細については、WDM のドキュメントを参照してください。



3 **OK** をクリックして設定を保存します。

ディスプレイ設定の設定

デュアルディスプレイ設定は、マルチモニタをサポートするために、ThinOS 8.5.1 リリースで導入された新機能です。**ディスプレイ設定の**ダイアログボックスを使用して、接続されたモニタの表示設定を設定します。
ディスプレイ設定を設定するには：

1 デスクトップメニューで**システム設定**をクリックし、ディスプレイをクリックします。
ディスプレイ設定ダイアログボックスが表示されます。
2 **ディスプレイ設定**ダイアログボックスで、次のオプションを設定します。
- **ミラーモード**——**ミラーモード**チェックボックスをオンにすると、接続されたモニタはすべて、プライマリモニタに設定されたものと同じ表示設定を使用できます。
次の画面はミラーモード設定を示しています。

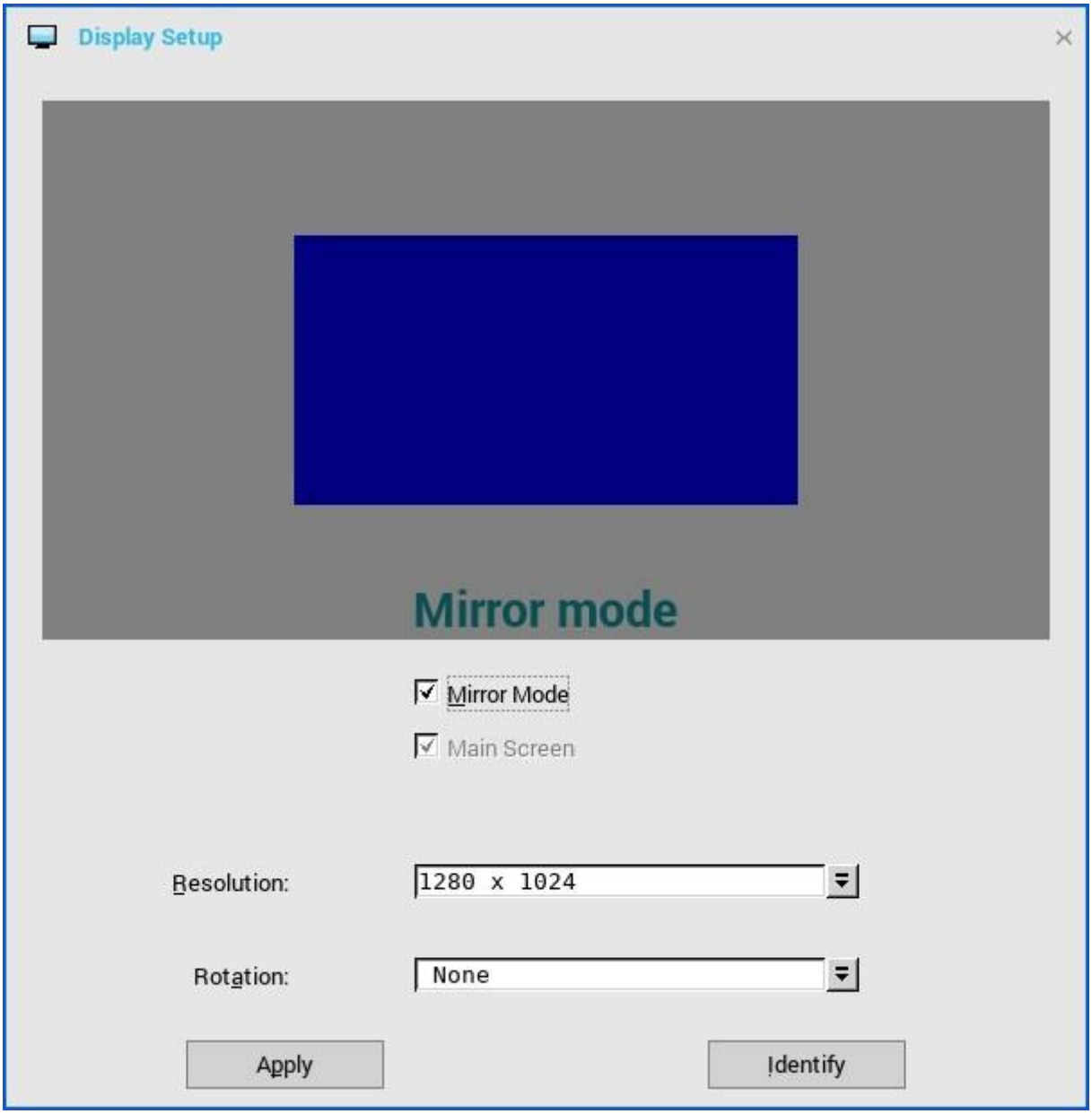


図 14.　ディスプレイ設定（Wyse 5070 シンクライアント）

ミラーモードチェックボックスをオフにすると、**スパンモード**が有効になります。次の画面はスパンモード設定を示しています。

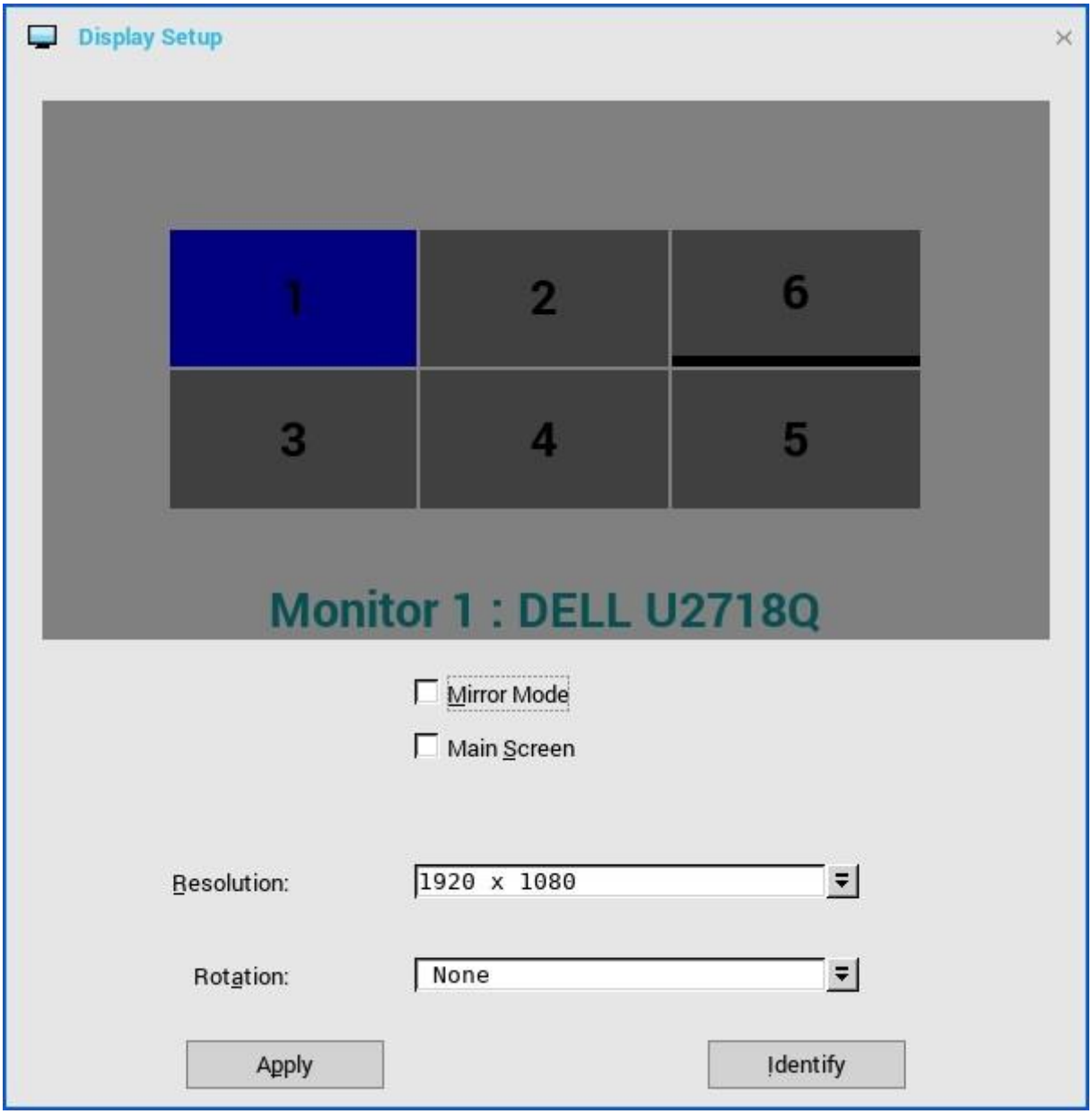


図 15.　ディスプレイ設定（Wyse 5070 シンクライアント）

画面に表示されたブロックは、シンクライアントに接続されたモニタ画面の数を示しています。各ブロックは 1 つのモニタ画面を表わしています。

各モニタには固有の表示順序番号と表示設定が含まれています。ブロックを水平や垂直に動かして、さまざまな方向にデュアルディスプレイのレイアウトを作ることができます。新しいディスプレイレイアウトを作成するには、ブロックを好きな位置に移動して**適用**をクリックします。新しいディスプレイレイアウトが作成されました。ただし、ブロックが不適切な位置に移動された場合は、システムがそのブロックをデフォルトの位置に設定します。

メモ：Wyse 5070 Extended シンクライアントは、最大 6 台のモニタをサポートします。

- **主スクリーン**——**主スクリーン**チェックボックスをオンにすると、そのモニタはプライマリモニタまたはメイン画面に設定されます。モニタをメイン画面に設定するには、モニタブロックをクリックして、**主スクリーン**チェックボックスをオンにします。モニタをメイン画面に設定すると、モニタブロックは下線付きで高輝度表示され、そのモニタブロックには**主スクリーン**オプションが無効となります。他のモニタブロックでは**主スクリーン**オプションが利用できます。

メモ：主スクリーンオプションはスパンモードでのみ有効で、ミラーモードでは常に無効です。

- **解像度**——**解像度**ドロップダウンリストで、お使いのモニタでサポートされているディスプレイ解像度を選択します。
  ミラーモードでは、接続されたすべてのモニタの解像度の共通部分から解像度の一覧が得られます。

  スパンモードでは、モニタブロックを選択し、**解像度**ドロップリストで解像度を変更します。
- 回転——**回転**ドロップダウンリストで、モニタ画面を異なる方向に回転させるオプション（**左へ 90 度回転**または**右へ 90 度回転**）を選択します。このオプションはデフォルトでは**無し**に設定されています。

3 **適用**をクリックします。

新しい表示設定が適用され、修正されたディスプレイを表示できます。

4 **OK** をクリックして新しい設定を確定します。

メモ：識別オプションを使用すると、接続されたモニタの表示順序番号が分かります。

ハードウェアの能力

このセクションではハードウェアの表示能力について説明しています。

表 18. ポート優先権（Wyse 5070 シンクライアント）

モデル	要約
Wyse 5070 シンクライアント（Celeron Processor 搭載）	• Wyse 5070 シンクライアント（ワイヤレスモジュールなし）では、オプションのポートは 2 番目の RJ-45、SFP、VGA として、または 2 番目のシリアルポートとして使用できます。 • Wyse 5070 シンクライアント（ワイヤレスモジュール搭載）では、オプションのポートを 2 番目の RJ-45 または SFP として使用できません。 • モニタが USB Type-C ポートに接続されると、DisplayPort 2 は非アクティブになります。
Wyse 5070 シンクライアント（Pentium Processor 搭載）	• Wyse 5070 シンクライアント（ワイヤレスモジュールなし）では、オプションのポートは 2 番目の RJ-45、SFP、VGA として、または 2 番目のシリアルポートとして使用できます。 • Wyse 5070 シンクライアント（ワイヤレスモジュール搭載）では、オプションのポートを 2 番目の RJ-45 または SFP として使用できません。 • フロントヘッドフォンを使用している場合、バックヘッドセットが無効になります。 • モニタが USB Type-C ポートに接続されると、DisplayPort 2 は非アクティブになります。 • VGA モニタが VGA オプションポートに接続されていると、DisplayPort 3 は非アクティブになります。
Wyse 5070 Extended シンクライアント	• Wyse 5070 Extended シンクライアント（ワイヤレスモジュールなし）では、オプションのポートを 2 番目の RJ-45、SFP、VGA のいずれかとして使用できます。 • Wyse 5070 Extended シンクライアント（ワイヤレスモジュール搭載）では、オプションのポートを 2 番目の RJ-45 または SFP として使用できません。 • フロントヘッドフォンを使用している場合、バックヘッドセットが無効になります。 • モニタが USB Type-C ポートに接続されると、DisplayPort 2 は非アクティブになります。 • VGA モニタが VGA オプションポートに接続されていると、DisplayPort 3 は非アクティブになります。 • 電源オプションは 1 番目のシリアルポートに使用できます。 • PCIe スロットが使用できます。

Wyse 5070 シンクライアント（Celeron Processor 搭載）

表 19. ディスプレイマトリックス

ディスプレイの数	サポートされている表示解像度	
	4K 解像度	4K 解像度以外

ディスプレイの数	サポートされている表示解像度	
	3840 x 2160 @ 60 Hz	最大 2560 x 1600 @ 60 Hz
ディスプレイ 1 台	はい	はい
ディスプレイ 2 台	はい	はい
ディスプレイ 3 台	いいえ [1]	はい [2]

[1]VGA ポートは 4K 表示をサポートしません。ただし、画面解像度 1080p のディスプレイはサポートします。

[2] または 4K ディスプレイ以外では、2560 x 1600 @ 60 Hz までの画面解像度が、VGA を除くすべてのポートでサポートされています。VGA ポートは解像度 1080p のみサポートします。

表 20. ポート

ポート	DP1	DP2	VGA	USB Type-C
モニタ優先順位	1	2B[1]	3	2A[1]
4K ディスプレイ	はい	はい	いいえ [2]	はい
4K ディスプレイ以外	はい	はい	はい [2]	はい

[1]DP2 と USB Type-C ポートは相互排他的で、USB Type-C ポートの優先順位が高くなります。

[2]VGA ポートは解像度 1080p のみサポートします。

メモ：USB Type-C ポートの 4K 解像度@ 60 Hz は、Type-C to HDMI/DP 変換アダプタを使用してテストしました。USB Type-C ポート付き Dell モニタ S2718D は、最大解像度 2560 x 1440 をサポートします。

Wyse 5070 シンクライアント（Pentium Processor 搭載）

表 21. ディスプレイマトリックス

ディスプレイの数	サポートされている表示解像度	
	4K 解像度 3840 x 2160 @ 60 Hz	4K 解像度以外 最大 2560 x 1600 @ 60 Hz
ディスプレイ 1 台	はい	はい
ディスプレイ 2 台	はい	はい
ディスプレイ 3 台 [1]	はい	はい

[1] デルは、安定性と性能を最適化するために、4K 解像度のディスプレイは最大 2 台とし、DisplayPort 3 の 3 台目は 4K 解像度以外のディスプレイ構成にすることをお勧めします。ただし、Wyse 5070 シンクライアント（Pentium プロセッサ搭載）の実用上の最大性能に基づいて、ThinOS は最大 3 台の 4K ディスプレイをサポートします。

表 22. ポート

ポート	DP1	DP2	DP3	VGA	USB Type-C
モニタ優先順位	1	2B[1]	3B[2]	3A[2]	2A[1]
4K ディスプレイ	はい	はい	はい	いいえ [3]	はい
4K ディスプレイ以外	はい	はい	はい	はい [3]	はい

[1]DP2 と USB Type-C ポートは相互排他的で、USB Type-C ポートの優先順位が高くなります。

[2]DP3 と VGA ポートは相互排他的で、VGA ポートの優先順位が高くなります。

[3]VGA ポートは解像度 1080p のみサポートします。

メモ：USB Type-C ポートの 4K 解像度@ 60 Hz は、Type-C to HDMI/DP 変換アダプタを使用してテストしました。USB Type-C ポート付き Dell モニタ S2718D は、最大解像度 2560 x 1440 をサポートします。

Wyse 5070 Extended シンクライアント（AMD GPU 搭載）

表 23. Wyse 5070 Extended シンクライアント（AMD GPU 搭載）

ディスプレイの数	サポートされている表示解像度	
	4K 解像度 3840 x 2160 @ 60 Hz	4K 解像度以外 最大 2560 x 1600 @ 60 Hz
ディスプレイ 1 台	はい	はい
ディスプレイ 2 台	はい	はい
ディスプレイ 3 台 [1]	はい	はい
ディスプレイ 4 台 [2]	はい	はい
ディスプレイ 5 台 [2]	はい	はい
ディスプレイ 6 台 [2]	はい [2]	はい

[1] ディスプレイが 3 台の場合は、デルは、メインボード（DP1～DP3）に最初の 2 台の 4K ディスプレイ、AMD GPU カードに 3 番目の 4K ディスプレイという構成をお勧めします。

[2] デルは、安定性と性能を最適化するために、4K 解像度のディスプレイは最大 4 台とし、DisplayPort 3 と DisplayPort 6 の残りのディスプレイは、4K 解像度以外の構成とすることをお勧めします。ただし、Wyse 5070 Extended シンクライアントの実用上の最大性能に基づいて、ThinOS は最大 6 台の 4K ディスプレイをサポートします。

メモ：Best practice——4K ディスプレイの出力を最大にするために、デルは DisplayPort 3 に 1080p を設定し、残りのモニタを 4K 解像度にして、性能を最適化することをお勧めします。

表 24. ポート

ポート	DP1	DP2	DP3	VGA	USB Type-C	mDP4	mDP5	DP6
モニタ優先順位	1	2B[1]	3B[2]	3A[2]	2A[1]	4	5	6
4K ディスプレイ	はい	はい	はい	いいえ [3]	はい	はい	はい	はい
4K ディスプレイ以外	はい	はい	はい	はい [3]	はい	はい	はい	はい

[1]DP2 と USB Type-C ポートは相互排他的で、USB Type-C ポートの優先順位が高くなります。

[2]DP3 と VGA ポートは相互排他的で、VGA ポートの優先順位が高くなります。

[3]VGA ポートは解像度 1080p のみサポートします。

メモ：USB Type-C ポートの 4K 解像度@ 60 Hz は、Type-C to HDMI/DP 変換アダプタを使用してテストしました。USB Type-C ポート付き Dell モニタ S2718D は、最大解像度 2560 x 1440 をサポートします。

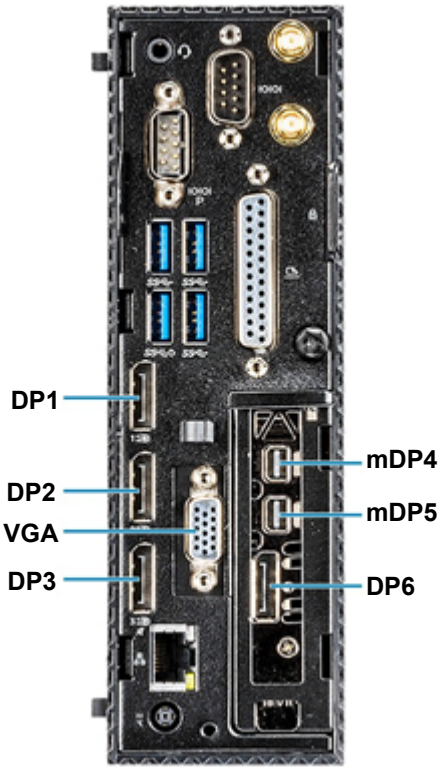


図 16.　Wyse 5070 Extended シンクライアントのポート

モニタの優先順位——次の順序は、Wyse 5070 Extended シンクライアントの ThinOS に設定されているモニタの優先順位を定義したものです。

- DP1 > DP2 > DP3 > mDP4 > mDP5 > DP6
- DP1 > USB Type-C > DP3 > mDP4 > mDP5 > DP6
- DP1 > DP2 > VGA > mDP4 > mDP5 > DP6
- DP1 > USB Type-C > VGA > mDP4 > mDP5 > DP6

メモ：モニタケーブルのホットプラグ——画面レイアウトの設定は、サポートされているモニタの解像度とモニタが接続されているポートに基づいて変更されます。

メモ：ThinOS の初期のゼロテーマでは、ディスプレイ設定ウィンドウは左側の設定パネルとつながっていました。現在のシナリオでは、ディスプレイ設定ウィンドウは Classic/Zero モードにかかわらず、画面の中央にあります。この機能改善によって、確認ウィンドウと連動する表示設定が簡単に設定できるようになっています。

既知の問題

- VDI 接続のセッション中に、モニタのプラグの抜き差しをすると、ブラックスクリーン状態になる場合があります。セッション画面を正常な状態に戻すには、モニタの電源をオフにしてから電源をオンにする必要があります。この問題は次のリリースで解消されます。
- VDI 接続中またはディスプレイ設定中に、モニタのプラグの抜き差しをすると、端末がフリーズする、画面レイアウトが変わるなどの予期しない問題が発生する場合があります。この問題は次のリリースで解消されます。

周辺機器設定の設定

周辺機器ダイアログボックスでは、キーボード、マウス、オーディオ、シリアル、カメラ、タッチスクリーンおよび Bluetooth 設定を設定できます。

- キーボード設定の設定
- マウス設定の設定
- オーディオ設定の設定
- シリアル設定の設定
- カメラ設定の設定
- タッチスクリーン設定の設定
- Bluetooth 設定の設定

キーボード設定の設定

キーボード設定を設定するには :

1 デスクトップメニューで**システム設定**をクリックし、**周辺機器**をクリックします。
周辺機器ダイアログボックスが表示されます。
2 **キーボード**タブをクリックし、文字セット、キーボード言語、リピート前の遅延およびリピート速度パラメータを設定します。次の表ではキーボードパラメータについて説明しています。

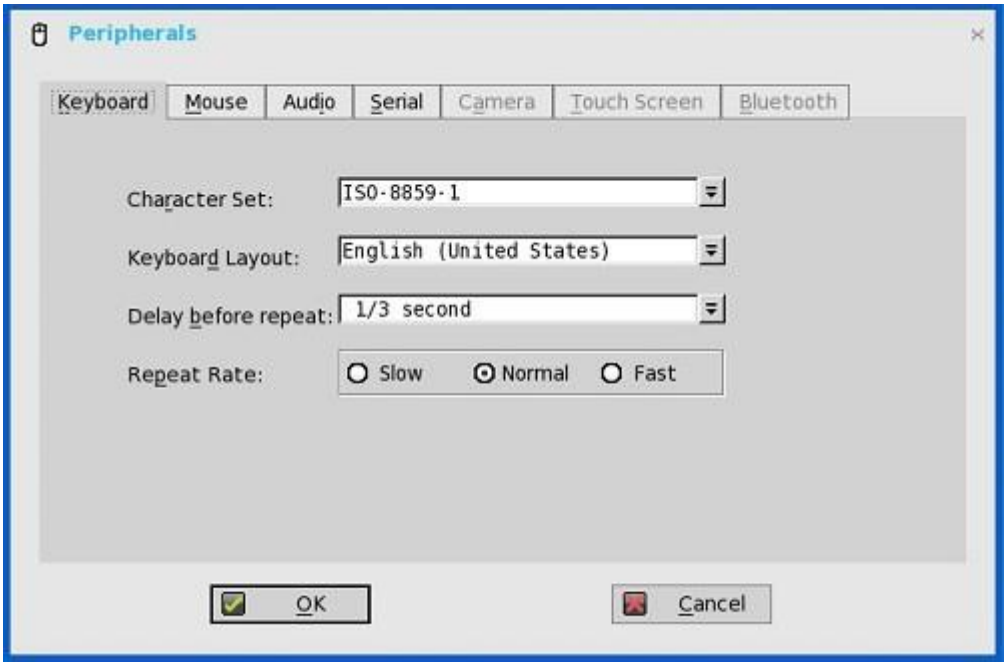


表 25. キーボード設定

パラメータ	説明
文字セット	文字セットを指定します。それぞれの文字は、数値で表されます。たとえば、ASCII 文字セットでは、0〜127 の数値ですべての英文字と特殊文字を表します。European ISO 文字セットは ASCII と似ていますが、

パラメータ	説明
	欧州言語に対応する追加の文字が含まれています。
キーボード言語	現在、**キーボード言語**ドロップダウンリストに表示されているキーボード言語がサポートされています。デフォルト値は**日本語**です。
リピート前の遅延	押したままのキーに対する repeat パラメータを指定します。Delay before repeat の値には、**1/5 秒**、**1/4 秒**、**1/3 秒**、**1/2 秒**、**3/4 秒**、**1 秒**、**2 秒 s** または**リピートなし**のいずれかを選択します。デフォルトは **1/3 秒**です。
リピート速度	**遅く**、**普通**、または**早く**を選択します。デフォルト値は普通です。

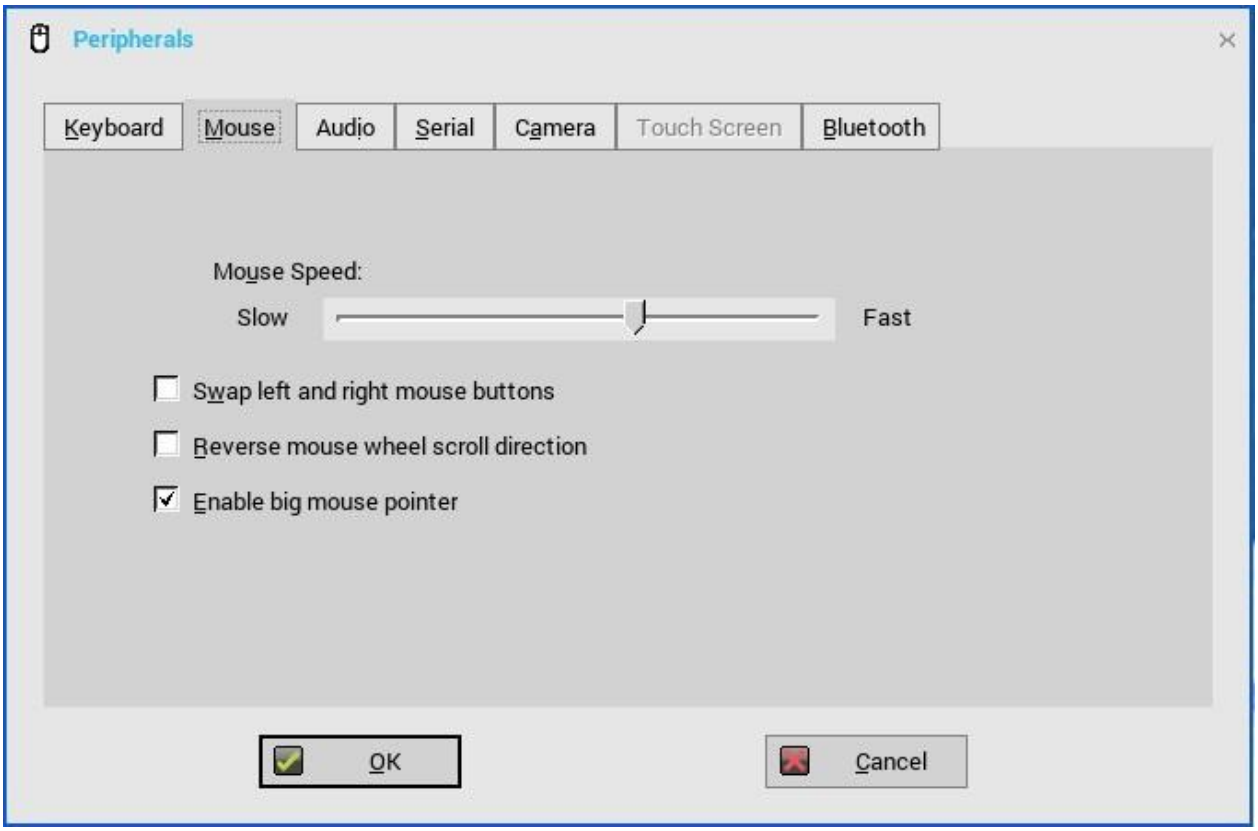
3 **OK** をクリックして設定を保存します。

マウス設定の設定

マウス設定を設定するには：

1 デスクトップメニューで**システム設定**をクリックし、**周辺機器**をクリックします。
周辺機器ダイアログボックスが表示されます。

2 **マウス**タブをクリックし、マウスの速度とマウスの向きを選択します。



3 **左右のボタン機能を切り替える**チェックボックスをオンにすると、左利きの操作に対応するようマウスボタンが入れ替わります。

4 **マウスホイール逆方向スクロール**チェックボックスをオンにすると、マウスのスクロールホイールの向きが逆になります。

5 **大型マウスポインターの有効化**チェックボックスをオンにすると、ローカルマウスポインター—のサイズが 2 倍になります。

6 **OK** をクリックして設定を保存します。

オーディオ設定の設定

オーディオ設定を設定するには

1 デスクトップメニューで**システム設定**をクリックし、**周辺機器**をクリックします。
周辺機器ダイアログボックスが表示されます。
2 **音声**タブをクリックして、接続されているデバイスのボリューム設定を選択します。

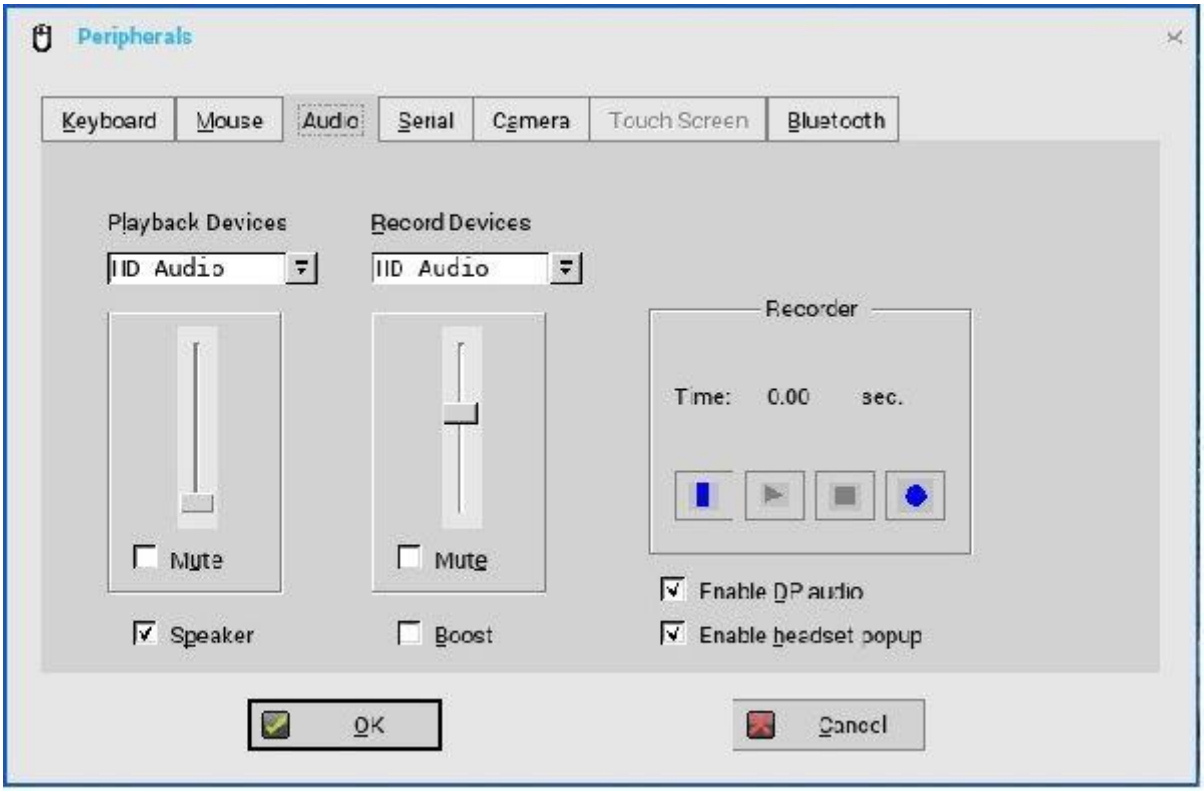


図 17. 音声タブ

a **再生デバイスの**タブをクリックして、ドロップダウンメニューからオーディオのタイプを選択します。
- HD オーディオと DP オーディオのオプションが再生デバイスで利用可能な場合、DP ケーブルが接続されていると、シンクライアントは HD オーディオと DP オーディオの優先順位を決定します。このシナリオでは、お好みに基づいて再生デバイスのタイプを選択し、**OK** をクリックします。選択した再生デバイスが優先となります。
- **スライダ**を使用して、再生デバイスのボリューム設定を制御します。
- ミュートするにはチェックボックスをオンにします。

b **録音デバイスの**タブをクリックし、ドロップダウンメニューから録音のタイプを選択します。
- **スライダ**を使用して、録音デバイスのボリューム設定を制御します。
- ミュートするにはチェックボックスをオンにします。

c **再生アイコン**をクリックするとオーディオを再生します。

d **録音アイコン**を使用して次の操作を行います。
- 使用中のスピーカとマイクの情報を収集します。
- 使用中のスピーカとマイクの性能を確認します。

たとえば、接続されている USB ヘッドセットがドロップダウンに表示されます。アナログイヤホンを使用するには **HD Audio** オプションを選択し、内蔵スピーカを有効にするには Speaker チェックボックスをオンにします。また、オーディオを拡張するには**ブースト**チェックボックスをオンにします。

e スピーカを接続するには**スピーカー**チェックボックスをオンにします。

f 接続されているデバイスをブーストするには**ブースト**チェックボックスをオンにします。

g **DP オーディオの有効**のチェックボックスをオンにすると、シンクライアントの DisplayPort オーディオ機能が有効になります。

h アナログヘッドセットをフロントヘッドセットジャックに差し込んだ時に、**ヘッドセットポップアップの有効化の**ダイアログボックスを表示させたい場合は、**ヘッドセットポップアップの有効化の**チェックボックスをオンにします。
、**ヘッドセットポップアップ**ダイアログボックスでは、次のオーディオデバイスのいずれか 1 つを選択します。

- ヘッドセット
- ヘッドフォン
- スピーカ

メモ：、ヘッドセットポップアップダイアログボックスを無効にするには、Not show again チェックボックスをオンにし、OK をクリックします。INI パラメータを使用してヘッドセットポップアップダイアログボックスを有効または無効にすることもできます。INI パラメータの詳細については、最新の『Dell Wyse ThinOS INI Reference Guide』を参照してください。

既知の問題の詳細については、最新の『Dell Wyse ThinOS リリースノート』を参照してください。

DisplayPort オーディオの使用

DisplayPort（DP）インターフェイスを使用して、シンクライアントを表示デバイスに接続します。このインターフェイスでは、ビデオ信号と同じケーブルで、オーディオ信号を送ることができます。DisplayPort オーディオを有効にするには、必ず次のコンポーネントを設定してください。

- DisplayPort オーディオおよび／またはデュアルモードオーディオをサポートするシンクライアント
- ICA、RDP、Blast、PCoIP のいずれかのセッションで、オーディオ再生をサポートする、モニタなどの表示デバイス
- アナログオーディオデバイスまたはモニタ内蔵スピーカ

Wyse 5070 シンクライアントでは、DisplayPort オーディオは、DisplayPort 1 と DisplayPort 2 のみでサポートされます。ThinOS の DisplayPort オーディオの有効化：

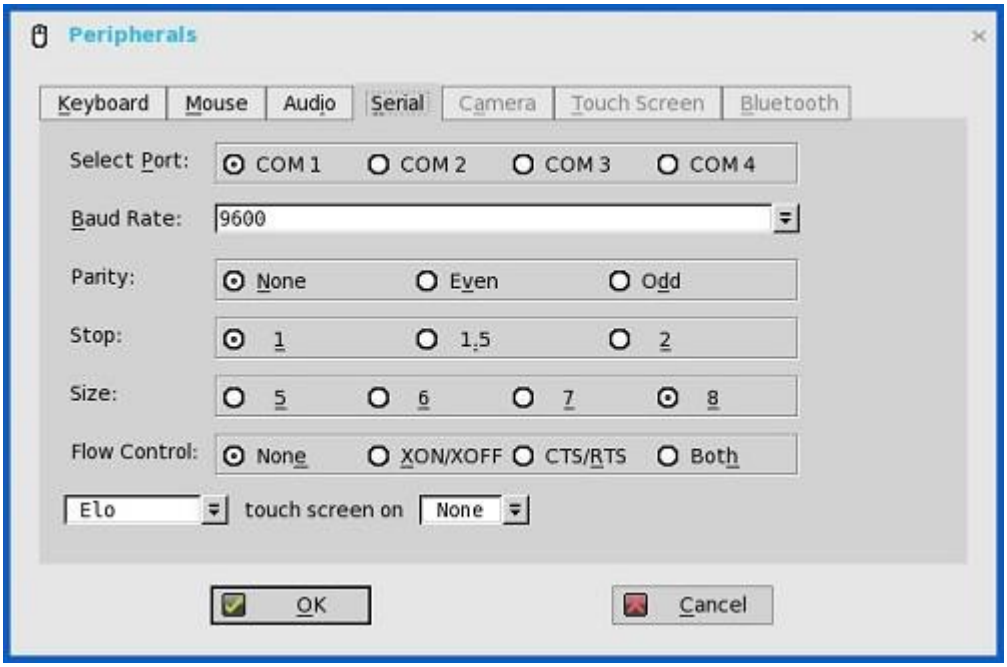
1 DP オーディオサポート付きのモニタを設定します。
2 ThinOS クライアントを DP ケーブルでモニタに接続します。
3 アナログヘッドセットのプラグを、モニタ DP のオーディオインターフェイスに差し込みます。
4 ThinOS デスクトップで、**システム設定 > 周辺機器 > 音声> 再生デバイス**の順にクリックして、**DP オーディオの有効化**チェックボックスをオンにします。
5 RDP、ICA、PCoIP、Blast のいずれかのセッションを開始します。
6 ビデオを再生し、アナログヘッドセットを使用してオーディオ出力を確認します。

メモ：ThinOS は、DisplayPort オーディオ再生のみをサポートしています。DisplayPort を使用したオーディオ録音は、サポートされていません。

シリアル設定の設定

シリアル設定を設定するには

1 デスクトップメニューで**システム設定**をクリックし、**周辺機器**をクリックします。
周辺機器ダイアログボックスが表示されます。
2 **シリアル**タブをクリックし、次の操作を行います。



a **ポートの選択**——ボタンをクリックして、ポートを選択します。デフォルトは **COM 1** です。

b **ボーレート**——ドロップダウンリストでボーレートを選択します。デフォルトは **9600** です。

c **パリティ**——ボタンをクリックして、パリティを選択します。

d **ストップ**——ボタンをクリックして、ストップビットを 1、1.5、2 から選択します。デフォルト値は **1** です。

e **サイズ**——ボタンをクリックして、文字サイズを **5**、**6**、**7** または **8** ビットから選択します。**デフォルトは 8 です。**

f **フロー制御**——ボタンをクリックして、フロー制御を選択します。なし（Flow Control なし）、XON/XOFF と CTS/RTS のいずれか 1 つまたは両方が選択可能です。デフォルトは None です。

g **シリアルタッチスクリーンのオプション**——ドロップダウンリストから必要なタッチスクリーンを選択します。選択できるオプションは、ELO、MicroTouch および FastPoint です。

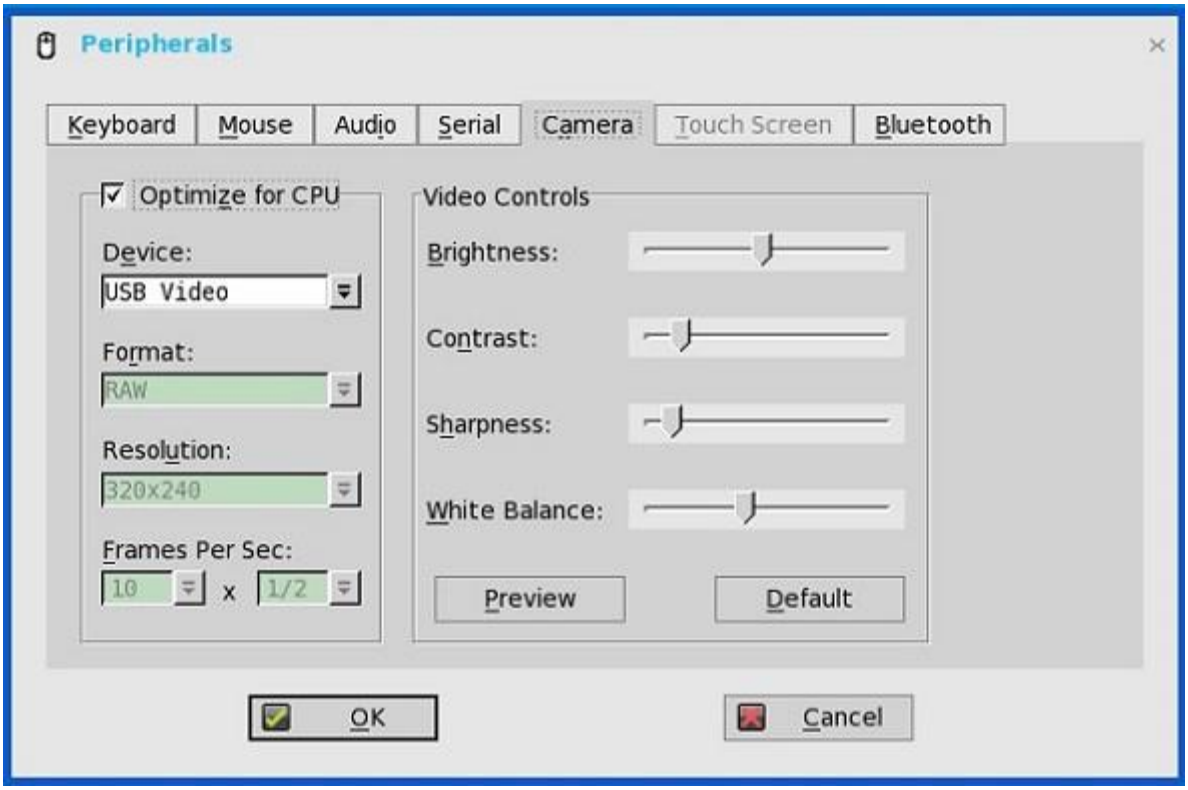
h **タッチパネル**——ドロップダウンリストから必要なシリアルポート（COM ポート）または**なし**を選択します。

3 **OK** をクリックして設定を保存します。

カメラ設定の設定

カメラタブを使用すると、ローカルでシンクライアント（USB）に接続されている、UVC ドライバ対応のカメラと連動します。XenDesktop または XenApp の HDX RealTime Web カメラ機能を使用すると、最大解像度や 1 秒あたりのフレーム数（10 FPS を推奨）などのオプションを制御できます。

デフォルトでは、USB カメラのフォーマットは RAW です。



メモ：
（Web カメラが Universal Video Driver をサポートしている場合）**CPU への最適化**チェックボックスをオフにすると、シンクライアントから直接パフォーマンスを最適化し、1 秒あたりのフレームレートを変更できます。サポートする値は、1/1、1/2、1/3、1/4、1/5 および 1/6 です。

また、この機能は CPU を集中的に使用するため、ハイパフォーマンス製品で推奨されます。

タッチスクリーン設定の設定

タッチパネルタブを使用して、**シンクライアント**に接続されているタッチスクリーンを設定します。シンクライアントによって、タッチスクリーンが USB ポートまたはシリアルポートを介して接続されていて、設定または調整がまだ実行されていないことが検出された場合、このタブは使用できます（グレーアウトされません）。Touch Setup ウィンドウにより、画面上の 2 つの円にタッチし、校正で必要な調整を行うよう求められます。調整された校正値は、システムが工場出荷時のデフォルトにリセットされるか、別のタイプのタッチモニタが接続されるまでローカルターミナルの NVRAM に保存されます。

メモ：ThinOS バージョン 8.5 から、ELO タッチスクリーンは特定のシナリオでは動作しません。詳細については、最新の『Dell Wyse ThinOS リリースノート』を参照してください。

Bluetooth 設定の設定

Bluetooth の機能により、ヘッドセットおよびマウスなどの Bluetooth 対応デバイスとシンクライアントを接続できます。

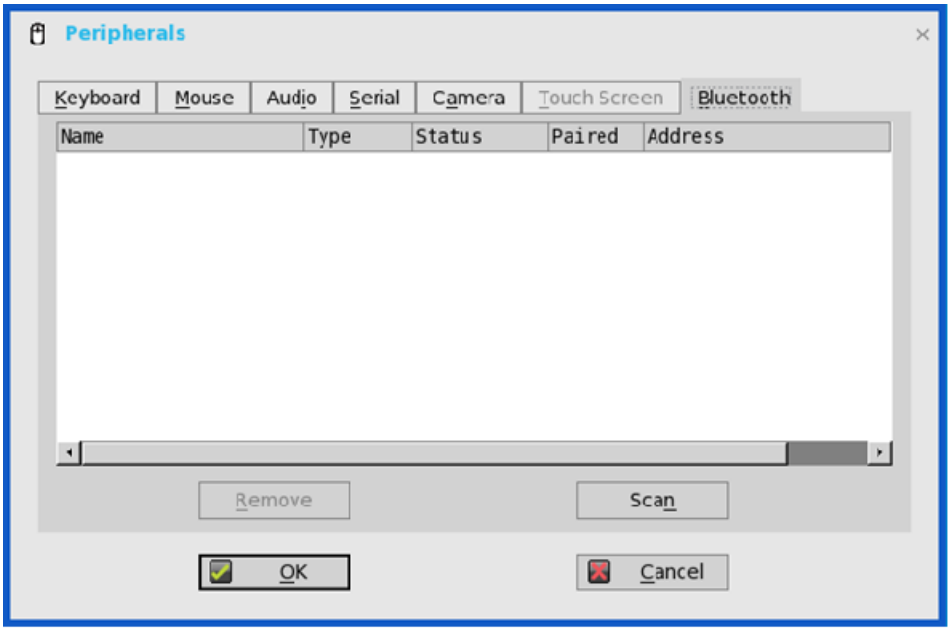
ThinOS は、Intel Dual Band Wireless AC 9560 チップセットをサポートします。マウス、キーボード、ヘッドセットについては、ThinOS は、Bluetooth 3.0 と 4.0 の両方をサポートします。

Bluetooth 4.0 は、Classic および Bluetooth Low Energy（BLE）をサポートします。ただし、Bluetooth Alternate MAC/PHY（AMP）はサポートしていません。

Bluetooth 設定を設定するには

1　デスクトップメニューで**システム設定**をクリックし、**周辺機器**をクリックします。

周辺機器ダイアログボックスが表示されます。



2 **Bluetooth** タブをクリックし、次のガイドラインに従います。

シンクライアント環境で使用可能なヘッドセットやマウスなどの Bluetooth 対応デバイスが、**Bluetooth** ページに表示されます。次の属性が、リストに表示されます。

- **名前**——Bluetooth 対応デバイスの名前を指定します。
- **種類**——ヘッドセット、マウスおよびキーボードなどの Bluetooth 対応デバイスのタイプを指定します。
  ヒューマンインターフェイスデバイス（HID）および**ヘッドセット** Bluetooth デバイスの両方がサポートされます。
  - **HID** タイプ
    - HID には、マウスやキーボードなどが含まれます。
    - 接続可能な HID の最大数は 7 です。
  - **Headset** タイプ
    - このリリースでは、Bluetooth ヘッドセットがサポートされています。
    - 接続可能な Bluetooth ヘッドセットの最大数は 1 です。

  重要: その他のタイプの Bluetooth デバイスはスキャンされず、サポートされません。ヘッドセットの通話レベルのオーディオ品質はサポートされます。ただし、マルチメディアはまだサポートされていません。

- **状態**——**Bluetooth ステータス**ページには、**状態**と**ペアリング**という 2 つの項目があります。

表 26. Bluetooth ステータス

属性	値	要約
状態	Connected	Bluetooth デバイスは、ThinOS デバイスと接続されています。デバイスは、使用する準備ができています。
	Connecting	Bluetooth デバイスは、ThinOS デバイスに接続しようとしています。
	Disconnected	Bluetooth デバイスは、ThinOS デバイスと接続されていません。
ペアリング	はい	Bluetooth デバイスは、ThinOS デバイスとペアリングされています。
	いいえ	Bluetooth デバイスは、ThinOS デバイスとペアリングされていません。

- **アドレス**——シンクライアントに接続した Bluetooth デバイスのアドレスを表示します。

次に示すのは、ユーザーのシナリオと、Bluetooth ページに表示される対応する Bluetooth ステータスです。

表 27.　ユーザーのシナリオ

ユーザーのシナリオ	Status
デバイスをオフにする	Disconnected | Paired
デバイスをオンにする	Connected | Paired
デバイスを ThinOS から切断する	Disconnected | Not Paired

- **スキャン**——すべての Bluetooth デバイスが**ページスキャン**モードに入ります。特定のボタンを 3 回押す、または特定のボタンを LED が青に変わるまで押したままにするなど、Bluetooth デバイスによってページスキャンモードに入る操作は異なります。
- **接続**——特定の Bluetooth 対応デバイスを選択し、**接続**をクリックして、選択したデバイスをシンクライアントに接続します。Bluetooth デバイスが正常に接続されると、**Bluetooth** ウィンドウに表示されるステータスは **Connected** となります。
- **削除**——特定の Bluetooth デバイスを選択し、**Remove** をクリックすると、デバイスが切断され、リストから削除されます。
- **Auto Connect function**——Auto Connect 機能は、HID 向けに設計されています。
  - ThinOS に USB HID または Bluetooth HID などの HID が接続されていない
  - Bluetooth HID が、ページスキャンモードに設定されている

  ThinOS クライアントを起動すると、スキャン操作やペアリング操作なしで、Bluetooth HID が ThinOS に自動的に接続できます。Bluetooth HID は、ThinOS クライアントのリスタート後、自動的に再接続します。
- **Reconnect function**——Reconnect 機能は、HID およびヘッドセット向けに設計されています。
  すでにペアリングされている、接続済みの Bluetooth デバイス（HID/ヘッドセット）を含むシステムをリスタートすると、Bluetooth デバイスは、数秒以内に自動的に再接続します。

  たとえば、Bluetooth マウスを静止させてから数回クリックすると、Bluetooth マウスを正常に再接続できます。Bluetooth ヘッドセットは自動的に再接続されますが、場合によっては、手動でデバイスを閉じたり、再度開いたりする必要があります。

認定デバイスの詳細については、最新の『Dell Wyse ThinOS リースノート』を参照してください。

Bluetooth 機能の既知の問題

1　マウス以外の Bluetooth デバイスが複数接続されているときに、Bluetooth マウスデバイスを複数の ThinOS に接続していると、Bluetooth 接続のパフォーマンスが低下する原因となる可能性があります。
回避策——デルは、Bluetooth 接続では、ThinOS で 1 つのマウスと 1 つのキーボードを使用することを推奨します。

2　Bluetooth デバイスの名前に、N/A と表示されることがあります。
回避策——リストからこのデバイスを削除して、再スキャンします。

3　Bluetooth ヘッドセットでは、ボリュームボタンとミュートボタンのみ使用できます。

4　ワイヤレス接続時には Bluetooth 機能のパフォーマンスが低下します。

5　4K モニタを Wyse 5070 シンクライアント（Intel Dual Band Wireless AC 9560 チップセット搭載）の DP1 ポートに接続すると、画面が黒くなったり、ちらつきがあったりします。ThinOS 8.5_107 ビルドがこれに該当します。
回避策——DP1 ポートに接続したモニタのディスプレイ解像度を 4K 未満に設定します。これは DP1 ポート特有のことで、他のポートに接続したデバイスは無関係です。

6　リブートすると、Bluetooth ヘッドセットに再接続できません。再接続するには、ヘッドセットをリブートする必要があります。この機能は Intel の設計の通り作動します。
回避策——Bluetooth ヘッドセットを再開して再接続します。

7　シンクライアントを工場出荷時の設定に戻すと、Bluetooth デバイスに最初に接続したときに、Bluetooth 接続がエラーになる場合があります。ただしシンクライアントは、2 番目のインスタンス以降は、Bluetooth デバイスに接続します。

8　Bluetooth を初期化すると、クライアントの電源を切断して再度電源を入れる（動力サイクル）前に、1 度だけ画面が黒く点滅します。
ThinOS 8.5_108 ビルドがこれに該当します。この問題は次のリリースで解消されます。

USB サポート

USB ポート——USB 3.0 は USB 2.0 と互換性があります。USB 2.0 デバイスが 3.0 ポートに接続されている場合は、デバイスの動作に変更はありません。USB 3.0 デバイスを 3.0 ポートに接続するには、デバイスの種類が 5 Gbps のデバイスにする必要があります。すべての種類の USB デバイスが、USB 3.0 ポートとの接続時に動作します。

USB ハードディスク——USB ハードディスクを 10 個以上のドライブに差し込まないでください。または、10 個以上の USB キーを ThinOS クライアントに差し込まないでください。USB ディスクが 10 個以上のドライブに接続されると、ThinOS は USB ディスクを検知できません。

既知の問題——カメラのプレビューに既知の問題がいくつかあります。

USB Type-C のサポート

Wyse 5070 シンクライアントは、USB Type-C ポートをサポートします。

- USB 3.1 Type-C コネクタは、次の作業を実施するのに使用できます。
  - USB マスストレージを使用したデータ転送
  - モニタの接続

    メモ：USB Type-C を使用する場合、背面パネルからモニタ 1 台分が減少し、DP2 は無効になります。
  - スマートフォンへのチャージ
  - USB 2.0、3.0、および 3.1 互換デバイスへに接続します。
- USB 3.1 Type-C は、次の用途には使用できません。
  - Thunderbolt、HDMI Alt Mode、MHL Alt Mode
  - ドッキングステーション
  - シンクライアントの電力供給
- 制限——Wyse 5070 シンクライアントでは、XHCI がすべてのタイプの USB デバイスに使用されます。USB 3.0 と USB Type-C の転送速度の違いは軽微です。

プリンタ設定の設定

プリンタ設定ダイアログボックスを使用して、シンクライアントに接続されたネットワークプリンタおよびローカルプリンタを設定できます。USB ポートを介して、シンクライアントでは複数のプリンタをサポートできます。複数のプリンタを使用する場合にシンクライアントに余っているポートがなく、使用するポートを USB モデムコンバータで共有しなければならないときは、ポートに USB ハブを接続します。

次のオプションを使用して、プリンタ設定を設定します。

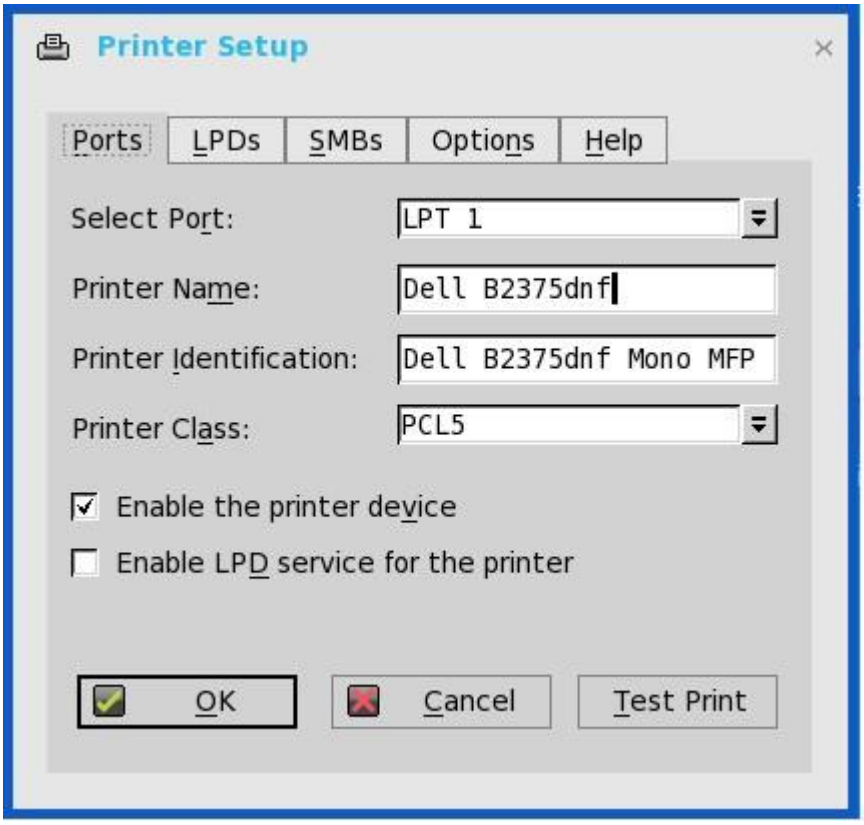
- ポート設定の設定
- LPD 設定の設定
- SMB 設定の設定
- プリンタ設定オプションの使用
- ヘルプの使用
- Citrix UPD プリンタの設定

ポート設定の設定

ポート設定を設定するには：

1 デスクトップメニューで**システム設定**をクリックし、**プリンタ**をクリックします。
プリンタ設定ダイアログボックスが表示されます。

2 **ポート**タブをクリックし、次のガイドラインに従います。



a **ポートの選択**——リストからポートを選択します。 **LPT1** または **LPT2** により、直接接続された USB プリンタへの接続を選択できます。

b **プリンタ名**——（必須）プリンタのリストに表示する名前を入力します。
USB に直接接続されたプリンタでは、ほとんどの場合、自動的にプリンタ名が報告または入力されます。

> ⓘ **メモ：このプリンタの LPD サービスを有効にするが選択されている場合、他のクライアントが LPR を使用してこのプリンタに印刷する際のキュー名になります。**

c **プリンタ ID**——大文字やスペースも含めて、Windows プリンタドライバの名前とまったく同じになるように、プリンタのタイプまたはモデルを入力します。USB に直接接続されたプリンタでは、ほとんどの場合、自動的にプリンタ識別情報が報告または入力されます。
ここには、Microsoft Windows システムのプリンタに対応するデバイスドライバ名か、デバイスドライバにマップするキーを入力する必要があります。指定していないと、Windows ホストとの接続時に、標準の直接接続の USB プリンタの場合は、デフォルトで名前はプリンタが提供する識別情報になり、USB 以外で接続されたプリンタの場合は **Generic / Text Only** になります。ドライバ名のマッピングは、システムによってグローバルプロファイル（wnos.ini）の一部として読み取られるプリンタマッピングファイルを介して行われるか、MetaFrame サーバによって MetaFrame プリンタ設定ファイル（¥winnt¥system32¥wtsprnt.inf）を介して行われます。

> ⓘ **メモ：プリンタ ID フィールドで使用できる文字数は最大 31 文字です。お使いのプリンタドライバの文字列が 31 文字より長い場合（空白を含む）、テキストファイル（printer.txt）を作成して、ファイルサーバにアップロードできます。テキストファイルを編集してその中に「"HP Color" = "HP Color LaserJet CM1312 MFP PCL6 Class Driver"」のように入力します。wnos.ini ファイルにコマンドライン「printermap=printer.txt」を追加します。これで、プリンタ ID フィールドに、ドライバの文字列全部を入力する代わりに、“HP Color”と入力できます。**

d **プリンタクラス**——これはオプションです。**PCL5**、**PS**、または **TXT** あるいは **PCL4** のリストからプリンタクラスを選択します。

e **プリンタデバイスを有効にする**——このオプションを選択して、直接接続のプリンタを有効にできます。リモートホストでデバイスを表示できます。

f **このプリンタの LPD サービスを有効にする**——これを選択して、シンクライアントをネットワークからの LPR 印刷要求に対応する LPD（Line Printer Daemon）ネットワークプリントサーバにします。

> ⓘ **メモ：**
> シンクライアントを LPD プリンタサーバとして使用する場合は、DHCP は使用しないで、静的 IP アドレスをクライアントに割り当てる必要があります。「ネットワーク設定の設定」を参照してください。

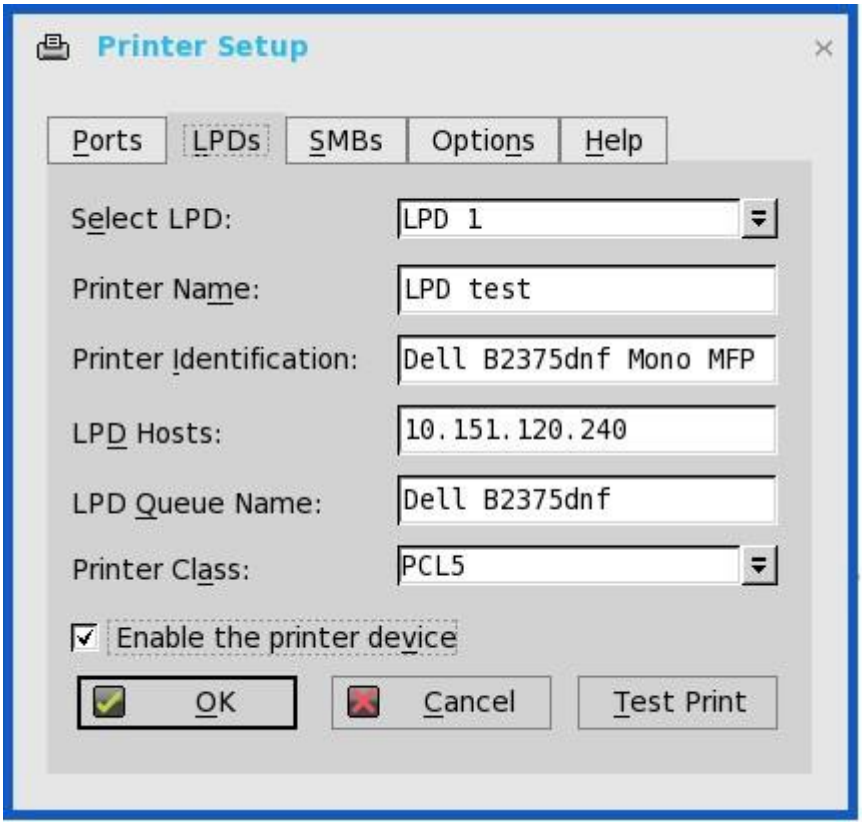
3 **OK** をクリックして設定を保存します。

LPD 設定の設定

LPD 設定を設定するには：

1 デスクトップメニューで**システム設定**をクリックし、**プリンタ**をクリックします。
プリンタ設定ダイアログボックスが表示されます。

2 Windows 以外のネットワークプリンタに印刷する場合は、**LPD** タブをクリックし、次のガイドラインに従います。



ⓘ **メモ：プリンタがラインプリンタ要求の印刷要求を受け付けられることを、ベンダーに確認してください。**

a **LPD ポートの選択**——リストからポートを選択します。

b **プリンタ名**——（必須）プリンタのリストに表示する名前を入力します。

c **プリンタ ID**——大文字やスペースも含めて、Windows プリンタドライバの名前とまったく同じになるように、プリンタのタイプまたはモデルを入力します。

この名前は、Microsoft Windows システムのプリンタに対応するデバイスドライバ名か、デバイスドライバにマップするキーにする必要があります。指定していないと、Windows ホストとの接続時に、標準の直接接続の USB プリンタの場合は、デフォルトで名前はプリンタが提供する識別情報になり、USB 以外で接続されたプリンタの場合は **Generic / Text** になります。ドライバ名のマッピングは、システムによってグローバルプロファイル（wnos.ini）の一部として読み取られるプリンタマッピングファイルを介して行われるか、MetaFrame サーバによって MetaFrame プリンタ設定ファイル（¥winnt¥system32¥wtsprnt.inf）を介して行われます。

d **LPD ホスト**——ネットワークプリンタ用のサーバの DNS 名または WINS 名です。ネットワーク上のプリンタの IP アドレスも、入力できます。
ネットワーク上でプリンタが別のシンクライアントに接続されている場合、LPD ホストボックスには、そのシンクライアントの名前またはアドレスを入力します。

e **LPD キュー名**——LPD ホストには、サポート対象のプリンタごとに名前付きのキューが保持されます。使用するプリンタと関連付けられたキューの名前を入力します。

この名前は、ベンダーごとに変えることができます。このフィールドは必須で、ネットワークプリンタが、送信されるプリンタジョブを正しく受け付けるために、正確に指定する必要があります。たとえば、HP LaserJet 4200n PCL6 の場合、HP の Web サイトにあるドキュメントに従って、auto を使用できます。

メモ：ネットワーク上でプリンタが別のシンクライアントに接続されている場合、LPD キュー名は、プリンタが接続されているシンクライアントのプリンタ名ボックスの内容と一致する必要があります。

f **プリンタクラス**——（オプション）リストからプリンタクラスを選択します。

g **プリンタデバイスを有効にする**——選択して、プリンタを有効にする必要があります。このオプションにより、デバイスは有効になり、リモートホストで表示されます。

3 **OK** をクリックして設定を保存します。

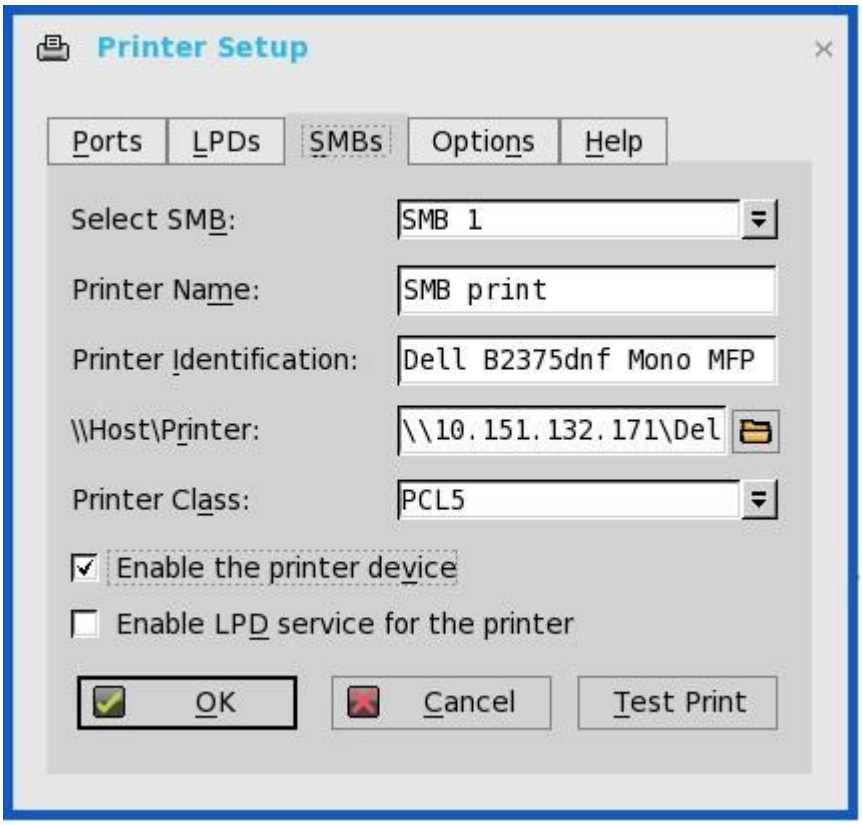
メモ：LPD プリンタが 1 つのセッションにマップされ、ユーザーが LPD サービスホストにアクセスできない場合、TCP 接続は LPD サービスホストへの接続を試みます。タイムアウト時間は 60 秒です。このタイムアウト時間中に、セッションを終了しようとすると、セッションは LPD プリンタの接続が確立するまで待機します。初期化エラーのログが表示されます。

SMB 設定の設定

SMB 設定を設定するには

1 デスクトップメニューで**システム設定**をクリックし、**プリンタ**をクリックします。
プリンタ設定ダイアログボックスが表示されます。

2 Windows のネットワークプリンタに印刷する場合は、**SMB** タブをクリックし、次のガイドラインに従います。



a **SMB の選択**——リストから SMB を選択します。

b **プリンタ名**——（必須）プリンタのリストに表示する名前を入力します。

c **プリンタ ID**——大文字やスペースも含めて、Windows プリンタドライバの名前とまったく同じになるように、プリンタのタイプまたはモデルを入力します。

この名前は、Microsoft Windows システムのプリンタに対応するデバイスドライバ名か、デバイスドライバにマップするキーにする必要があります。指定していないと、Windows ホストとの接続時に、標準の直接接続の USB プリンタの場合は、デフォルトで名前はプリンタが提供する識別情報になり、USB 以外で接続されたプリンタの場合は **Generic / Text** になります。ドライバ名のマッピングは、システムによってグローバルプロファイル（wnos.ini）の一部として読み取られるプリンタマッピングファイルを介して行われるか、MetaFrame サーバによって MetaFrame プリンタ設定ファイル（¥winnt¥system32¥wtsprnt.inf）を介して行われます。

d **¥¥Host¥Printer**——ホスト¥プリンタを入力するか、ボックスの横にあるフォルダ参照用のアイコンを使用して Microsoft ネットワークを参照し、使用可能なネットワークプリンタ（ネットワーク上の Windows プリントサーバの DNS 名または IP アドレス）からプリンタを選択します。

e **プリンタクラス**——（オプション）リストからプリンタクラスを選択します。

f **プリンタデバイスを有効にする**——選択して、プリンタを有効にする必要があります。このオプションにより、デバイスは有効になり、リモートホストで表示されます。

g **このプリンタの LPD サービスを有効にする**——これを選択して、シンクライアントをネットワークからの LPR 印刷要求に対応する LPD（Line Printer Daemon）ネットワークプリントサーバにします。「プリントサーバとしてのシンクライアントの使用（LPD）」を参照してください。

シンクライアントを LPD プリンタサーバとして使用する場合は、DHCP は使用しないで、「ネットワーク設定の設定」の説明に従って静的 IP アドレスをシンクライアントに割り当てる必要があります。

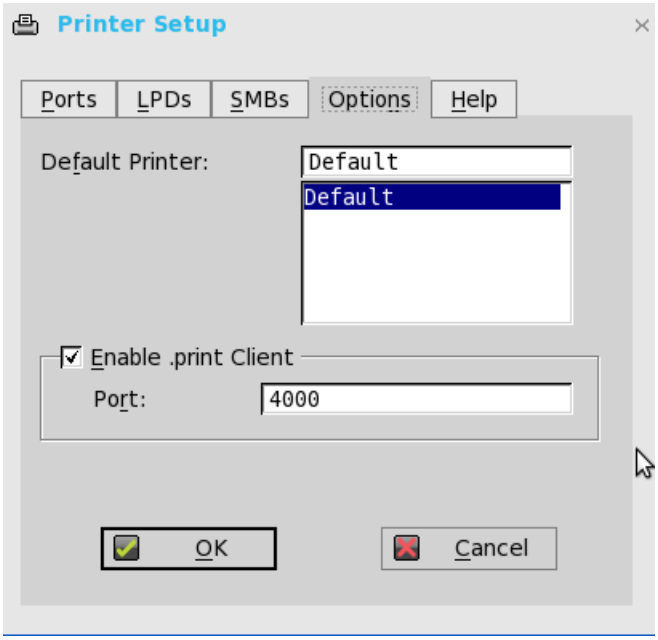
3 **OK** をクリックして設定を保存します。

プリンタ設定オプションの使用

プリンタ設定オプションを設定するには：

1 デスクトップメニューで**システム設定**をクリックし、**プリンタ**をクリックします。
プリンタ設定ダイアログボックスが表示されます。

2 **オプション**タブをクリックし、次のガイドラインに従います。



a **デフォルトプリンタ**——使用可能なプリンタのリストからデフォルトプリンタにするプリンタを選択します。

b **.print クライアントを有効にする**と**ポート**——print Client を有効にする場合は、**.print クライアントを有効にするのチェックボックス**をオンにし、**ポート**を入力します。

3 **OK** をクリックして設定を保存します。

ヘルプの使用

Help タブをクリックすると、テキストボックスに次のメッセージが表示されます。

Printer Identification is supplied by printer device.Change it to a Window’s printer driver name or setup a driver mapping file.

リセット機能

リセット機能では、次の操作を行うことができます。

- G キーリセットを使用した工場出荷時のデフォルトへのリセット
- シャットダウンリセットを使用した工場出荷時のデフォルトへのリセット
- V キーリセットを使用したディスプレイ設定のリセット

G キーリセットを使用した工場出荷時のデフォルトへのリセット

権限の強いユーザーまたはスタンドアロンユーザーは、G キーリセット機能を使用して、シンクライアントを工場出荷時のデフォルト設定にリセットできます。

シンクライアントを工場出荷時のデフォルト設定にリセットするには、シンクライアントをリスタートし、リスタート処理中に G キーを連続してタップします。G キーリセットは、ローカルの NV-RAM に定義されたネットワーク設定と接続だけでなく、それら以外を含むすべての設定項目に影響します。

メモ：ロックダウンモードでは、G キーリセットは、権限の弱いユーザーと権限のないユーザーに対して無効です。

シャットダウンリセットを使用した工場出荷時のデフォルトへのリセット

権限の強いユーザーまたはスタンドアロンユーザーは、**シャットダウン**ダイアログボックスからシンクライアントを工場出荷時のデフォルト設定にリセットできます。シンクライアントを工場出荷時のデフォルトにリセットするには

1 デスクトップメニューで、**シャットダウン**をクリックします。
シャットダウンダイアログボックスが表示されます。
2 **システムのシャットダウンと再起動**をクリックして、シンクライアントをリスタートします。
3 **システムを出荷時設定にリセットの項目に**チェックボックスをオンにして、システム設定を工場出荷時のデフォルト設定に復元します。
4 **OK** をクリックして設定を保存します。
シャットダウンリセットは、ローカルの NV-RAM に定義されたネットワーク設定と接続だけでなく、それら以外を含むすべての設定項目に影響します。ただし、ターミナル名は変更されません。

メモ：
ロックダウン状態であるかどうかに関係なく、シャットダウンリセットは、Privilege の Low ユーザと None ユーザに対して無効です。

V キーリセットを使用したディスプレイ設定のリセット

接続されている特定のモニタのディスプレイ設定が不適切な場合は、シンクライアントのリスタート時にディスプレイが適切に機能しない可能性があります。この状態を正しくするには、V キーを連続してタップしながらシンクライアントを電源投入します。これにより、シンクライアントがデフォルトまたは自動設定の画面解像度でリスタートします。

診断の実行

診断には、以下が必要です。

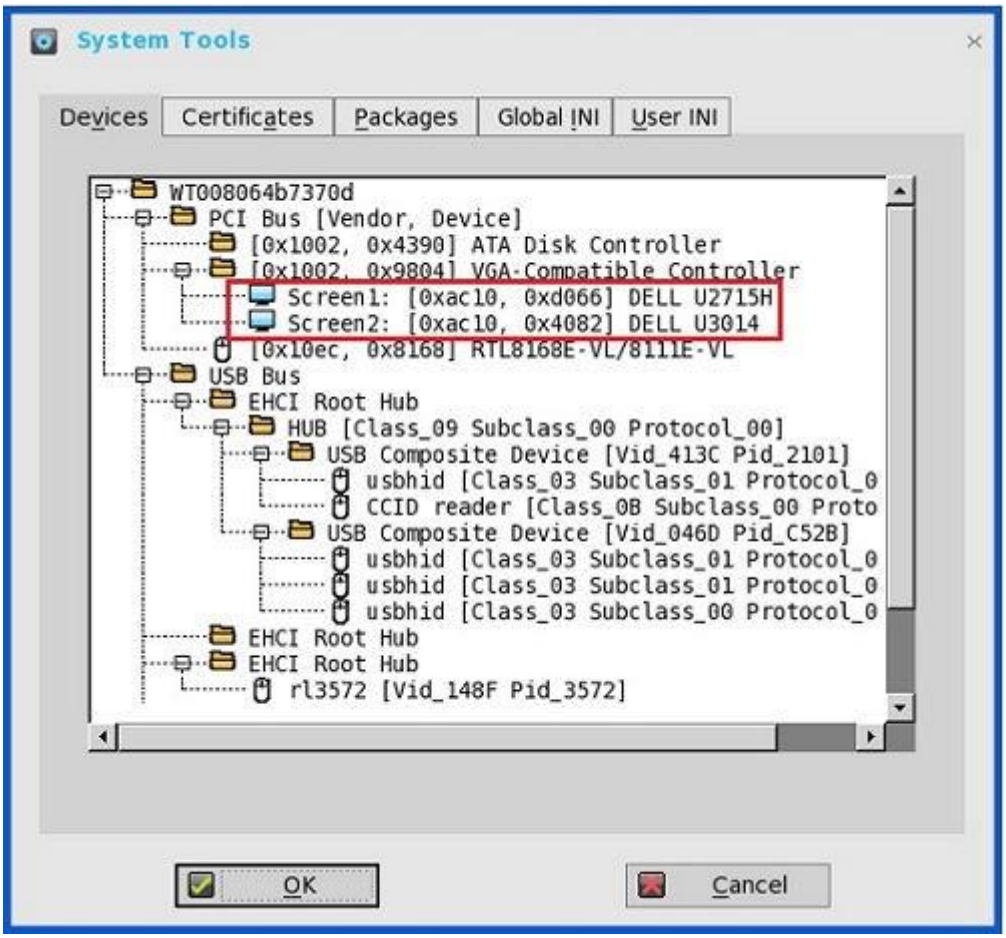
- システムツール
- トラブルシューティングのオプションの使用

システムツール

システムツールダイアログボックスを使用して、デバイス詳細、パッケージ詳細および Global INI／User INI 情報を表示します。**証明書**タブを使用して証明書をインポートすることもできます。

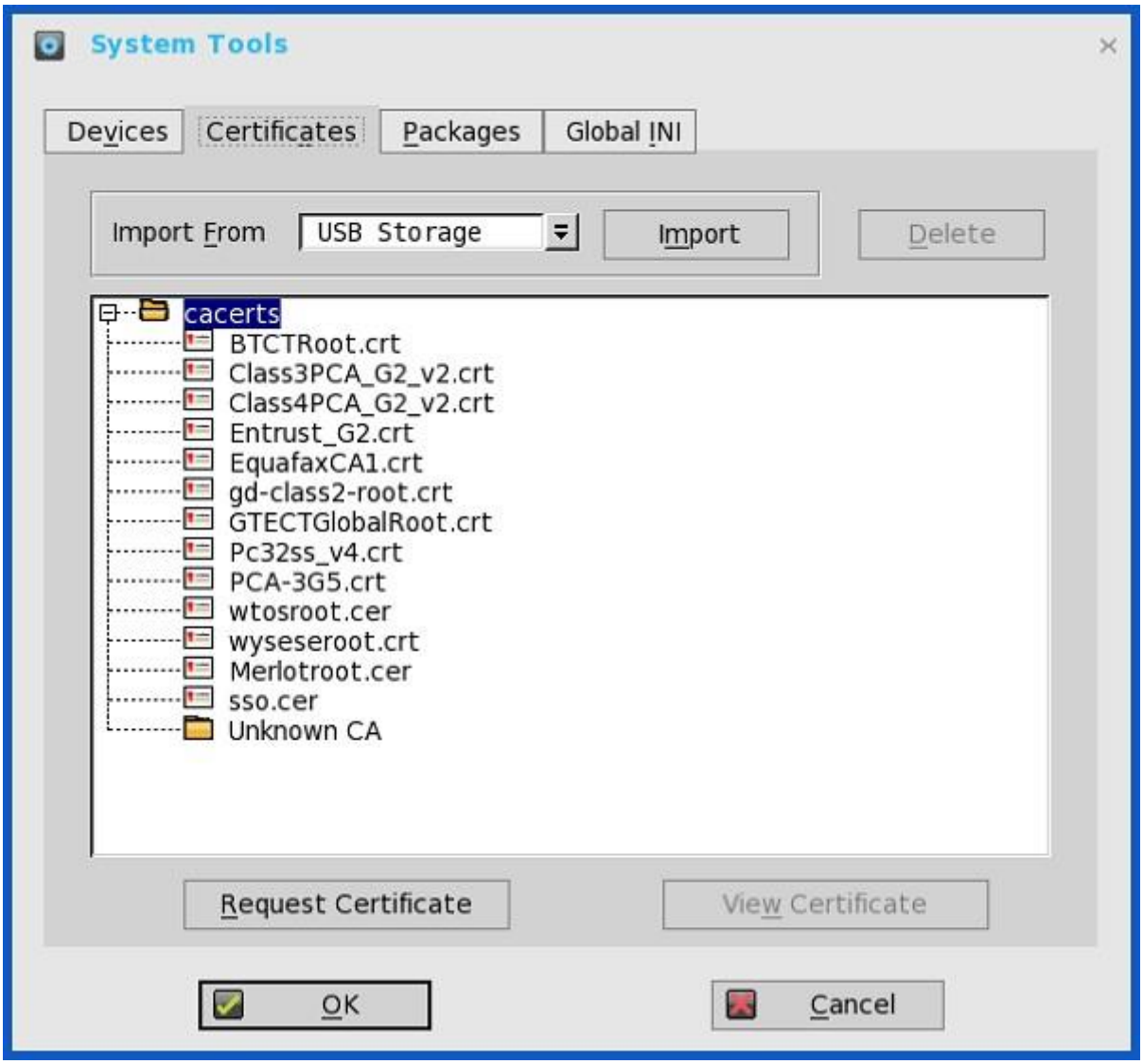
1 デスクトップメニューで、**システムツール**をクリックします。
システムツールダイアログボックスが表示されます。

2 **デバイス参照**タブをクリックし、該当するプラットフォームの USB、シリアルおよびパラレルなど、ローカルで接続されているデバイスをすべて表示します。シンクライアントに接続されているモニタの詳細も表示されます。
Device Viewer ボタンは、以前は**システム情報**ダイアログボックスの**デバイス参照**タブで使用できました。



メモ：ミラーファイルサーバタブは Global Ini タブから表示できるようになったため、システムツールダイアログボックスからは削除されました。

3 **証明書**タブをクリックし、次のガイドラインに従います。



a 証明書をインポートするには、USB Storage または File Server のいずれかをドロップダウンリストから選択し、**登録**をクリックして必要な証明書をインポートします。

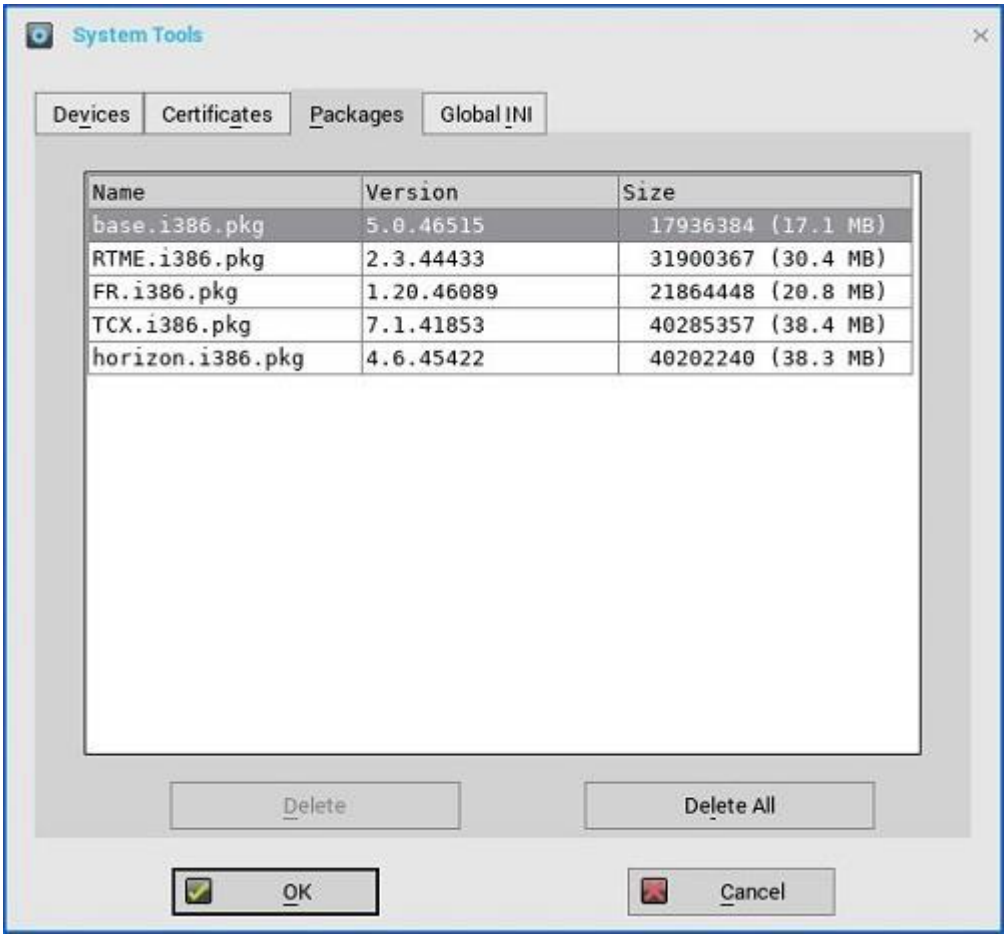
b インポートした証明書を削除するには、**削除**をクリックします。

c バージョン、有効期間およびシリアル番号など、インポートした証明書の情報を表示するには、**証明書参照**をクリックします。証明書のパスと証明書のステータスも表示できます。デフォルト証明書の詳細については、「デフォルト証明書について」を参照してください。

d **証明書の要求**をクリックし、手動でクライアントの証明書を要求します。Simplified Certificate Enrollment Protocol の詳細については、「Simplified Certificate Enrollment Protocol」を参照してください。

4 **パッケージ**タブをクリックし、次のガイドラインに従います。

シンクライアントにインストールされている ThinOS パッケージが、**パッケージ**タブに表示されます。



a **削除**ボタンをクリックし、選択したパッケージを削除します。

b **すべて削除**ボタンをクリックし、すべてのパッケージを削除します。

次のパッケージが、**パッケージ**タブに表示されます。

- base.i386.pkg
- FR.i386.pkg——このパッケージは、Flash リダイレクトをサポートするために導入されます。
- RTME.i386.pkg——このパッケージは、Citrix RTME および VMware Realtime Audio-Video をサポートするために導入されます。
- Horizon.i386.pkg——このパッケージは、VMware Blast プロトコルをサポートするために導入されます。パッケージのバージョン番号は、最新の Horizon クライアントと一致するように更新されます。

このパッケージをインストールするには、PKG インストール INI ファイルを、AddPkg=“horizon”に変更する必要があります。

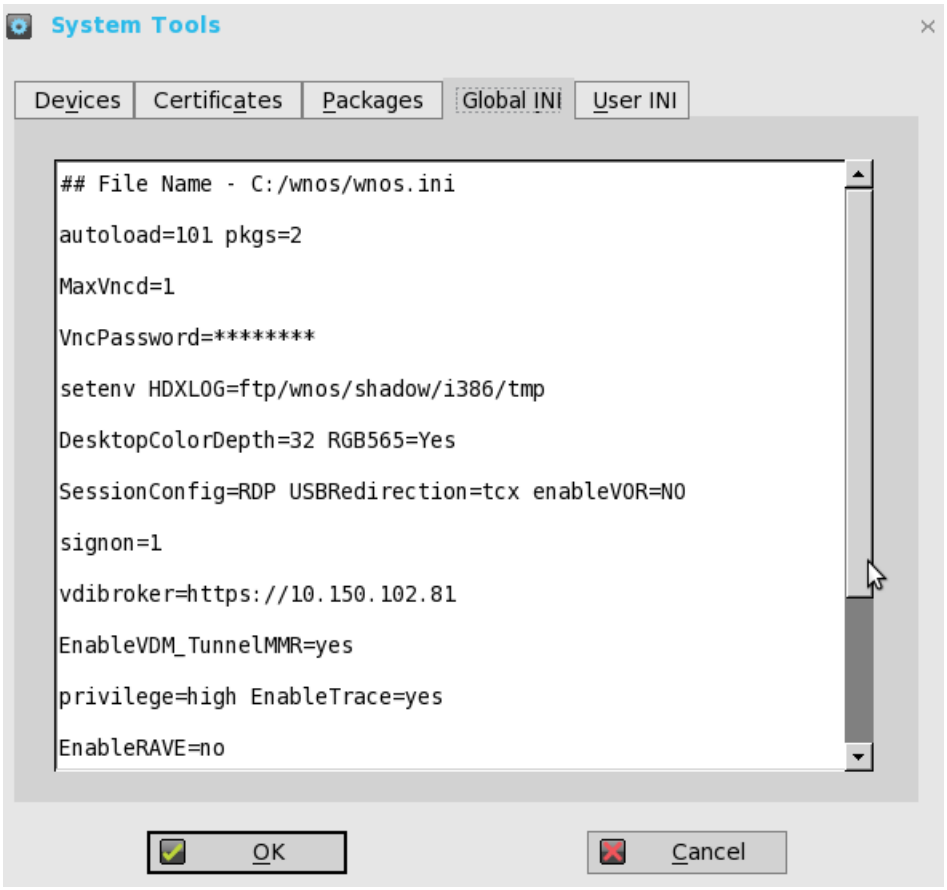
- pcoip.i386.pkg——このパッケージは、PCoIP 対応クライアントにのみ利用できます。
- TCX.i386.pkg——このパッケージは、TCX をサポートするために導入されます。

ベースパッケージを個別に削除することはできません。**すべて削除**をクリックすると、ベースパッケージを含む、すべてのパッケージが削除されます。**すべて削除**をクリックすると、デバイスの再起動を要求するメッセージが表示されます。

base.i386.pkg はすべての ThinOS クライアントで必須です。現時点では、PCoIP 対応のシンクライアントには PCoIP パッケージが必須です。その他のパッケージはオプションです。ベースパッケージと PCoIP パッケージは、ThinOS ファームウェアイメージに統合されています。最新の ThinOS ファームウェアイメージをインストールすると、これらのパッケージの最新バージョンが ThinOS クライアントに自動でインストールされます。これらの埋め込み型パッケージを手動でインストールしたり、アップグレードしたりすることはできません。ただし、各パッケージのパッケージバージョンの詳細は、エンジニアリング情報の目的でのみ、**パッケージ**タブに表示されます。

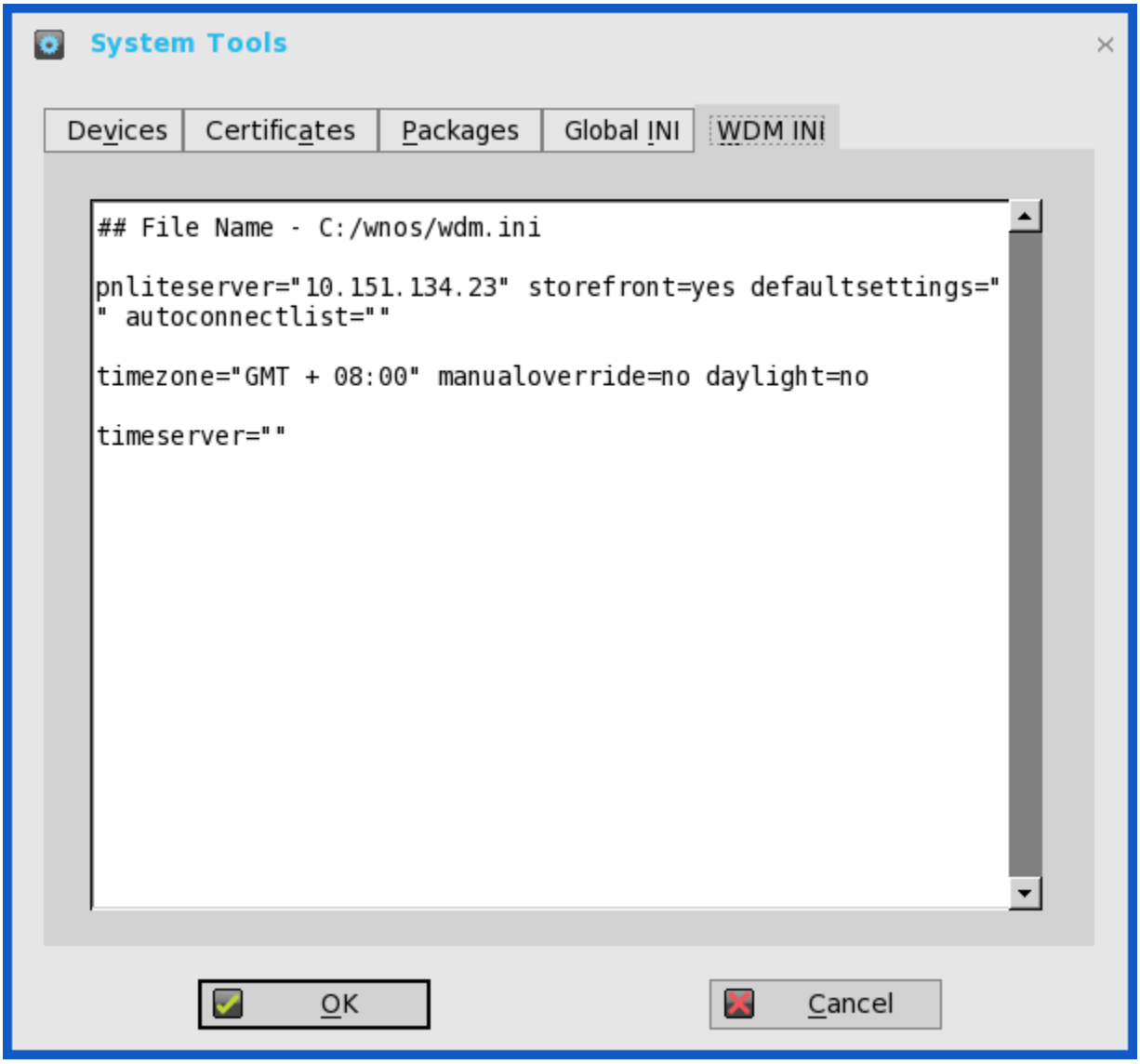
メモ：ThinOS がリリースされるごとに、パッケージが最新バージョンに更新される可能性があります。最新のパッケージのバージョン情報については、最新の『Dell Wyse ThinOS リリースノート』を参照してください。

5 **Global INI** タブをクリックし、wnos.ini の情報を表示します。



6 **User INI** タブをクリックし、wnos.ini の情報を表示します。

7 **WMS INI** をクリックし、受信した WMS 設定を表示します。



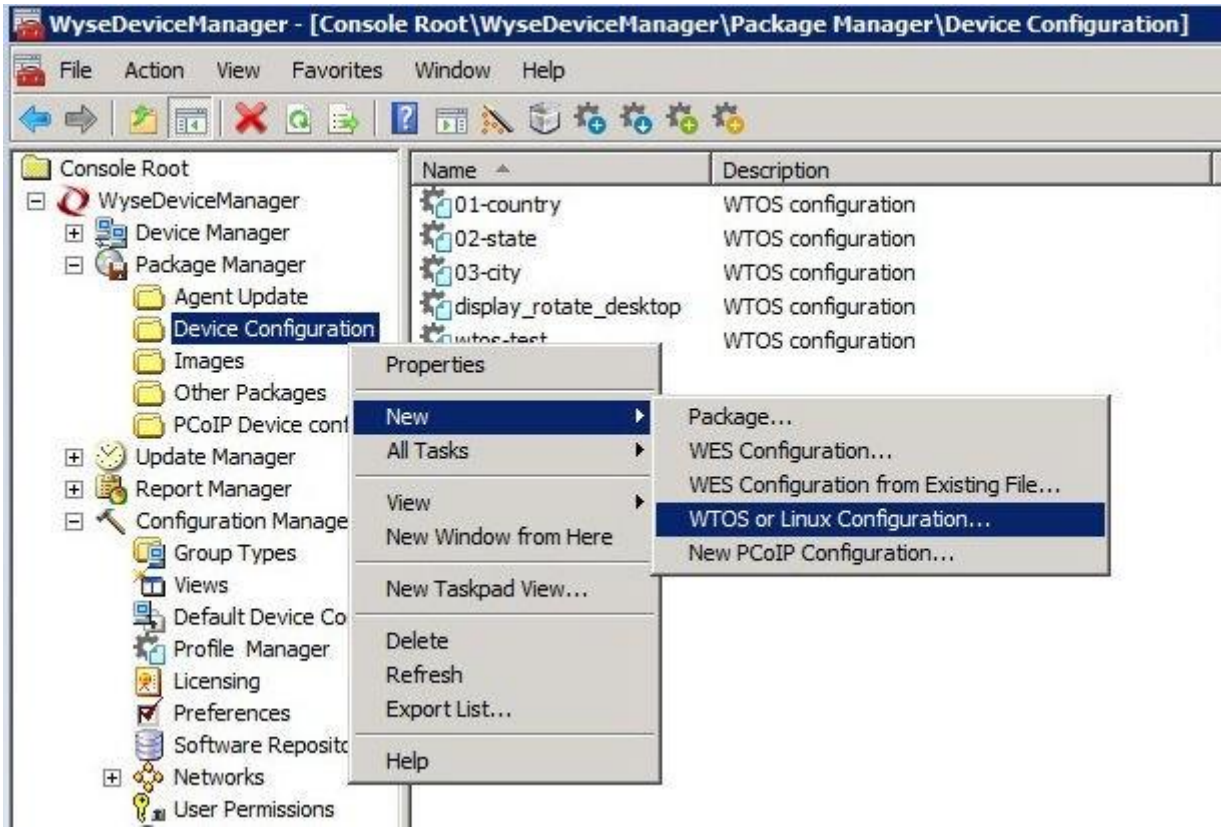
WCM 機能は、総合的なクライアントの設定を行うために WDM からサポートされます。可能な場合、クライアントはサーバからの設定なく、キャッシュした設定（wdm.ini）をロードします。

制限

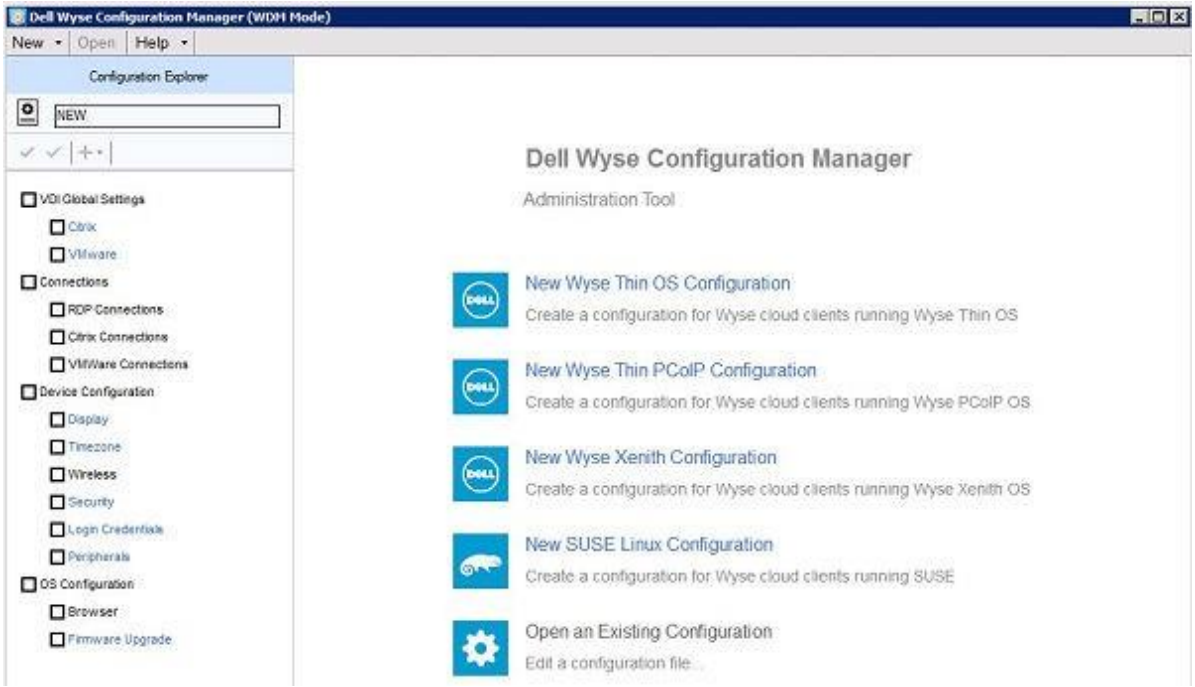
WCM でファームウェアやイメージをアップグレードまたはダウングレードするには、WDM Configuration Manager の WTOS 環境設定の **WTOS INI path upon checkin (FTP/HTTPS/HTTP/CIFS)**チェックボックスをオンにして、WDM ファイルサーバ機能を有効にする必要があります。

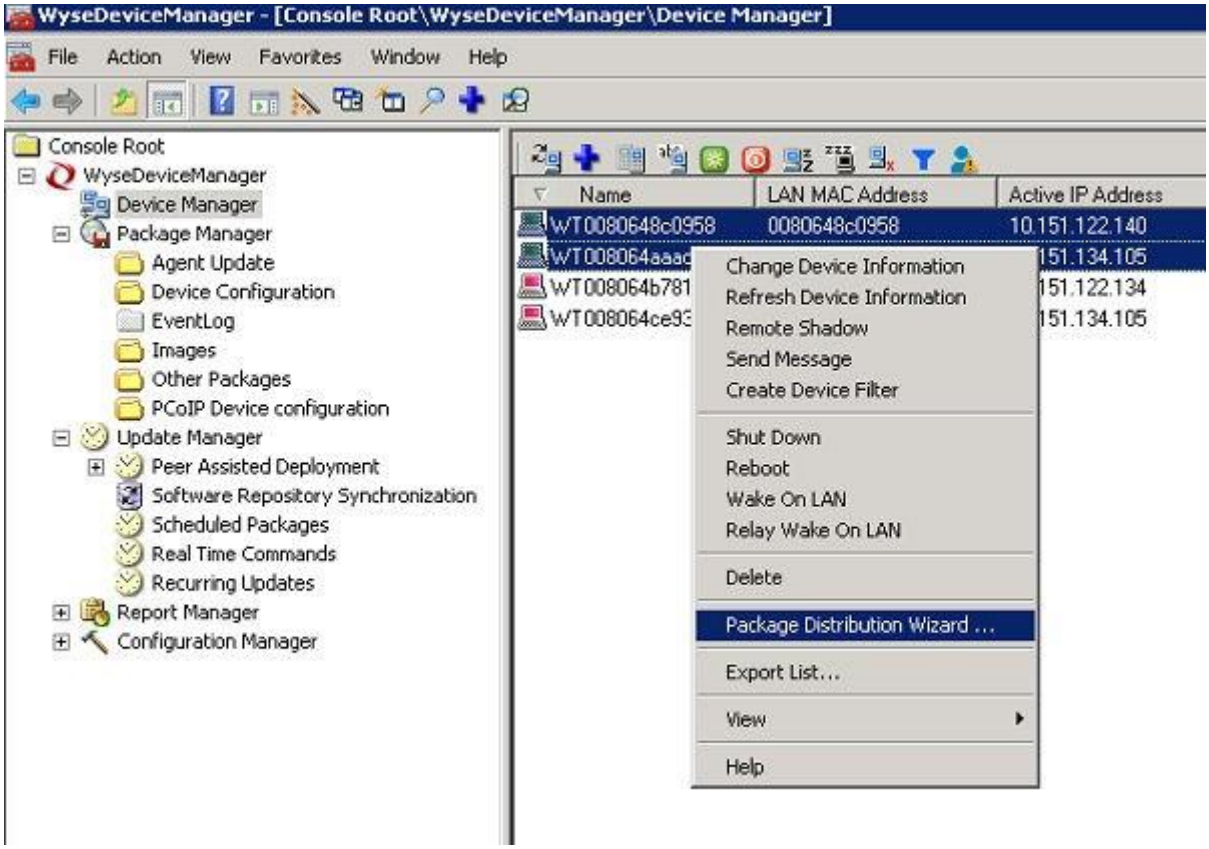
ユーザーのシナリオ

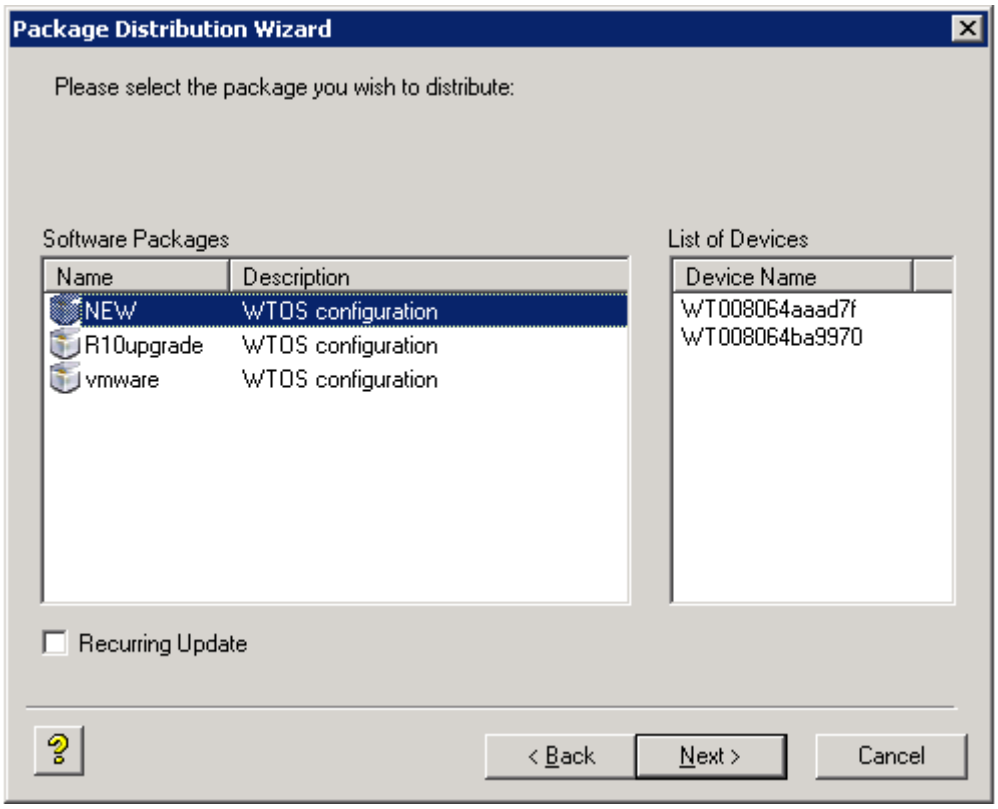
a　WCM（JSON）からクライアント設定を作成または編集します。



b　対象デバイスを選択し、**Package Distribution Wizard** から構成設定を発行します。







Wyse Device Manager（WDM）の Package Manager および Profile Manager の詳細については、『WDM 管理者ガイド』を参照してください。

8 **OK** をクリックして設定を保存します。

Simplified Certificate Enrollment Protocol

Simplified Certificate Enrollment Protocol（SCEP）は、すべてのエンドポイントが信頼できる、クローズドネットワークで使用するように設計されました。SCEP の目的は、拡張性のある方法で、証明書をネットワークデバイスに安全に発行するのを支援することです。企業ドメイン内で、ドメイン資格のないネットワークデバイスが、Certification Authority（CA）の証明書を登録できるようにします。

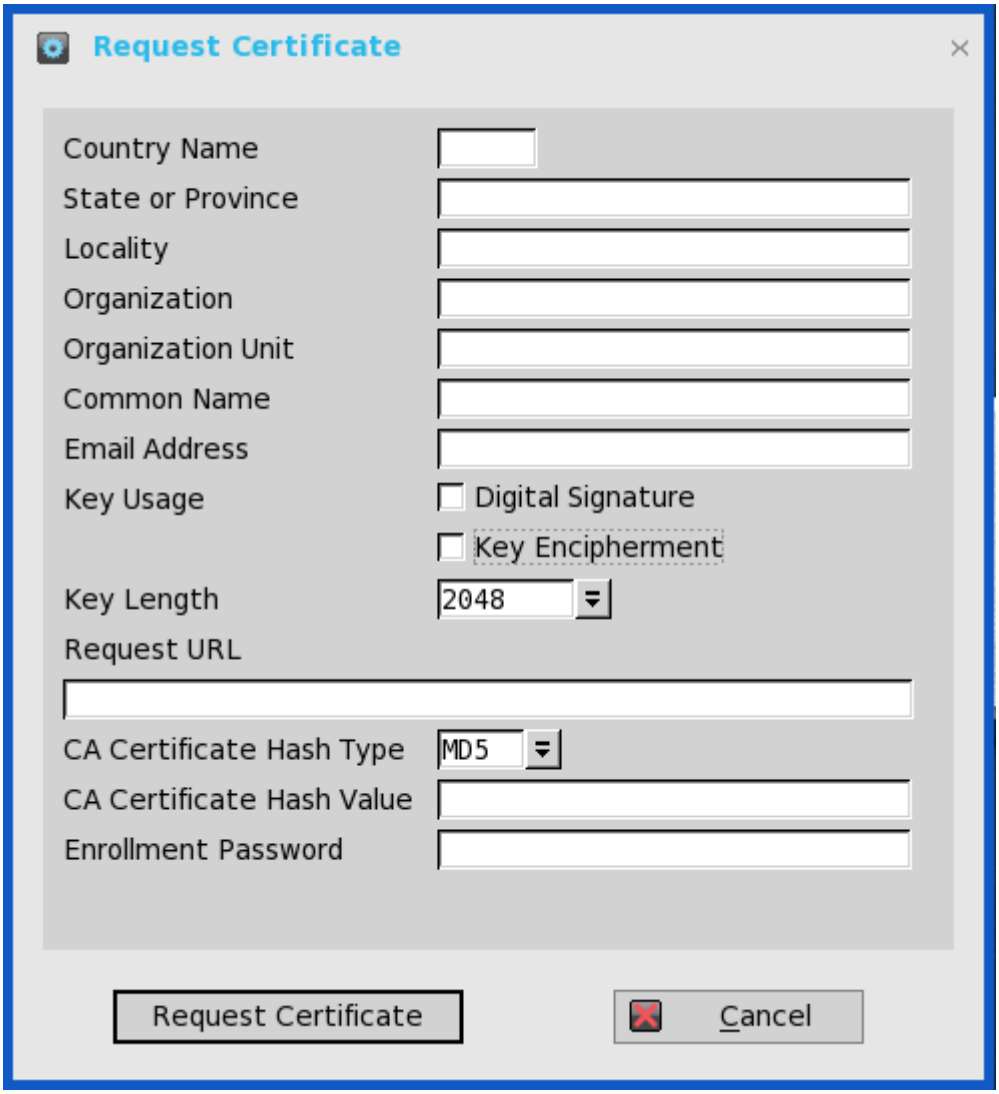
このプロトコルで定義されたトランザクションの最後で、ネットワークデバイスは、CA が発行したプライベートキーとそれに関連付けられた証明書を取得します。デバイスのアプリケーションは、そのキーと関連付けられた証明書を使用して、ネットワークの他のエンティティと情報のやり取りをします。このネットワークデバイスの証明書が最もよく使われるのは、IPSec セッションでのデバイス認証です。

ThinOS はネットワークデバイスとして扱われます。ThinOS SCEP の機能には、手動証明書要求、自動証明書要求、および自動証明書更新があります。

証明書を手動で要求

証明書を手動で要求するには、次の操作を行います。

1 **システムツール** > **証明書** >**証明書の要求**の順に進みます。
証明書の要求ダイアログボックスが表示されます。



2 **証明書の要求**ダイアログボックスに適切な値を入力し、**証明書の要求**ボタンをクリックします。
証明書要求がサーバに送信され、クライアントはサーバからの回答を受信し、CA 証明書とクライアント証明書の両方をインストールします。

3 **OK** をクリックして変更を保存します。

メモ：

- CA 証明書ハッシュ型タイプは現在、MD5、SHA1 および SHA256 をサポートしています。
- 要求サーバの URL は、HTTP リンクでも HTTPs リンクでも可能です。URL の前にプロトコルプレフィックスを付けることができます。

証明書を自動的に要求

INI パラメータを使用して、証明書の**要求と更新**処理を自動化します。関連する INI パラメータはグローバルスコープで、INI パラメータ ScepAutoEnroll と共に使用する必要があります。

INI パラメータの使用の詳細については、最新の『Dell Wyse ThinOS INI Reference Guide』を参照してください。

デフォルト証明書について

ThinOS の中にあるデフォルト証明書が**証明書**ダイアログボックスに表示されます。デフォルト証明書を表示するには、ThinOS を工場出荷時の設定に設定し、デスクトップで、**システム設定 > システムツール > 証明書**を順にクリックします。次のデフォルト証明書が、**cacerts** フォルダに、拡張可能なツリー構造フォーマットで表示されます。

- BTCTRoot.crt
- Class3PA_G2_v2.crt
- Class4PA_G2_v2.crt
- Entrust_G2.crt
- EquafaxCA1.crt
- gd-class2–root.crt
- GTECTGlobalRoot.crt
- Pc32ss_v4.crt
- PCA-3G5.crt

各証明書を表示するには、表示する証明書を選択して、**証明書参照**をクリックします。**証明書**ダイアログボックスで、次のタブのいずれかをクリックして対応する証明書の属性を表示します。

1 **全般**——次の値が表示されます。
   - 証明書の目的
   - 証明書の発行先
   - 証明書の発行元
   - 証明書の有効期間
2 **詳細**——証明書の詳細が、対応するデフォルト値と共に表示されています。個別の証明書の詳細については、「**証明書の詳細**」セクションを参照してください。
3 **証明のパス**——証明書が保管されているフォルダのパスが表示されます。証明書の状況は、ウィンドウの下部のペインに表示できます。

証明書の詳細

このセクションでは、証明書とその有効な属性、対応するデフォルト値を記載します。

証明書の名前——BTCTRoot.crt

表 28. BTCTRoot.crt Certificate の詳細

証明書のフィールド	デフォルト値／フォーマット
バージョン	V3
シリアル番号	02 00 00 b9
署名アルゴリズム	sha1RSA
発行者	Baltimore CyberTrust Root CN=Baltimore CyberTrust Root OU=CyberTrust O=Baltimore

証明書のフィールド	デフォルト値／フォーマット
	C=IE
有効期限の開始	2000–05–12 18:46:00
有効期限の終了	2025–05–12 23:59:00
サブジェクト	Baltimore CyberTrust Root CN=Baltimore CyberTrust Root OU=CyberTrust O=Baltimore C=IE
公開キー	RSA（2048 ビット）。 キーのビット数は、ウィンドウ下部のペインに表示されています。
キー使用法	証明書の検証、CRL の署名検証
サブジェクトキー識別子	e5 9d 59 30 82 47 58 cc ac fa 08 54 36 86 7b 3a b5 04 4d f0
基本制限	Subject Type=CA, Path Length Constraints=None
サムプリントアルゴリズム	sha1
拇印	d4 de 20 d0 5e 66 fc 53 fe la 50 88 2c 78 db 28 52 ca e4 74

証明書の名前——Class3PCA_G2_v2.crt

表 29. Class3PCA_G2_v2.crt Certificate の詳細

証明書のフィールド	デフォルト値／フォーマット
バージョン	V1
シリアル番号	7d d9 fe 07 cf a8 le b7 10 79 67 fb a7 89 34 c6
署名アルゴリズム	sha1RSA
発行者	VeriSign Trust Network OU=VeriSign Trust Network OU=(c) 1998 VeriSign, Inc. – For authorized use only OU=Class 3 Public Primary Certification Authority – G2 O=VeriSign, Inc C=US
有効期限の開始	1998–05–18 00:00:00
有効期限の終了	2028–08–12 23:59:59
サブジェクト	VeriSign Trust Network OU=VeriSign Trust Network OU=(c) 1998 VeriSign, Inc. – For authorized use only OU=Class 3 Public Primary Certification Authority – G2 O=VeriSign, Inc

証明書のフィールド	デフォルト値／フォーマット
	C=US
公開キー	RSA（1024 ビット）。 キーのビット数は、ウィンドウ下部のペインに表示されています。
拇印アルゴリズム	sha1
拇印	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

証明書の名前——Class4PCA_G2_v2.crt

表 30. Class4PCA_G2_v2.crt Certificate の詳細

証明書のフィールド	デフォルト値／フォーマット
バージョン	V1
シリアル番号	32 88 8e 9a d2 f5 eb 13 47 f8 7f c4 20 37 25 f8
署名アルゴリズム	sha1RSA
発行者	VeriSign Trust Network OU=VeriSign Trust Network OU=(c) 1998 VeriSign, Inc. – For authorized use only OU=Class 4 Public Primary Certification Authority – G2 O=VeriSign, Inc C=US
有効期限の開始	1998–05–18 00:00:00
有効期限の終了	2028–05–01 23:59:59
サブジェクト	VeriSign Trust Network OU=VeriSign Trust Network OU=(c) 1998 VeriSign, Inc. – For authorized use only OU=Class 4 Public Primary Certification Authority – G2 O=VeriSign, Inc C=US
公開キー	RSA（1024 ビット）。 キーのビット数は、ウィンドウ下部のペインに表示されています。
拇印アルゴリズム	sha1
拇印	0b 77 be bb cb 7a a2 47 05 de cc 0f bd 6a 02 fc 7a bd 9b 52

証明書の名前——Entrust_G2.crt

表 31. Entrust_G2.crt Certificate の詳細

証明書のフィールド	デフォルト値／フォーマット
バージョン	V3
シリアル番号	4a 53 8c 28
署名アルゴリズム	sha256RSA
発行者	Entrust Root Certification Authority CN=Entrust Root Certification Authority—G2 OU=(c) 2009 Entrust, Inc. – For authorized use only OU=www.entrust.net/legal-terms を参照してください。 O=Entrust, Inc. C=US
有効期限の開始	2009–07–07 17:25:54
有効期限の終了	2030–12–07 17:55:54
サブジェクト	Entrust Root Certification Authority CN=Entrust Root Certification Authority—G2 OU=(c) 2009 Entrust, Inc. – For authorized use only OU=www.entrust.net/legal-terms を参照してください。 O=Entrust, Inc. C=US
公開キー	RSA（2048 ビット）。 キーのビット数は、ウィンドウ下部のペインに表示されています。
キー使用法	証明書の検証、CRL の署名検証
サブジェクトキー識別子	6a 72 26 7a d0 1e ef 7d e7 3b 69 51 d4 6c 8d 9f 90 12 66 ab
基本制限	Subject Type=CA, Path Length Constraints=None
拇印アルゴリズム	sha1
拇印	8c f4 27 fd 79 0c 3a d1 66 06 8d e8 1e 57 ef bb 93 22 72 d4

証明書の名前——EquafaxCA1.crt

表 32. EquafaxCA1.crt Certificate の詳細

証明書のフィールド	デフォルト値／フォーマット
バージョン	V3
シリアル番号	04
署名アルゴリズム	md5RSA
発行者	Equifax Secure eBusiness CN=Equifax Secure eBusiness CA-1 0=Equifax Secure Inc.

証明書のフィールド	デフォルト値／フォーマット
	C=US
有効期限の開始	1999–06–21 04:00:00
有効期限の終了	2020–06–21 04:00:00
サブジェクト	Equifax Secure eBusiness CN=Equifax Secure eBusiness CA-1 0=Equifax Secure Inc. C=US
公開キー	RSA（1024 ビット）。 キーのビット数は、ウィンドウ下部のペインに表示されています。
キー使用法	デジタル署名、キー暗号化、データ暗号化、キーの共有、証明書の署名、CRL の署名、暗号化専用、復号専用
サブジェクトキー識別子	4a 78 32 52 11 db 59 16 36 5e df c1 14 36 40 6a 47 7c 4c a1
認証局鍵識別子	80 14 4a 78 32 52 11 db 59 16 36 5e df c1 14 36 40 6a 47 7c 4c a1
基本制限	Subject Type=CA, Path Length Constraints=None
拇印アルゴリズム	sha1
拇印	da 40 18 8b 91 89 a3 ed ee ae da 97 fe 2f 9d f5 b7 d1 8a 41

証明書の名前——gd-class2–root.crt

表 33. gd-class2–root.crt Certificate の詳細

証明書のフィールド	デフォルト値／フォーマット
バージョン	V3
シリアル番号	00
署名アルゴリズム	sha1RSA
発行者	Go Daddy Class 2 Certification Authority OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US
有効期限の開始	2004–06–29 17:06:20
有効期限の終了	2034–06–29 17:06:20
サブジェクト	Go Daddy Class 2 Certification Authority OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US
公開キー	RSA（2048 ビット）。 キーのビット数は、ウィンドウ下部のペインに表示されています。

証明書のフィールド	デフォルト値／フォーマット
キー使用法	デジタル署名、キー暗号化、データ暗号化、キーの共有、証明書の署名、CRL の署名、暗号化専用、復号専用
サブジェクトキー識別子	d2 c4 b0 d2 91 d4 4c 11 71 b3 61 cb 3d a1 fe dd a8 6a d4 e3
認証局鍵識別子	キーのビット数は、ウィンドウ下部のペインに表示されています。
基本制限	Subject Type=CA, Path Length Constraints=None
拇印アルゴリズム	sha1
拇印	27 96 ba e6 3f 18 01 e2 77 26 1b a0 d7 77 70 02 8f 20 ee e4

証明書の名前——GTECTGlobalRoot.crt

表 34. GTECTGlobalRoot.crt Certificate の詳細

証明書のフィールド	デフォルト値／フォーマット
バージョン	V1
シリアル番号	01 a5
署名アルゴリズム	md5RSA
発行者	GTE CyberTrust Global Root CN=GTE CyberTrust Global Root OU=GTE CyberTrust Solutions, Inc. O=GTE Corporation C=US
有効期限の開始	1998–08–13 00:29:00
有効期限の終了	2018–08–13 23:59:00
サブジェクト	GTE CyberTrust Global Root CN=GTE CyberTrust Global Root OU=GTE CyberTrust Solutions, Inc. O=GTE Corporation C=US
拇印アルゴリズム	sha1
拇印	97 81 79 50 d8 1c 96 70 cc 34 d8 09 cf 79 44 31 36 7e f4 74

証明書の名前——Pc32ss_v4.crt

表 35. Pc32ss_v4.crt Certificate の詳細

証明書のフィールド	デフォルト値／フォーマット
バージョン	V1
シリアル番号	70 ba e4 1d 10 d9 29 34 b6 38 ca 7b 03 cc ba bf
署名アルゴリズム	md2RSA

証明書のフィールド	デフォルト値／フォーマット
発行者	Class 3 Public Primary Certification Authority OU=Class 3 Public Primary Certification Authority O=VeriSign, Inc. C=US
有効期限の開始	1996–01–29 00:00:00
有効期限の終了	2028–08–01 23:59:59
サブジェクト	Class 3 Public Primary Certification Authority OU=Class 3 Public Primary Certification Authority O=VeriSign, Inc. C=US
公開キー	RSA（1024 ビット）。 キーのビット数は、ウィンドウ下部のペインに表示されています。
拇印アルゴリズム	sha1
拇印	74 2c 31 92 e6 07 e4 24 eb 45 49 54 2b e1 bb c5 3e 61 74 e2

証明書の名前——PCA-3G5.crt

表 36. PCA-3G5.crt Certificate の詳細

証明書のフィールド	デフォルト値／フォーマット
バージョン	V3
シリアル番号	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
署名アルゴリズム	sha1RSA
発行者	VeriSign Class 3 Public Primary Certification Authority — G5 CN=VeriSign Class 3 Public Primary Certification Authority — G5 OU=(c) 2006 VeriSign, Inc. – For authorized use only OU=VeriSign Trust Network O=VeriSign, Inc C=US
有効期限の開始	2006–11–08 00:00:00
有効期限の終了	2036–07–16 23:59:00
サブジェクト	VeriSign Class 3 Public Primary Certification Authority — G5 CN=VeriSign Class 3 Public Primary Certification Authority — G5 OU=(c) 2006 VeriSign, Inc. – For authorized use only OU=VeriSign Trust Network O=VeriSign, Inc C=US

証明書のフィールド	デフォルト値／フォーマット
公開キー	RSA（2048 ビット）。 キーのビット数は、ウィンドウ下部のペインに表示されています。
キー使用法	証明書の検証、CRL の署名検証
サブジェクトキー識別子	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
基本制限	Subject Type=CA, Path Length Constraints=None
拇印アルゴリズム	sha1
拇印	4e b6 d5 78 49 9b 1c cf 5f 58 le ad 56 be 3d 9b 67 44 a5 e5

トラブルシューティングのオプションの使用

システム診断ダイアログボックスを使用して、追跡およびイベントログの設定、クライアントの CPU とメモリ、ネットワーク情報を表示するパフォーマンスモニタのグラフ、および CMOS 管理による設定の抽出と復元を設定できます。また、トラブルシューティングの目的で、wnos.ini のキャッシュされた情報を表示することもできます。

トラブルシューティングのオプションの使用：

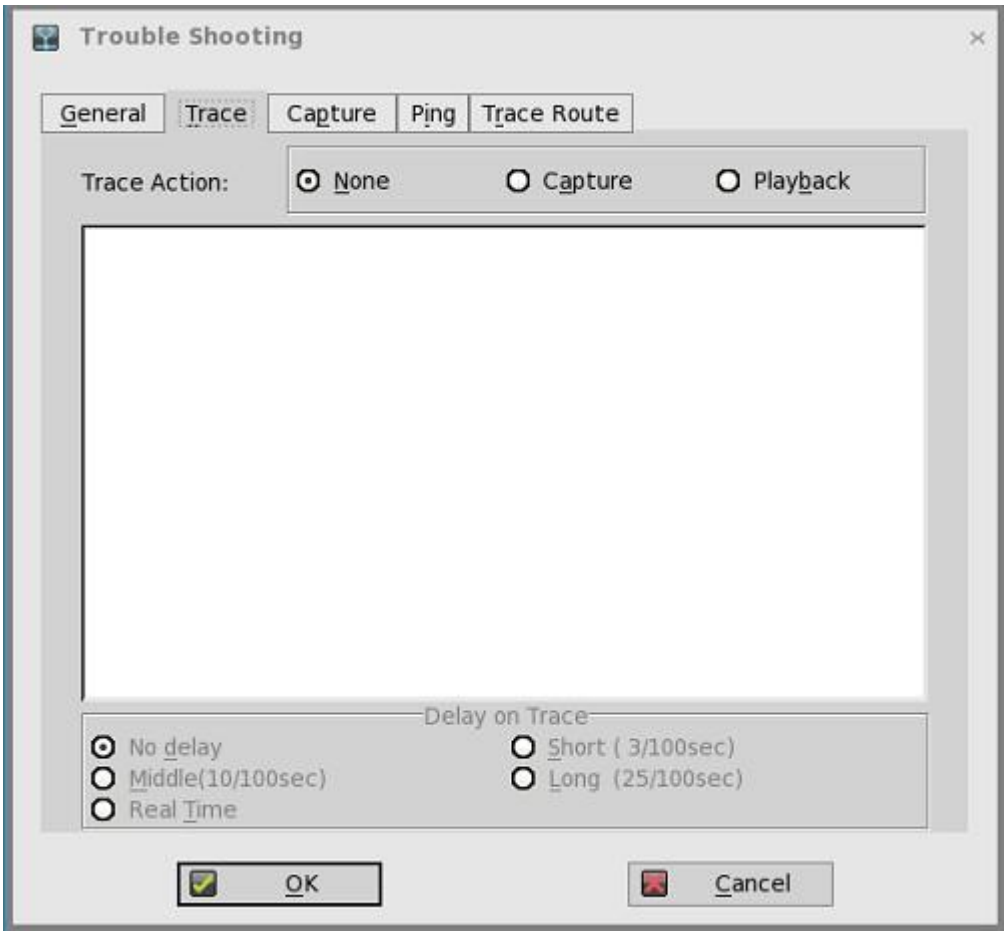
1 デスクトップメニューで、システム設定の**システム診断**をクリックします。
システム診断ダイアログボックスが表示されます。

2 **全般**タブをクリックし、次のガイドラインに従います。

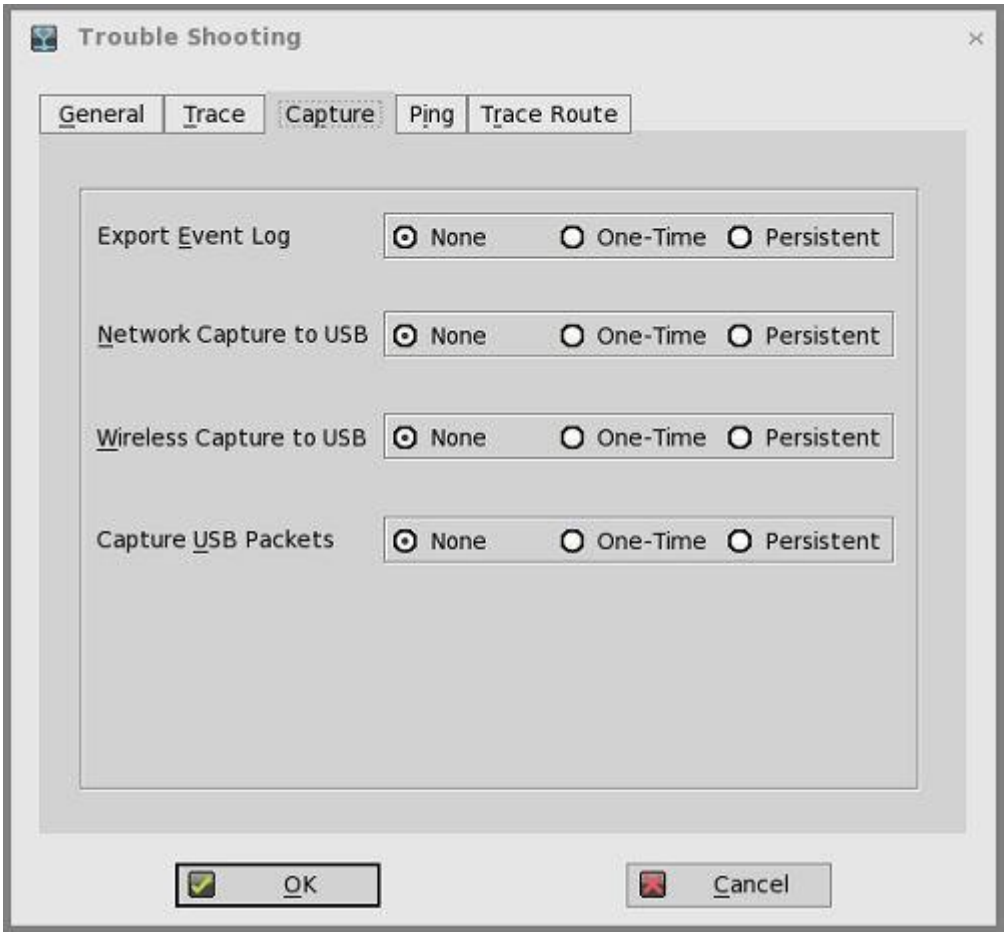
- CMOS 管理で使用するターゲットデバイスを選択するには、**USB** または **File Server** のいずれかをクリックします。

- **CMOS のバックアップ**——このオプションをクリックすると、選択した目的のデバイスに基づいて、CMOS 設定が USB キーまたはファイルサーバに抽出されます。
- **CMOS のリストア**——このオプションをクリックすると、CMOS 設定が USB キーからターゲットシンクライアントに書き込まれます。
- **パフォーマンスモニタ**——このオプションをクリックすると、シンクライアントの CPU、メモリおよびネットワーク情報が表示されます。グラフは、すべてのウィンドウで最上部に表示されます。
- **強制コアダンプ**——このオプションを使用すると、システムが応答しないときに、技術調査用にデバッグ情報が強制的に生成されます。コアダンプファイルとトラップ情報イメージは両方ともローカルドライブに保存されます。シンクライアントを再起動後、コアダンプファイルとトラップ発行スクリーンショットファイルは、ファイルサーバか USB ドライブの **/wnos/troubleshoot/**ディレクトリにアップロードされます。
- **シャドウ tmp のエクスポート**——デバッグ目的のテンポラリログをエクスポートするには、このオプションを使用します。ログファイルは、対象の機器構成に応じて、USB ドライブまたはファイルサーバにエクスポートできます。
- **スクリーンショットエクスポート**——ファイルサーバか USB ドライブにスクリーンショットをエクスポートするには、このオプションを使用します。トラブルシューティングの役に立つように、エクスポート済みのファイルの名前にビルド情報が追加されます。スクリーンショットがクリップボードに存在する場合は、目的の場所にエクスポートされます。スクリーンショットが使用できない場合は、画面全体が自動的にコピーされて目的の場所にエクスポートされます。
- **INI ファイルのエクスポート**——グローバル INI ファイル（wnos.ini または xen.ini）、wdm.ini、ccm.ini、mac.ini などのマシンに対応した INI ファイルを、ファイルサーバか USB ドライブにエクスポートするには、このオプションを使用します。username.ini ファイルのみではエクスポートできません。

3 **トレース**タブをクリックし、セッションのトレースと再生時に表示を遅延を設定します。操作のトレースで使用できるオプションは、なし、記録および再生です。

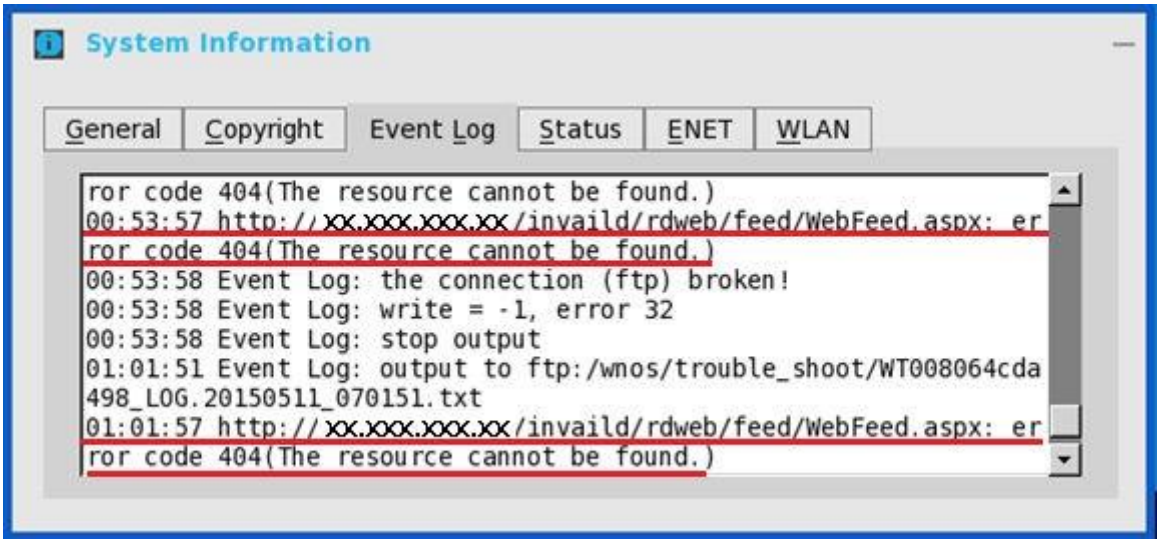


4 **キャプチャ**タブをクリックし、イベントログを記録、USB にキャプチャ[有線]、USB にキャプチャ[無線]を設定し、USB パケットを記録などを設定し、操作のトレースおよびシステム診断ログをキャプチャします。



エラーメッセージを有効にするには、次のガイドラインに従います。

- **一回限り**または**常に有効**オプションのいずれかをクリックすると、予期しないエラーメッセージをログに記録できます。
- ログをオフにしてから、ftp:/wnos/trouble_shoot フォルダにあるログファイルを確認します。



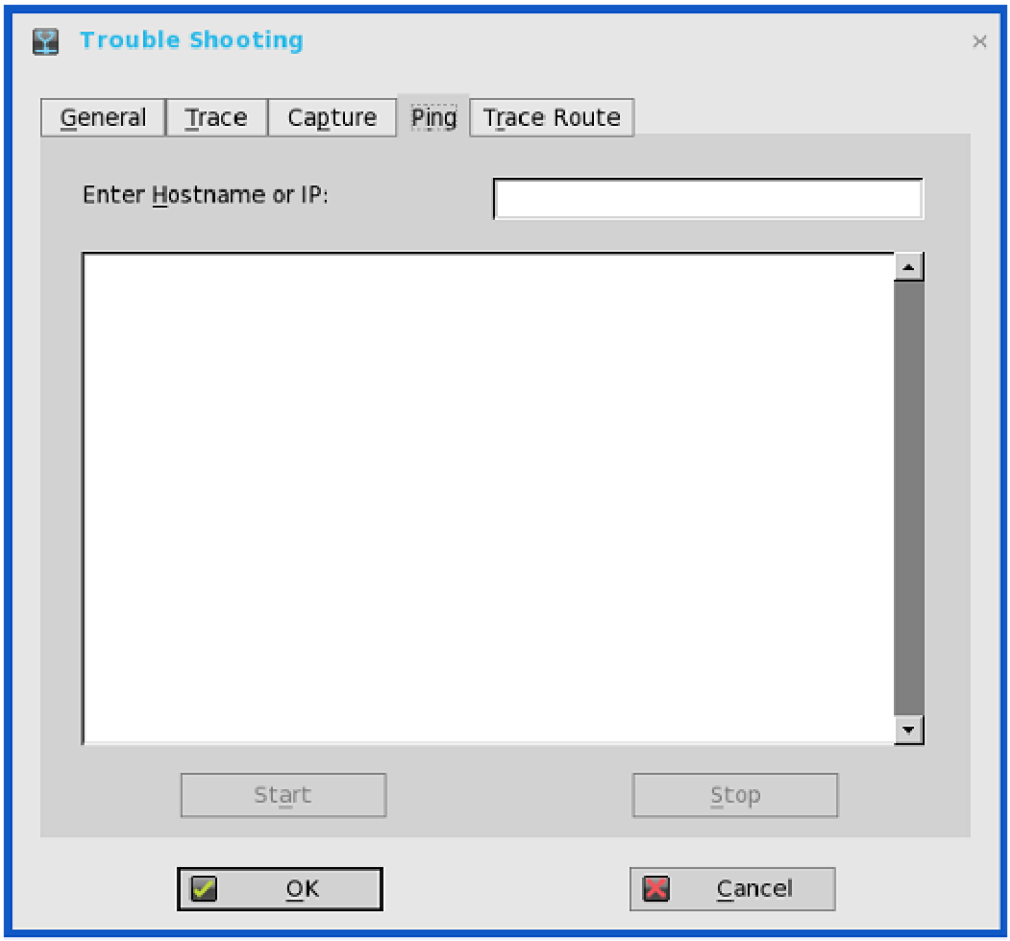
- wnos.ini ファイルの Privilege パラメータの Trace オプションを必ず有効にします。詳細については、『Dell Wyse ThinOS INI ガイド』を参照してください。
- **USB にキャプチャ[有線]**オプションを使用して、ネットワーク情報の取得を有効にします。つまり、シンクライアントに挿入されている USB ドライブに、シンクライアントが送受信するすべてのトラフィックのネットワーク追跡を取得できます。

XenDesktop サーバまたはネットワークにログインし、これらのサーバまたはネットワークを使用すると、**/wnos/troubleshoot/[Terminal Name]_[ENET or WS]. [Date_Time].pcap** ファイルが USB ドライブに保存されます。このファイルは、ネットワークのトラブルシューティングや分析に使用するパケットアナライザなどのソフトウェアによって分析できます。

たとえば、Ethernet の場合は、ファイル名は、yx008064b2bfd7_ENET.20150415_064455.pcap です。ワイヤレスの場合は、ファイル名は、yx008064b2bfd7_WS.20150415_064455.pcap です。

メモ：USB ドライブをシンクライアントに挿入してから、USB にキャプチャ[有線]オプションを選択してください。USB ドライブが挿入されていない状態でダイアログボックスを終了した場合、またはシンクライアントをリスタートした場合は、USB にキャプチャ[有線]オプションは、自動的にオフになります。必要に応じて、このオプションを再度選択する必要があります。

5 **Ping** タブをクリックし、次のガイドラインに従って、Ping 診断ユーティリティを実行し、応答メッセージを表示します。



- **ホスト名/IP アドレス**——Ping の宛先となる IP アドレス、DNS 登録ホスト名、または WINS 登録ホスト名を入力します。
- **データ領域**——Ping 応答メッセージを表示します。Ping コマンドでは、1 秒あたり 1 つの Echo 要求を送信して往復時間とパケット損失に関する統計を計算し、計算が完了すると簡単な要約を表示します。
- **開始**——Ping コマンドを実行します。ホストが稼働していてネットワーク上にある場合、そのホストは Echo 要求に応答します。デフォルトでは、Echo 要求は、**中止**をクリックして中断されるまで送信されます。
- **中止**——Ping 要求を終了し、**Ping** ダイアログボックスを開いたままにすると、データ領域で提示された要約を読むことができます。

メモ：

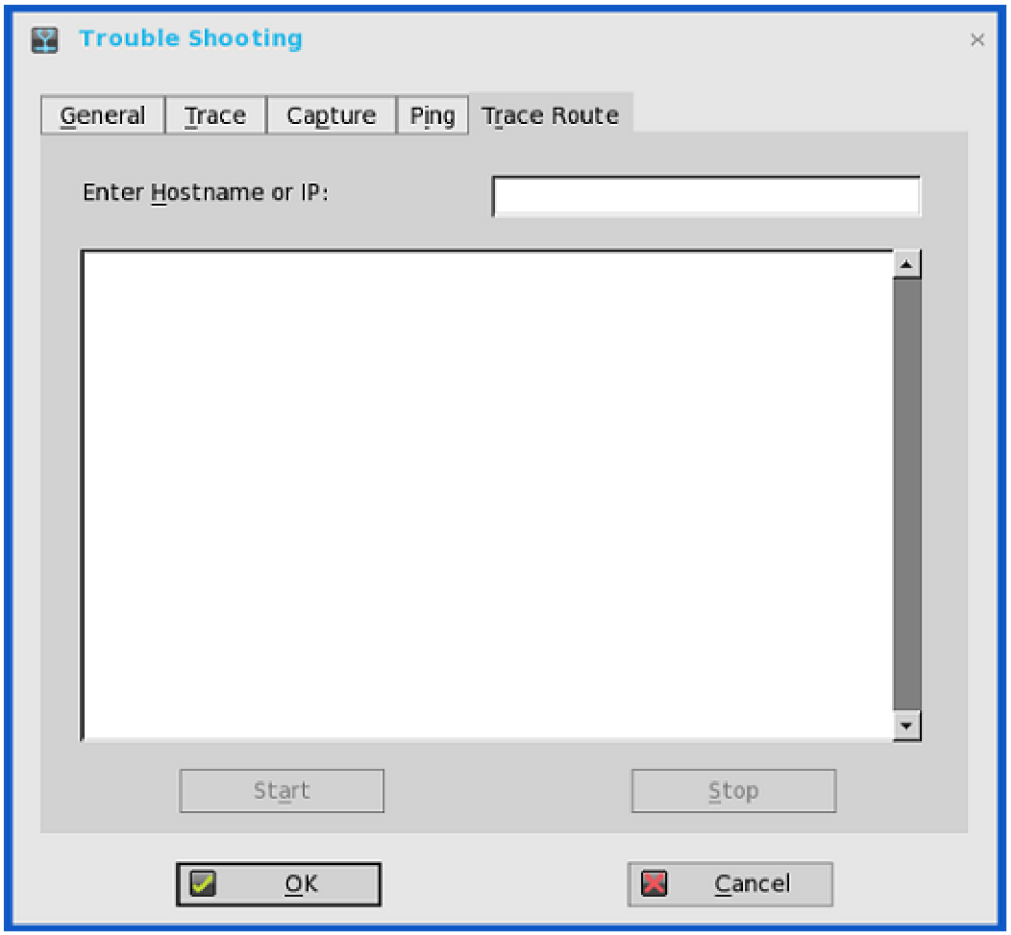
Ping では、Echo 要求をネットワークホストに送信します。ホストパラメータは有効なホスト名か IP アドレスのいずれかです。ホストが稼働していてネットワーク上にある場合、そのホストは Echo 要求に応答します。Ping では、1 秒あたり 1 つの Echo 要求を送信して往復時間とパケット損失に関する統計を計算します。計算が完了すると簡単な要約を表示します。

Ping ユーティリティは、次の目的に使用できます。

- ネットワークおよびさまざまな外部ホストのステータスを特定します。
- ハードウェアおよびソフトウェアの問題を追跡したり、切り分けたりします。
- ネットワークをテスト、測定、および管理します。
- ホスト名だけがわかっている場合に、ホストの IP アドレスを特定します。

重要: Ping はサービス拒否攻撃で一般的に使用されるメカニズムであるため、すべてのネットワーク機器が Ping のパケットに応答するとは限りません。応答がない状態でも、Ping の宛先がその他の用途に使用できないとは限りません。

6 **TraceRoute** タブをクリックし、tracert 診断ユーティリティを実行し、応答メッセージを表示します。次のガイドラインに従います。



- **ホスト名/IP アドレス**——追跡対象となる IP アドレス、DNS 登録ホスト名、または WINS 登録ホスト名を入力します。
- **データ領域**——往復の応答時間とパス内の各デバイスの識別情報を表示します。
- **開始**——tracert コマンドを実行します。
- **中止**——tracert コマンドを終了し、**Trace Route** ダイアログボックスを開いたままにすると、データ領域で提示された情報を読むことができます。

tracert ユーティリティでは、シンクライアントからネットワークホストへのパスを追跡します。ホストパラメータは有効なホスト名か IP アドレスのいずれかです。tracert ユーティリティでは、パス内の各デバイス（ルーターとコンピュータ）に情報のパケットを 3 回送出し、メッセージボックスに往復の応答時間と識別情報を表示します。

7 **OK** をクリックして設定を保存します。

TCX Suite

Dell Wyse TCX Suite は、クラウドクライアントコンピュータの利点を提供する、単体のソフトウェアソリューションです。Dell Wyse TCX Suite のサポート対象となる環境は、Microsoft Remote Desktop Services、Citrix XenApp、Citrix XenDesktop、Teradici、および VMware Horizon View です。Dell Wyse TCX で使用される Collaborative Processing Architecture（CPA）によって、作業負荷がサーバと Plug-n-Play USB デバイスに配分されます。TCX Suite は、確立されたソフトウェアプロトコルを使用して、クラウドクライアントコンピュータ環境に、画期的なマルチメディアおよびオーディオ技術を提供します。TCX 機能の詳細については、最新の『Dell Wyse TCX 管理者ガイド』を参照してください。

TCX Suite によって、鮮やかな Flash 動画の再生、マルチモニタ認識、鮮やかなマルチメディア再生、高品質の双方向オーディオ機能、クラウドクライアントのシームレスな USB デバイスアクセスなどが可能になります。

TCX Suite は次の機能を提供します。

- **TCX Flash Acceleration および TCX Flash Redirection**——リモートコンピュータ環境の Flash 動画コンテンツの性能を向上します。
- **TCX Multidisplay**——仮想デスクトップを使用することで、マルチモニタでクラウドクライアントの生産性を向上し、優位性を強化します。
- **TCX Multimedia**——MPEG、WAV、WMV、H.264 などのマルチメディアファイルフォーマットの再生の拡張をサポートします。このソフトウェアには、サーバとクライアントの両方のコンポーネントが含まれており、マルチメディア処理タスクをクライアントとサーバ間でリダイレクトすることで、豊かなユーザーエクスペリエンスが可能となります。
- **TCX Rich Sound**——仮想デスクトップとアプリケーションに双方向オーディオ機能を提供し、音声の録音と再生のアプリケーションをサポートします。妥協のない導入をサポートします。
- **TCX USB Virtualizer**——USB デバイスを仮想デスクトップとアプリケーションから確認できるシンクライアントやエンドポイントに接続します。これによって、プリンタ、スキャナー、ストレージデバイス、Palmtop、BlackBerry、Pocket PC ハンドヘルド端末、HID デバイス、Web カメラ、ヘッドセット、iPhone、クレジットカードマシン、スマートカードなど、さまざまな USB ベースのデバイスが、限られたローカルデバイスドライバに依存しなくてもよくなります。
- **TCX Monitor**——USB や Flash リダイレクトモジュールが正しく機能しているかどうか、システムの状態を効率的に特定できます。

TCX Flash Redirection

TCX Flash Redirection は、クライアントの CPU を使用し、Flash を復号して表示します。TCX Flash Redirection は、クライアントの NPAPI インターフェイスをサポートする Adobe Flash Player プラグインを使用します。TCX Flash Redirection は、RDP プロトコルと PCoIP プロトコルにまたがってサポートされます。TCX Flash Redirection は、サーバの CPU サイクルをあまり使用しません。

前提条件

- この機能を動作させるには、**TCX.i386.pkg** をクライアントにインストールする必要があります。
- **TFRSServerBHO** クラスは、ブラウザのアドオンで有効にする必要があります。
- **Enable Protected Mode** は、Internet Explorer のセキュリティオプションでオフにします。
- **Enable third-party browser extensions** は、Internet Explorer の詳細オプションで有効にします。

TCX Flash Redirection の動作ステータスを確認

TCX Flash Redirection のステータスの確認は、HDX FR と同様です。

HW ラベルを表示するには、次の INI パラメータを使用します。

MMRConfig=VIDEO flashingHW=1

TCX Flash Redirection の既知の問題

ThinOS の TCX FR は、一定の Flash 動画ページでは動作しません。ただし、RDP を使用した FR や PCoIP を使用した FR で同じ結果となります。デルは、TCX FR を全システムに導入する前に、動作しない URL を確認して、それをブロックすることをお勧めします。

Trusted Platform Module バージョン 2.0

Wyse 5070 シンクライアントは、Trusted Platform Module（TPM）バージョン 2.0 を使って、ディスクの暗号化と復号をサポートします。

- Measured Boot——SHA1（Secure Hash Algorithm 1）が、ThinOS イメージのハッシュ値を生成するために使用され、TPM 内の Platform Configuration Registers（PCR）（**TPM_PCR16**）の完全性測定を拡張します。 これはディスクの暗号化／復号キーを生成するのに使用されます。
- ディスクの暗号化／復号キー
  - ユーザーデータの入った Disk C とシステムライブラリの入った Disk B が暗号化されます。
  - 事前に保存された **KeyStub** と **TPM_PCR16** が、TPM によるディスクの暗号化および復号キーを生成するのに使用されます。実際の実行は、TPM 開封の操作をベースにしたものです。
  - キーが修正されると、このキーによる特定のディスクパーティションの確認はできません。ディスクパーティションを有効にするために、フォーマットされます。以下のスクリーンショットは、イベントログを示しています。

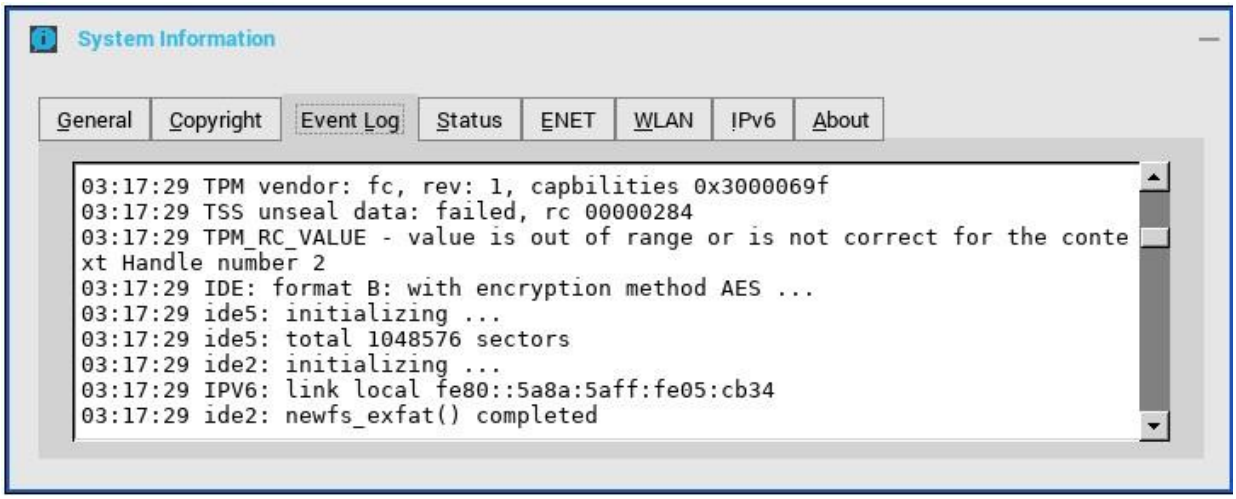


図 18.イベントログタブ

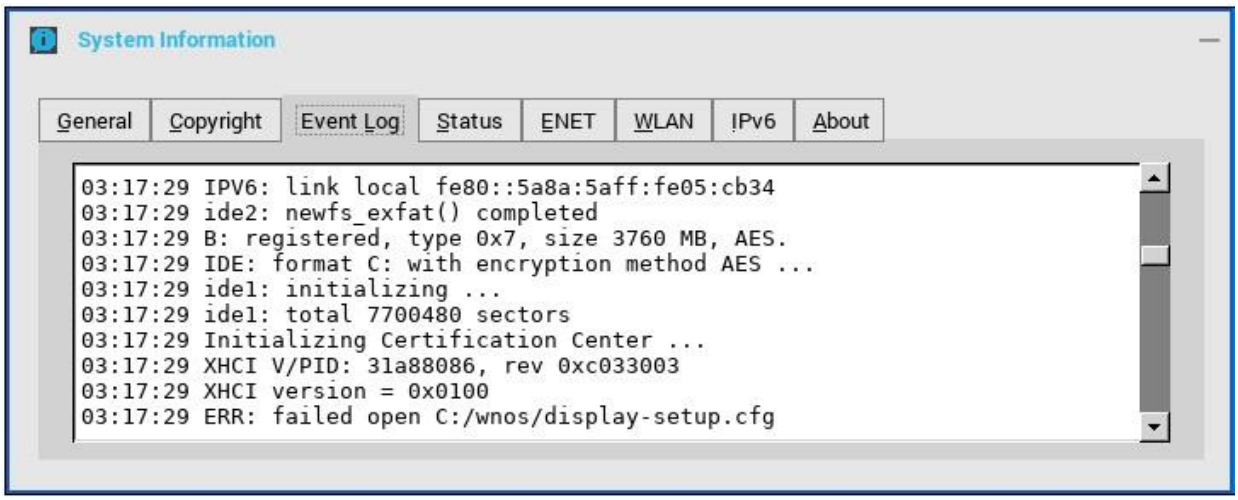


図 19.イベントログタブ

– ディスクパーティションがフォーマットされると、ディスプレイ設定、ユーザー証明書、ワイヤレス設定（第 1 SSID は NVRAM に保管されているので除く）、クッキー、ミラーファイルサーバデータなど、一部のユーザー設定は失われます。

ThinOS の BIOS 管理

この付録では、デル標準 BIOS を搭載した ThinOS の BIOS 管理について説明します。

Wyse と Dell BIOS の BIOS 管理に一貫性をもたせるために、デル標準 BIOS の INI パラメータ **Device=DellCmos** が導入されます。

BIOS 設定にパスワードが設定されている場合は、設定を変更するには、パスワードの入力が必要になります。たとえば、設定を更新する INI パラメータの後に、「CurrentPassword={}」を付ける必要があります。これは Dell BIOS には必須です。

BIOS 機能マトリックス

表 37. BIOS 機能マトリックス

主要要件	BIOS 管理の INI パラメータ	Wyse 5070 シンクライアント
警告音なしの電源投入	該当なし	はい
ファイルサーバからの BIOS 更新	該当なし	はい
INI で BIOS パスワードを変更	Device=DellCmos CurrentPassword={} NewPassword={} Device=Cmos CurrentPassword={} NewPassword={}	はい
INI で起動順序を変更	Device=cmos BootOrder={PXE, HardDisk, USB}	該当なし
INI で PXE イメージを有効化／無効化	Device=DellCmos PXEBootSupport={yes, no}	はい
INI で USB イメージを有効化／無効化	Device=cmos BootFromUSB={yes, no} Device=DellCmos USBBootSupport={yes, no}	はい
INI で AC 電源復旧を管理	Device=cmos AutoPower={yes, no} Device=DellCmos ACRecovery={PowerOff, PowerOn, LastState}	はい
INI で自動電源オンを管理	Device=DellCmos AutoPower={Disable, Daily, Workday} AutoPowerTime=hh:mm Device=Cmos AutoPowerDate=yes AutoPowerTime=2:30:30 AutoPowerDays=Sunday;Friday	はい
CMOS の抽出および復元	Device=cmos Action={extract, restore} CurrentPassword={} Device=DellCmos Action={extract, restore} CurrentPassword={}	はい
INI でオーディオ管理	Device=cmos OnboardAudio={yes, no} Device=DellCmos Audio={yes, no}	はい

主要要件	BIOS 管理の INI パラメータ	Wyse 5070 シンクライアント
INI で USB ポート管理	Device=cmos USBController={yes, no} Device=DellCmos USBRearPort={yes, no} USBFrontPort={yes, no} (Rear/Front for Dell BIOS only)	はい
INI で Admin ロックアップ管理	Device=DellCmos AdminLock= {yes, no}	はい
Wake on USB のサポート	Device=DellCmos WakeOnUSB={yes, no}	はい
Wake On LAN	Device=cmos WakeOnLan= {yes, no} Device=DellCmos WakeOnLan= {Disable, LAN, PXE}	はい

BIOS 設定のアクセス

シンクライアントを起動すると、短時間、Dell のロゴが表示されます。ロゴが表示されている間に、F2 キーを押し続けます。

プロンプトが表示されたら、パスワード **Fireport** を入力し、BIOS 設定画面を表示します。たとえば、F7 キーを使用すると、最適化されたデフォルトを使用できます（BIOS セットアップユーティリティのすべての項目に対する最適なデフォルト値がロードされます）。

デル標準 BIOS の管理

このセクションでは、ThinOS クライアントをデル標準 BIOS で設定、管理する方法について説明します。

次の Dell BIOS 設定がファイルサーバ（INI パラメータ）を使用することでサポートされています。

表 38. BIOS 設定オプション

パラメータ	設定
システム設定	オーディオ
セキュリティ	• Admin 設定ロックアウト • Admin パスワード – Admin パスワード有効化／無効化 – Admin パスワード更新
USB 設定	• 前面の USB ポートの有効化 • 背面左のデュアル USB 2.0 ポートの有効化
電源管理	• Wake-On-LAN – 無効 – LAN Only – LAN with PXE Boot • AC 電源復旧 – 電源オフ – 電源オン – 電源切断時の状態 • 自動電源オン – 無効

パラメータ	設定
	– 毎日 – 平日 – 日を選択 • Wake-On-USB
デバイスブート	• USB ブート • PXE ブート

INI パラメータとその使用法の詳細については、最新の『Dell Wyse ThinOS INI Reference Guide』を参照してください。

次が INI パラメータの例です。

- **Device=DellCmos newpassword=1234567** または **newpasswordenc=encrypted strings**——パスワードが設定されていないときに admin パスワードを作成するには、この INI パラメータを使用します。
- **Device=DellCmos currentpassword=1234567 newpassword=""**または **currentpasswordenc=encrypted strings**——既存のパスワードをクリアするときは、この INI パラメータを使用します。

Wyse 5070 シンクライアントの BIOS のアップグレード

このセクションでは、ThinOS を搭載した Wyse 5070 シンクライアント、および PCoIP を搭載した Wyse 5070 シンクライアントの BIOS を、ファイルサーバを使用して更新する手順について説明します。デル標準 BIOS ファイルが、署名とセキュリティのために、BIN ファイルフォーマットに変換されます。BIN ファイルのフォーマットは **Wyse_5070_version.bin** です。

ファイルサーバを使用した BIOS のアップグレード :

1 デルサポートサイトから Dell BIOS ファイルをダウンロードします。
ここでは例として **Wyse_5070_1.0.3.bin** を使用します。 BIOS のバージョンは、リリースごとに更新されている可能性があります。最新の BIOS のバージョンについては、最新の『Dell Wyse ThinOS リリースノート』を参照してください。
2 Dell BIOS ファイルを **X10_bios.bin** にリネームします。
3 リネームした BIOS ファイルを、ファイルサーバの **WNOS** フォルダに、ftp または https でアップロードします。
4 **WNOS.INI** の INI パラメータ **autoload** は、ファームウェアを更新する場合は必ず有効にします。
5 シンクライアントを再起動します。
BIOS は自動的に更新されます。

新しい BIOS が正しく更新されているかどうか確認するには、デスクトップメニューから、**システム情報**オプションをクリックするか、ゼロモードで**システム情報**アイコンをクリックします。**イベントログ**タブに、BIOS バージョンログが表示されます。
たとえば、**System Version: 8.5_108—ROM 1.0.3.**

このログによって、BIOS のバージョンが v1.0.3 に更新されたことが分かります。

BIOS のバージョンは、**BIOS Setup** 画面に表示できます。**BIOS Setup** にアクセスするには、以下の操作を行います。

1 シンクライアントを再起動し、システム起動中に F2 キーを押します。
2 admin パスワードが設定されている場合は、BIOS パスワードを入力します。
3 **Settings > General > System Information** の順にクリックします。
BIOS のバージョンが画面に表示されます。

BIOS は、Wyse Management Suite バージョン 1.2 コンソールを使用して更新することもできます。Wyse Management Suite の詳細については、『Dell Wyse Management Suite 管理者ガイド』を参照してください。

セキュリティ

新しいグローバルセキュリティポリシーが、ThinOS 用に定義されました。このポリシーは、若干の例外はあるものの、すべてのセキュアな接続（https/SSL connections）に適用されます。
目的——セキュリティレベルをデフォルトで強化し、グローバル設定を追加することです。このセキュリティポリシーによって、各アプリケーションのセキュリティ設定が統一されます。

表 39. INI パラメータ

INI パラメータ	説明
SecurityPolicy={full | **warning** (default) | low} SecuredNetworkProtocol={yes | no (default)} TLSMinVersion={1 (default), 2, 3} TLSMaxVesion={1, 2, 3 (default)}	**Full**——SSL 接続はサーバ証明書の確認を必要とします。サーバ証明書の信頼がない場合は、接続を取り消します。 **Warning（デフォルト）**——SSL 接続はサーバ証明書の確認を必要とします。サーバ証明書の信頼がない場合は、ユーザーは継続できるか、接続を取り消します。 **Low:** サーバ証明書は確認されません。これは少数のアプリケーションのために設定された値です。 ファームウェアが更新されるとすぐに、使用可能なアプリケーションすべてに対して、デフォルト値が Warning に設定されます。 ファイルサーバと WDM には 1 つの例外があります。 Privilege セグメントの古い INI の「SecurityLevel | SecureProtocol」は削除されます。

デフォルトの SSL セキュリティモードで実行しているアプリケーションは、すべてグローバルモードに従います。グローバルモードでは、デフォルト値は Warning です。影響を受けるアプリケーションには、VMware View、Amazon Workspaces（AWS）、File Server、WDMService、Caradigm Server、OneSign Server などがあります。

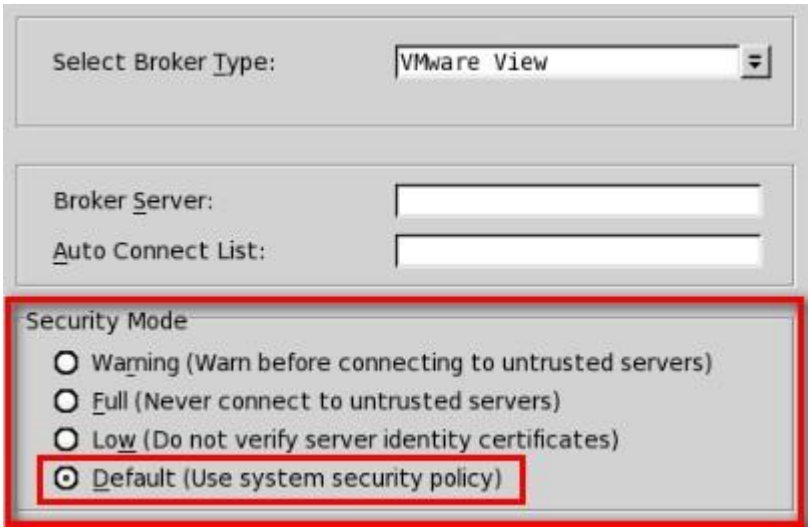
セキュリティモードの INI パラメータの詳細については、『Dell Wyse ThinOS INI ガイド』を参照してください。

次は例外です。

- 工場出荷時の設定にリセットされた状態の File Server と WDM：INI パラメータがロードされる前は、SSL セキュリティモードが Low に設定され、INI パラメータがロードされた後は、SSL セキュリティモードがグローバルモードに従って変更されます。たとえば、その値が INI パラメータで変更されていない場合は、デフォルト値は Warning に設定されます。

  ユニットがアップグレードされると、前の設定値（デフォルト値は Low に設定）を持つシステムはグローバルモードに従います。たとえば、その値が INI パラメータで変更されていない場合は、デフォルト値は Warning に設定されます。
- VMware View および AWS ブローカーには独自のセキュリティ設定があります（GUI および INI）。

  追加のオプションは、グローバルモードに従って、新しいデフォルト値として追加されます。



- Wyse Management Suite、Microsoft RDS ブローカー、Citrix ブローカー、および SecureMatrix は常に Full です。

File Server のデフォルトプロトコルは、WDM/DHCP/INI で設定されなければ FTP のままで、常にプロトコルプレフィックス付きのフルアドレスを表示します。ここでは例として ftp://を使用します。

新しいファームウェア／クライアントのデプロイ情報

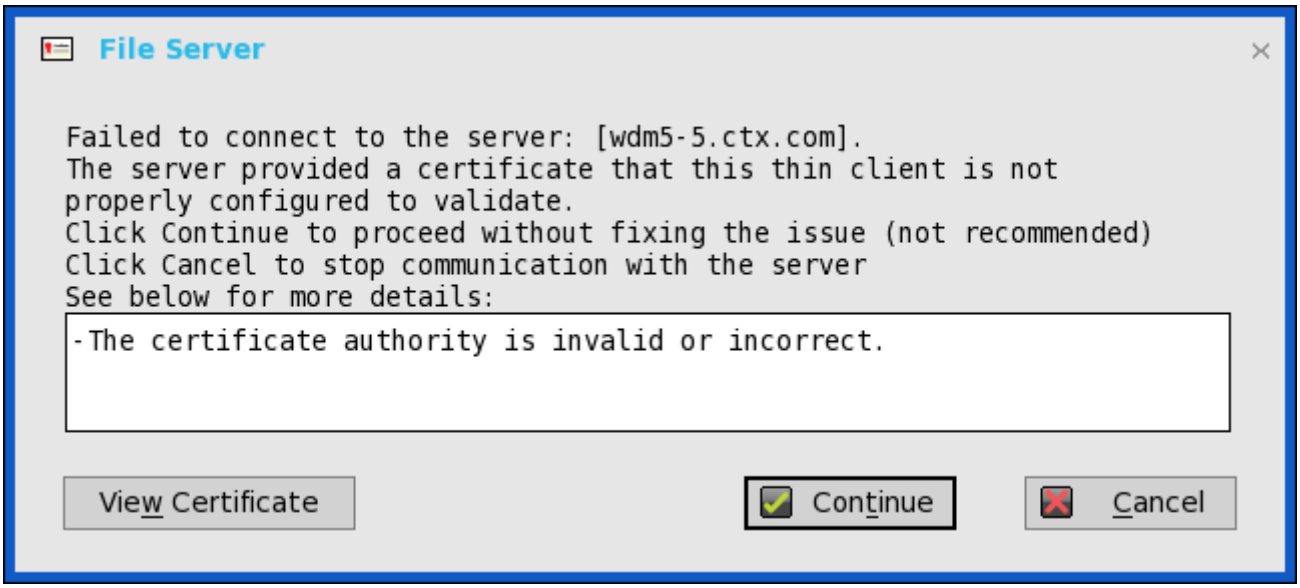
- SecurityPolicy=Full または Warning の場合、ファームウェアを更新する前に、それぞれの File、View、AWS、WDM、Wyse Management Suite、OneSign、および／または Caradigm サーバから、ThinOS クライアントに証明書を追加する必要があります。
- プロトコルが設定されなければ、File Server のデフォルトプロトコルは引き続き FTP で、ftp prefix が自動的に追加されます。

エラーと警告には分かりやすく修正されたメッセージを表示

UI の変更はなく、セキュリティエラー／警告のメッセージのみが修正されています。

フルセキュリティモードでは、次の警告メッセージが表示されます。

警告セキュリティモードでは、次の警告メッセージが表示されます。



WDM サーバが https と設定されている場合は、サーバアドレスは http に変換されません。

- 以前のシナリオでは、WDM サーバが HTTPS なしで設定され、ローカル WDM サーバアドレスが HTTPS で指定されている場合、システムはサーバアドレスを HTTP アドレスに変換します。
- 現在のシナリオでは、システムは WDM サーバアドレスを HTTP に変換しません。

トランスポート層セキュリティ

トランスポート層セキュリティ（TLS）は、クライアントアプリケーションとサーバアプリケーション間の通信におけるセキュリティを確保するプロトコルです。

トランスポート層セキュリティ（TLS）のアップグレード——ThinOS 8.2 リリースでは、TLS がバージョン 1.0 からバージョン 1.2 にアップグレードされました。デフォルトでは、ThinOS クライアントは通常 TLS 1.2 を使用して SSL/TLS 上の通信プロトコル、接続またはアプリケーションを保護し、サーバとネゴシエートするときは以前の SSL/TLS バージョンに切り替えます。

スマートカードとスマートカードリーダー

スマートカードは、集積回路を組み込んだセキュリティトークンです。スマートカードによって、データを保存し、それを処理できます。スマートカードリーダーは、スマートカードからデータを読み取る入力デバイスです。

- **Gemalto のスマートカード IDPrime MD840**—Gemalto のスマートカード IDPrime MD830 および MD840 がサポートされています。Windows のミドルウェア向けの IDGo 800 バージョン 1.2.1 - 01 には、Gemalto のスマートカード IDPrime MD840 のサポートが必須です。
  最新の MD830 Rev B カードの利用を可能にするために、Secure Messaging 機能がサポートされています。

Prime MD 840 スマートカードの既知の問題：最初のコンテナが使用されると、Xen ブローカーのログオンはエラーになります。

- **OMNIKEY スマートカードリーダー**——次の OMNIKEY スマートカードリーダーはサポートされています。
  - Omnikey 5427 CK（0x5427、0x076b）リーダーは、iclass15693、14443a、125k カードをサポート
  - Omnikey 5326 DFR（0x5326、0x076b）リーダーは、iclass15693 カードをサポート
  - Omnikey 5025 CL（0x502a、0x076b）リーダーは、125k カードをサポート
  - Ominkey 5325 CL, 5125（0x5125、0x076b）リーダーは、125k カードをサポート
  - Omnikey 5321 V2 CLi（0x532a、0x076b）リーダーは、13.56 MHz カードをサポート
  - Omnikey 5021 CL（0x5340、0x076b）リーダーは、13.56MHZ カードをサポート
  - Omnikey 5321 V2 Cl Sam（0x5341、0x076b）リーダーは、13.56 MHz カードをサポート
  - Omnikey 5421（0x5421、0x076b）リーダーは、13.56 MHz カードをサポート
  - Omnikey 5321 CR（0x5320、0x076b）
- **内蔵スマートカードリーダー**——内蔵スマートカードリーダーは、通常のスマートカードを処理します。機能は、他の外部 USB スマートカードリーダーや Dell KB-813 などの内蔵スマートカードリーダーと同様です。

試験済みのスマートカードとスマートカードリーダーの完全なリストについて詳しくは、最新の『Dell Wyse ThinOS リリースノート』を参照してください。

一元設定を使用したアップデートと設定の自動化

この付録では、3 つの簡単なステップで、ThinOS を実行するシンクライアントに自動的なアップデートと設定を提供する環境の設定方法を説明します。

メモ： Dell Wyse シンクライアントには、デバイス管理ソフトウェアは必要ありません。Dell Wyse シンクライアントは、DHCP サーバから IP アドレス、およびファームウェアと設定手順がある場所を取得するよう設定されています。ただし、Wyse Device Manager（WDM）または Wyse Management Suite(WMS)を使用すると、シンクライアントをより詳細に管理できます。シンクライアントと WDM サーバまたは Wyse Management Suite との通信の設定方法については、『Dell Wyse ThinOS INI ガイド』の関連する INI パラメータを参照してください。

自動アップデートおよび自動設定の設定方法

ThinOS を実行しているシンクライアントが正常に INI ファイルにアクセスし、サーバからシンクライアント自身をアップデートするには、INI ファイルとその他のアップデートファイルを含んだ正しいフォルダ構造のサーバを設定し、そのサーバをシンクライアントの参照先にして、シンクライアントを再起動または起動する必要があります。

DHCP とサーバが設定されて使用可能になると、シンクライアントは（毎回起動時に）事前定義されたサーバにアップデートがあるかどうかを確認します。DHCP オプション**#161** ではサーバ URL を、DHCP オプション**#162** ではサーバへのルートパスを指定できます。アップデートがある場合は、自動的にインストールされます。

DHCP オプションの使用

この表では、使用可能な DHCP オプションについて説明します。

表 40. DHCP オプション

オプション	説明	メモ
1	サブネットマスク	必須。ただし、シンクライアントが別のサブネット上のサーバとやり取りする必要がない場合は不要です。MS DHCP はサブネットマスクを必要とし、常にサブネットマスクを送信します。
2	時間オフセット	オプション
3	ルーター	オプションですが、推奨されます。シンクライアントが別のサブネット上のサーバとやり取りする必要がない場合は不要です。
6	ドメインネームサーバ（DNS）	オプションですが、推奨されます。
15	ドメイン名	オプションですが、推奨されます。オプション 6 を参照してください。
28	ブロードキャストアドレス	オプション
44	WINS サーバ IP アドレス	オプション
51	リース時間	オプションですが、推奨されます。
52	オプションのオーバーロード	オプション
53	DHCP メッセージタイプ	推奨。

オプション	説明	メモ
54	DHCP サーバ IP アドレス	推奨。
55	パラメータ要求リスト	シンクライアントによって送信されます。
57	最大 DHCP メッセージサイズ	オプション（常にシンクライアントによって送信されます）。
58	T1（更新）時間	オプションですが、推奨されます。
59	T2（再バインド）時間	オプションですが、推奨されます。
61	クライアント識別子	常に送信されます。
161	ファイルサーバ（ftp/http/https）	オプションの文字列。ファイルサーバの名前または IP アドレスのいずれかです。名前を指定すると、オプション 6 で指定した DNS サーバによって名前が解決されます。サーバが指定するオプションが空白であるか、サーバがフィールドに値を指定しない場合は、DHCP サーバが存在するマシンも、ファイルサーバであると仮定されます。
162	ファイルサーバ（ftp/http/https）へのルートパス	オプションの文字列。サーバが指定するオプションが空白で、サーバがフィールドに値を指定しない場合は、Null 文字列が使用されます。 ¥wyse¥wnos が検索パスに自動的に追加されます。たとえば、pub\serversoftware と入力すると、検索可能なパスは pub\serversoftware\wyse\wnos です。 **メモ：入力するパスにドル記号（$）を追加すると、検索パスに自動で含まれる ¥wyse を省略できます。たとえば、pub\serversoftware$と入力すると、検索対象のパスは pub\serversoftware\wnos となります。** **メモ：パスでの先行するスラッシュ（¥）の使用や省略は、一部のサーバでは極めて重要です。サーバによっては、ログイン時に指定するユーザーのルートパスへのアクセスを制限しています。このようなサーバに対しては、先行するスラッシュの使用はオプションとなっています。一部の*NIX サーバでは、ファイルユーザーがファイルシステム全体にアクセス可能になるよう設定できます。このようなサーバに対しては、先行するスラッシュを指定すると、ルートのファイルシステムからアクセスが開始されます。適切な動作を保証するには、使用するファイルサーバへのファイルの指定が正しく一致することが極めて重要です。保護されている Windows サーバでは、適切なアクセスを完了するために、スラッシュを指定する必要があります。**
165	WMS サーバ	オプションの文字列。Wyse Management Suite サーバの IP アドレスを指定します。

オプション	説明	メモ
166	WMS MQTT サーバ	オプションの文字列。MQTT サーバの IP アドレスを指定します。
167	WMS CA Validation	オプションの文字列。
181	PNAgent/PNLite サーバのリスト	オプションの文字列。シンクライアントは、サーバを使用してユーザーの Windows 資格情報を認証し、検証された資格情報に対して有効な ICA 公開アプリケーションのリストを取得します。ユーザーはシンクライアントにログインするときに、これらの資格情報を指定します。
182	PNAgent/PNLite の NT ドメインリスト	オプションの文字列。シンクライアントは、オプション 182 で提供された情報からドメインのプルダウンリストを作成します。このリストは、DHCP オプションに指定した順序で、シンクライアントログインで表示されます（たとえば、指定された最初のドメインはデフォルトになります）。選択したドメインは、ユーザーIDとパスワードを認証する必要があります。選択したドメインだけが、認証プロセスで使用されます。ドメインリストが不完全で、リスト外のドメインに対して資格情報を確認する必要がある場合（オプション 181 のサーバがリスト外のドメインに対して認証可能であることを前提とします）、ユーザーはオプション 182 で指定したドメインを使用せず、ログイン時に別のドメイン名を入力することができます。
184	ファイルサーバのユーザー名	オプションの文字列。オプション 161 で指定したサーバに対して認証する際に使用するユーザー名。
185	ファイルサーバのパスワード	オプションの文字列。オプション 161 で指定したサーバに対して認証する際に使用するパスワード。
186	WDM サーバリスト	オプションの WDM のバイナリ IP アドレス。このオプションでは、最大 2 つの WDM サーバを指定できます。2 つ指定されている場合、起動時にシンクライアントは最初のサーバにチェックインを試みます。最初のサーバに接続できない場合は、2 番目のサーバにチェックインを試みます。
187	WDM サーバポート	オプションの番号。バイト、ワードまたは 2 バイト配列。 **メモ：ベンダークラス固有情報オプションに埋め込まれていない場合、このオプションタグの値を 2 バイトとして送信すると、逆の順序で解釈されます。たとえば、値 0x0050 は 0x5000 と解釈されます。このオプションタグは、以前の ThinOS リリースで使用されていました。新しい ThinOS リリースでも、このオプションタグを受け入れて下位互換性を確保しています。**
188	仮想デスクトップブローカーサーバ	オプションの文字列。

オプション	説明	メモ
190	WDM セキュアポート	オプションの番号、ワードまたは 2 バイト配列。WDM との通信に、HTTP ではなく HTTPS を使用するために指定します。
192	WDM サーバポート	オプションの番号、ワードまたは 2 バイト配列。 **メモ：このオプションの値は、オプションタグ 187 と同じ情報を表します。違いは、ThinOS ではこのオプションタグの値が正しい順序で解釈されることにあります（たとえば、値 0x0050 は 0x0050 と解釈されます）。DHCP サーバがオプションタグ 192 と 187 の両方を提供する場合は、オプションタグ 192 が優先されます。**
194	WDM FQDN	オプションの WDM の完全修飾ドメイン名。
199	Wyse Management Suite のグループキー	オプションの文字列。Wyse Management Suite エージェントの Wyse Management Suite グループ登録キーを入力できます。Wyse Management Suite が無効で、Wyse Management Suite のグループキーが Null である場合、このオプションが有効になります。Wyse Management Suite は、グループ登録キーに任意の文字列を使用します。Wyse Management Suite サーバまたは MQTT サーバが Null である場合、Wyse Management Suite エージェントは値をデフォルトのサーバの値に設定します。

一般的な印刷設定の例

この付録では、印刷を行う一般的な状況での**プリンタ設定**ダイアログボックスと ThinOS INI パラメータの使用例を説明します。「プリンタセットアップの設定」での説明に加えて、これらの一般的なガイドラインにも従ってください。

重要: ホストベースのプリンタはサポートされていません。

以下の内容が含まれます。

- ローカルの USB プリンタまたはパラレルプリンタへの印刷
  - ローカルの USB プリンタまたはパラレルプリンタのためのプリンタ設定ダイアログボックスの使用
  - ローカルの USB プリンタまたはパラレルプリンタのための INI パラメータの使用
- Windows 以外のネットワークプリンタ（LPD）への印刷
  - Windows 以外のネットワークプリンタ（LPD）のためのプリンタ設定ダイアログボックスの使用
  - Windows 以外のネットワークプリンタ（LPD）のための INI パラメータの使用
- Windows ネットワークプリンタ（SMB）への印刷
  - Windows ネットワークプリンタのためのプリンタ設定ダイアログボックスの使用
  - Windows ネットワークプリンタ（LPD）のための INI パラメータの使用
- プリントサーバ（LPD）としてのシンクライアントの使用
  - LPD サービスの設定のためのプリンタ設定ダイアログボックスの使用
  - LPD サービスの設定のための INI パラメータの使用
- ThinPrint の設定

ローカルの USB プリンタまたはパラレルプリンタへの印刷

USB ポートまたはパラレルポートを介して、ローカルで接続されているプリンタに印刷できます。

重要: Microsoft リモートデスクトップセッションホスト（RDSH）、Microsoft ターミナルサービスおよび Citrix XenApp には、それぞれ独自の印刷ポリシーがあり、クライアント側での印刷を許可するにはこれらの印刷ポリシーを適切に設定する必要があります。これらの環境での印刷設定の詳細については、各ベンダーの手順を参照してください。

ローカルの USB プリンタまたはパラレルプリンタのためのプリンタ設定ダイアログボックスの使用

この例では、HP LaserJet 4000 がシンクライアントの USB ポートに接続されています。プリンタによっては、USB プリンタを接続するときに、プリンタ名フィールドとプリンタ ID フィールドに入力されています。
USB ポートまたはパラレルポートを介して、ローカルで接続されているプリンタに印刷するようプリンタを設定するには、次の手順を行います。

1 デスクトップメニューで、**システム設定** > **プリンタ**をクリックします。
プリンタ設定ダイアログボックスが表示されます。
2 **プリンタ設定**をクリックし、次のように、ローカルの USB プリンタに印刷する場合のポートタブに関するガイドラインに従います。

a **ポートの選択**——LPT1 または LPT2 ポートを選択します。
b **プリンタ名**——プリンタのリストに表示する名前を入力します。USB に直接接続されたプリンタでは、ほとんどの場合、自動的にプリンタ名が報告または入力されます。
c **プリンタ ID**——大文字やスペースも含めて、Windows プリンタドライバの名前とまったく同じになるように、プリンタのタイプまたはモデルを入力します。USB に直接接続されたプリンタでは、ほとんどの場合、自動的にプリンタ識別情報が報告または入力されます。この例では、HP LaserJet 4000 Series PCL と入力します。
d **プリンタクラス**——デフォルトのままでかまいません。
e **プリンタデバイスを有効にする**——直接接続されたプリンタを有効にするために選択する必要があります。プリンタデバイスを有効にして、リモートホストに表示します。

3 **OK** をクリックして設定を保存します。

ローカルの USB プリンタまたはパラレルプリンタのための INI パラメータの使用

ThinOS INI パラメータを使用してローカル印刷を設定すると、わかりやすい簡単な方法で環境内のすべてのクライアント用にプリンタを設定できます（すべてのプリンタが同じであることが前提です）。

次に示すのは、INI パラメータの例です。

```
Printer = LPT1 \
Name="HP LaserJet 4000" \
PrinterID="HP LaserJet 4000 Series PCL" \
Enabled = yes
```

メモ：PrinterID は Windows プリンタドライバとまったく同じテキストになります。よって、Windows でプリンタドライバの名前が HP LaserJet 4000 Series PCL という場合は、INI パラメータの PrinterID フィールドでも大文字やスペースを含めてまったく同じ名前にする必要があります。

Windows 以外のネットワークプリンタへの印刷

プリンタで LPR 印刷要求が受け付けられる場合、ThinOS は Windows 以外のネットワークプリンタに印刷できます。ほとんどのワークグループのプリンタや大規模ネットワークのプリンタには、この機能が備わっています。

LPR（Line Printer Request）印刷要求がプリンタで受け付けられるかどうかをベンダーに確認してください。LPR 対応プリンタに印刷するようシンクライアントを設定すると、クライアントは RDP または ICA 接続を介してこのプリンタをバックエンドのインフラストラクチャにリダイレクトします。このようにして、クライアントはバックエンドのインフラストラクチャに接続し、このネットワークプリンタがクライアントのローカルプリンタとして表示されます。

Windows 以外のネットワークプリンタのためのプリンタ設定ダイアログボックスの使用

Windows 以外のネットワークプリンタ（LPD）のために**プリンタ設定**ダイアログボックスを設定するには、次の操作を行います。

1 デスクトップメニューで**システム設定**をクリックし、**プリンタ**をクリックします。
プリンタ設定ダイアログボックスが表示されます。

この例では、HP LaserJet 4200n が LPR を介してシンクライアントに接続されています。

2 Windows 以外のネットワークプリンタに印刷する場合は、**LPD** タブをクリックし、次のガイドラインに従います。
a **LPD ポートの選択**——LPT1 または LPT2 ポートを選択します。
b **プリンタ名**——プリンタのリストに表示する名前を入力します。
c **プリンタ ID**——大文字やスペースも含めて、Windows プリンタドライバの名前とまったく同じになるように、プリンタのタイプまたはモデルを入力します。
この例では、HP LaserJet 4200n PCL6 と入力します。
d **LPD ホスト**——ネットワークプリンタ用のサーバの DNS 名または WINS 名です。前に示した例のように、ネットワーク上のプリンタの IP アドレスも入力できます。

メモ：ネットワーク上でプリンタが別のシンクライアントに接続されている場合、LPD ホストボックスには、そのシンクライアントの名前またはアドレスを入力します。

e **LPD キュー名**——LPD ホストには、サポート対象のプリンタごとに名前付きのキューが保持されます。使用するプリンタと

関連付けられたキューの名前を入力します。この名前は、ベンダーごとに変えることができます。このフィールドは必須で、ネットワークプリンタが、送信されるプリンタジョブを正しく受け付けるために、正確に指定する必要があります。例では、HP LaserJet 4200n PCL6 に対して、HP の Web サイトにあるドキュメントに従って、auto を使用できます。

メモ：ネットワーク上でプリンタが別のシンクライアントに接続されている場合、LPD キュー名は、プリンタが接続されているシンクライアントのプリンタ名ボックスの内容と一致する必要があります。

f **プリンタクラス**——デフォルトのままでかまいません。

g **プリンタデバイスを有効にする**——プリンタを有効にするために選択する必要があります。プリンタデバイスを有効にして、リモートホストに表示します。

Windows 以外のネットワークプリンタ（LPD）のための INI パラメータの使用

ThinOS INI パラメータを使用してネットワーク印刷を設定すると、わかりやすい簡単な方法で環境内のすべてのクライアント用にプリンタを設定できます（すべてのプリンタが同じであることが前提です）。

次に示すのは、INI パラメータの例です。

```
Printer = LPD1 \
LocalName="HP LaserJet 4200n" \
Host=10.10.10.1 \
Queue=auto \
PrinterID="HP LaserJet 4200 PCL6" \
Enabled = yes
```

メモ：PrinterID は Windows プリンタドライバとまったく同じテキストになります。よって、Windows でプリンタドライバの名前が HP LaserJet 4200n PCL6 という場合は、INI パラメータの PrinterID フィールドでも大文字やスペースを含めてまったく同じ名前にする必要があります。

Windows ネットワークプリンタへの印刷

ThinOS は、Microsoft プリントサーバによって共有されるプリンタに印刷できます。ThinOS からの SMB 印刷を設定する場合、シンクライアント設定への変更が必要となる可能性があるため、設定要件によっては検討が必要となります。

Microsoft Windows プリントサーバに接続するにはドメイン資格情報が必要であるため、ThinOS に資格情報を提供する必要があります。そのためには、プリンタの使用時に求められた場合に入力するか、または Dell Wyse ログイン画面からキャッシュされた資格情報を提供する管理者の設定を使用します。「Windows ネットワークプリンタ（SMB）のための INI パラメータの使用」の例「**3：ThinOS によってキャッシュされたユーザー資格情報を使用するための SMB プリンタの定義（詳細）」を参照してください。**このセクションでは、どちらの方法も説明します。

Windows ネットワークプリンタのためのプリンタ設定ダイアログボックスの使用

SMB プリンタをこの方法で設定すると、印刷する前に毎回ユーザーに資格情報の入力を強制します。つまり、ユーザーは資格情報を入力するために、リモートセッションから一時的に離されます（このことは、「Windows ネットワークプリンタのための INI パラメータの使用」で説明しているように INI ファイルを使用することで回避できます）。

ここではタスクのコンテキストを入力します（オプション）。ここには、導入用のコンテンツが配置されます。

1 デスクトップメニューで、**システム設定 > プリンタ**をクリックします。
プリンタ設定ダイアログボックスが表示されます。

2 Windows のネットワークプリンタに印刷する場合は、**SMBS** タブをクリックし、次のガイドラインに従います。

メモ：Windows によって共有されるプリンタ名には、スペースを含めないでください。ThinOS でプリンタが使用できなくなります。

a **SMB の選択**——リストから SMB を選択します。

b **¥¥ホスト¥プリンタ**—ボックスの横にあるフォルダ参照用のアイコンをクリックして Microsoft ネットワークを参照し、使用可能なネットワークプリンタ（ネットワーク上の Windows プリントサーバの DNS 名または IP アドレス）からプリンタを選択します。

必要なドメイン資格情報を入力した後に、**プリンタ設定**ダイアログボックスが表示されます。

c **プリンタ名**——プリンタのリストに表示する名前を入力します。

d **プリンタ ID**——大文字やスペースも含めて、Windows プリンタドライバの名前とまったく同じになるように、プリンタのタイプまたはモデルを入力します。

この例では、HP LaserJet 4100 Series PCL と入力します。

e **プリンタクラス**——デフォルトのままでかまいません。

f **プリンタデバイスを有効にする**——選択して、プリンタを有効にする必要があります。
このオプションにより、デバイスは有効になり、リモートホストで表示されます。

テスト印刷をクリックすると、Windows 資格情報を入力するよう求められます。この資格情報を使用して、プリンタ共有にアクセスします。このダイアログボックスは、このプリンタに印刷しようとするときにユーザーに表示されるダイアログボックスと同じです。

Windows ネットワークプリンタ（LPD）のための INI パラメータの使用

ThinOS INI パラメータを使用して SMB 印刷を設定すると、わかりやすい簡単な方法で環境内のすべてのクライアント用に、Windows サーバによって共有されているプリンタを設定できます。ThinOS INI パラメータを使用して SMB 印刷を設定する最も大きな利点は、プリンタの認証に使用するドメインアカウントを事前に定義できることです。次の例では、資格情報の提供方法を示しています。

1. プレーンテキストの一般的なユーザー資格情報を使用した SMB プリンタの定義

```
Printer=SMB1 \
LocalName="Demo SMB Printer" \
Host=\\dp-dc-ftp \
Name="TechSupportPrinter" \
PrinterID="HP LaserJet 4100 Series PCL" \
Enabled=yes \
Username=Username1 \
Password=Password \
Domain=contoso
```

2. 暗号化された一般的なユーザー資格情報を使用した SMB プリンタの定義

```
Printer=SMB1 \
LocalName="Demo SMB Printer" \
Host=\\dp-dc-ftp \
Name="TechSupportPrinter" \
PrinterID="HP LaserJet 4100 Series PCL" \
Enabled=yes \
Username-enc=PACGOGDBPKDOPGDGKC \
Password-enc=PFDBOHDBODCJPODP \
Domain=contoso
```

メモ：INI ファイルで使用する暗号化されたパスワードを作成するには、ConfGen などのプログラムを使用できます。このアプリケーションは、暗号化された文字列の作成をビルトインでサポートしています。ConfGen は、technicalhelp.de/からダウンロードできます。

重要: このツールはサポート対象外です。この例を説明する目的でのみ説明しています。

3. ThinOS によってキャッシュされたユーザー資格情報を使用するための SMB プリンタの定義（詳細）

メモ：この方法では、ユーザーは ThinOS にログインし、資格情報を後で使用できるようキャッシュに保存する必要があります。以下に示す INI セクションの例では、必要な最小限の要件が記載されています。

Signon=NTLM

```
Connect=RDP \
Host=1.2.3.4 \
Username=$UN \
Password=$PW \
Domain=$DN \
AutoConnect=1
```

```
Printer=SMB1 \
LocalName="Demo SMB Printer" \
Host=\\dp-dc-ftp \
Name="TechSupportPrinter" \
```

```
PrinterID="HP LaserJet 4100 Series PCL" \
Enabled=yes \
Username=$UN \
Password=$PW \
Domain=$DN
```

プリントサーバとしてのシンクライアントの使用

ThinOS のシンクライアントを基本的なネットワークプリントサーバとして設定すると、他のシンクライアントとローカルプリンタを共有できます。

LPD サービスの設定のためのプリンタ設定ダイアログボックスの使用

クラシックデスクトップモードでのみ、ネットワーク上でシンクライアントをプリンタサーバにして、LPD（Line Printer Daemon）サービスを提供するようシンクライアントを設定できます。次のように、LPD プリントサービスを提供するシンクライアントをセットアップします。
プリンタ設定ダイアログボックスを使用して、LPD サービスを設定するには、次の操作を行います。

1 デスクトップメニューで、**システム設定 > ネットワーク設定**をクリックし、**ネットワーク設定**ダイアログボックスを開きます。
2 シンクライアントの静的 IP アドレスを入力します。
3 デスクトップメニューで、**システム設定 > プリンタ**をクリックし、**プリンタ設定**ダイアログボックスを開いて、一覧から任意のポートを選択します。
4 LPT を選択します。
5 **プリンタ名**ボックスのプリンタに名前を付けます。
6 **プリンタ ID** に、プリンタのタイプまたはモデルを入力します。大文字やスペースも含めて、Windows プリンタドライバの名前とまったく同じにします。この例では、HP LaserJet 4000 Series PCL と入力します。
7 **プリンタクラス**はデフォルトのままでかまいません。
8 **プリンタデバイスを有効にする**を選択します。
9 **このプリンタの LPD サービスを有効にする**を選択します。
10 Windows 2003/2008 サーバをセットアップする場合は、「Windows 2003/2008 サーバのセットアップ」を参照してください。

Windows サーバのセットアップ

Windows 2003/2008 サーバ設定を設定するには

1 **Control Panel > Administrative Tools > Services** に移動して、Microsoft TCP/IP 印刷サービスがインストールされていることを確認します。インストールされていない場合は、Microsoft のインストール手順に従ってインストールします。
2 次の手順を完了して、LPD プリンタとしてシンクライアントを追加します。
   a **Control Panel > Printers > Add Printers > Local Printer > Create a new port** に移動して、**LPR PORT** を選択します。

ⓘ **メモ：LPR Port が表示されない場合は、Microsoft TCP/IP 印刷サービスが正しくインストールされていることを確認します。**

   b シンクライアントの IP アドレスまたは DNS 名を **Name or address of host providing LPD** ボックスに入力します。
   c 「LPD サービスの設定のためのプリンタ設定ダイアログボックスの使用」で割り当てたプリンタ名を **Name of printer on that machine** ボックスに入力します。
   d **OK** をクリックし、**NEXT** をクリックします。
3 プリンタを選択したら、アプリケーションサーバに対して通常のプリンタセットアップを実行できます。たとえば、製造元のプリンタタイプとプリンタ名を選択します。

LPD サービスの設定のための INI パラメータの使用

ThinOS INI パラメータを使用して LPD 印刷を設定すると、わかりやすい簡単な方法で ThinOS のシンクライアントを基本的なプリントサーバとして設定して、他のシンクライアントとローカルプリンタを共有できます。

次に示すのは、INI パラメータの例です。

```
Printer = LPT1 \
Name="HP LaserJet 4000" \
PrinterID="HP LaserJet 4000 Series PCL" \
Enabled=yes \
EnableLPD = yes
```

メモ：PrinterID は Windows プリンタ ドライバとまったく同じテキストになります。よって、Windows でプリンタ ドライバの名前が HP LaserJet 4000 Series PCL という場合は、INI パラメータの PrinterID フィールドでも大文字やスペースを含めてまったく同じ名前にする必要があります。

ThinPrint の設定

ThinPrint 固有の設定は、シンクライアントでは使用できません。そのため、ThinPrint を使用可能にするには、ユーザーは最初にユーザードキュメントに従ってプリンタをセットアップし、**プリンタ設定**ダイアログボックスを使用してシンクライアント上で ThinPrint を設定する必要があります。

ThinPrint を設定するには、次のガイドラインに従います。

- **プリンタ ID** フィールドを使用して、プリンタクラスを入力します（プリンタ名は必要に応じて変更できます）。
- 次のように、プリンタ ID が割り当てられます（物理ポートによって異なります）。
  - COM1 = 1
  - COM2 = 2
  - LPT1 = 3——USB プリンタは自動的に LPT1 で検出
  - LPT2 = 4
  - LPD0 = 5——LPD キュー名をプリンタ名として、プリンタ識別情報をクラスとして送信
  - LPD1 = 6——LPD キュー名をプリンタ名として、プリンタ識別情報をクラスとして送信
  - LPD2 = 7——LPD キュー名をプリンタ名として、プリンタ識別情報をクラスとして送信
  - LPD3 = 8——LPD キュー名をプリンタ名として、プリンタ識別情報をクラスとして送信
  - SMB1 = 9——¥¥ホスト¥プリンタ共有の形式
  - SMB2 = 10
  - SMB3 = 11
  - SMB4 = 12

関連する ThinPrint 製品をサーバにインストールするには、次のガイドラインに従います。

- **管理者が手動で作成したプリンタオブジェクト**——.print Engine をインストールした後、サーバにプリンタオブジェクトを作成して、ネイティブのドライバと、プリンタポートとして ThinPort を使用します。ThinOS には、すべてのプロトコル用に.print クライアントが備わっているため、どのプロトコル（TCP、RDP または ICA）でも使用できます。プリンタオブジェクトは、ThinPrint の命名規則に従う必要があります。たとえば、HPLJ5#_:2 の場合は、.print クライアントのポート ID を参照して、プリントジョブは ID 番号が.2 のローカルプリンタに送信されます。ID 番号がない場合は、.print クライアントは現在設定されているプリンタにプリントジョブを送信します。
- **ThinPrint AutoConnect によって自動作成されたプリンタオブジェクト**——ThinPrint AutoConnect を使用する場合は、シンクライアントは、シンクライアント ID 番号 84 で識別されるため、ローカルスプーラを持たないシンクライアントとして認識されます。また、ネイティブのドライバ（例、HPLJ5）と ThinPort を使用するサーバにテンプレートを設定し、このテンプレートに _#AnyName という形式で名前を付けることもできます。

  このサーバテンプレートを使用するために、ThinPrint Autoconnect [1]に対する規則が設定され、目的のローカルプリンタが割り当てられていることを確認できます。割り当てられたプリンタは、HPLJ5 ドライバと ThinPort を使用するセッションに表示されます。プリンタの名前は、クライアント側からのプリンタ名も含めて、ThinPrint の命名規則に従って自動的に命名されます。または、テンプレート名をクライアントプリンタ名に従って定義することもできます（.AnyName.を上のプリンタ名 4.および 5.で変更します。たとえば、_#HP Laserjet 5 にします）。これにより、ThinPrint Autoconnect で規則を定義することなく、ローカルプリンタオブジェクト.HP Laserjet 5.がこのテンプレートにマップされます。

重要なメモ

VNC RFB のバージョンのアップグレード——ThinOS 8.0_214 以降、VNC RFB のバージョンは 3.8 にアップグレードされました。このバージョンのアップグレードによって、DameWare などのアプリケーションがサポートされます。このため現在では管理者は、DameWare または VNC Viewer を使用して、リモートから ThinOS デバイスを利用できます。8.0_214 より以前は、VNC Viewer のみが使用できました。

トラブルシューティング

このセクションでは、何らかの問題を経験したときに、実施できる基本的なトラブルシューティングについて説明します。

- ファームウェア／パッケージのアップデート:パッケージのアップデートでエラーになる場合、新しいバージョンのファームウェアにアップデート後動作しない（デスクトップに接続できない）場合、あるいはそれ以上のエラーがある場合の回避策としては、すべてのパッケージを削除し、リブートしてパッケージを再インストールします。
- Blast 接続：起動に問題がある場合、リモートデスクトップのステータスとネットワークのステータスを確認します。たとえば、ユニットを何度か再起動してみて、デスクトップが正常に接続されるか、などです。

よくある質問

質問: RDP windows 10 セッションで USB リダイレクトを有効にする方法は？

回答——ポリシーを変更する必要があります。**Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Service > Remote Desktop Session Host > Device and Resource Redirection > Do not allow supported Plug and Play device redirection** と順番に進み、このポリシーを無効にします。

ファームウェアのインストール

ファームウェアのインストールとは、シンクライアントに ThinOS ファームウェアをインストールする一連の作業です。ThinOS ファームウェアをインストールするには、次の方法のいずれか 1 つを使用します。

- File Transfer Protocol（FTP）Windows サーバ
- HTTP/HTTPS Windows サーバ
- Dell Wyse Management Suite バージョン 1.2
- Dell Wyse USB Imaging Tool バージョン 3.1.0

表 41. ファームウェアイメージ

プラットフォーム	ThinOS	ThinOS（PCoIP 対応）
Wyse 5070 シンクライアント——Celeron Processor	X10_wnos	PX10_wnos
Wyse 5070 シンクライアント——Pentium Processor	X10_wnos	PX10_wnos
Wyse 5070 Extended シンクライアント——Pentium Processor	X10_wnos	PX10_wnos

表 42. パッケージの情報

パッケージ名	詳細
Base.i386.pkg	ファームウェアのアップグレード時に自動的にアップデートされます。
Pcoip.i386.pkg	PCoIP クライアントファームウェアのアップグレード時に自動的にアップデートされます。
RTME.i386.pkg	新しいパッケージを一元設定にアップロードすると、INI 設定をしなくてもシステムはアップデートできます。
Horizon.i386.pkg	新しいパッケージを一元設定にアップロードし、このパッケージをアップデートするように INI パラメータを設定します。
FR.i386.pkg	新しいパッケージを一元設定にアップロードし、このパッケージをアップデートするように INI パラメータを設定します。
TCX.i386.pkg	新しいパッケージを一元設定にアップロードし、このパッケージをアップデートするように INI パラメータを設定します。

メモ：

- – ファームウェアをインストールする前、または ThinOS クライアントを起動する前に、モニタ、キーボード、マウス、ネットワークを接続して、シンクライアントが正しく機能するかどうか確認することを、デルはお勧めします。
- – ThinOS は起動後、パッケージをロードする前に、ネットワーク接続をチェックします。

FTP サーバを使用したファームウェアのインストール

必ず Microsoft Internet Information Services（IIS）および FTP サービスをインストールして、Windows の PC または Server を設定してください。FTP サーバをインストールしていない場合、support.microsoft.com の FTP サーバの設定方法に関する記事を参照してください。

Windows IIS をインストールすると、ディレクトリ C:¥inetpub¥ftproot が作成されますが、これは FTP ルートと呼ばれます。FTP ルートディレクトリに、フォルダ wyse とサブフォルダ wnos を作成します。ディレクトリ構造は、C:¥inetpub¥ftproot¥WYSE¥wnos とな

る必要があります。

FTP サーバを使用した ThinOS ファームウェアのアップグレード：

1 www.dell.com/support にアクセスします。
2 お使いのシンクライアントのモデルに対応する、最新の ThinOS ファームウェアおよび最新の ThinOS パッケージをダウンロードします。ファームウェアとパッケージが圧縮された自己解凍形式（.EXE）または ZIP ファイル形式（.ZIP）の場合は、ファイルを抽出します。
3 抽出したファームウェアファイルとパッケージは FTP サーバのそれぞれ **C:¥inetpub¥ftproot¥WYSE¥wnos** フォルダと **C:¥inetpub¥ftproot¥WYSE¥wnos¥pkg** に置きます。
4 C:¥inetpub¥ftproot¥WYSE¥wnos フォルダに、次の INI パラメータを持つ wnos.ini テキストファイルを（テキストエディターを使用して）作成します。

   Autoload=1 loadpkg=1 Addpkg=TCX,FR,horizon

   Autoload=1 オプションによって、強制的にファームウェアのインストール／アップグレードを行うことが可能となります。LoadPkg オプションは、外部パッケージのアップデート方法を指定します。LoadPkg がステートメントにない場合、AutoLoad の値を継承します。

   ベースパッケージと PCoIP パッケージは、ThinOS ファームウェアイメージに統合されています。最新の ThinOS ファームウェアイメージをインストールすると、これらのパッケージの最新バージョンが ThinOS クライアントに自動でインストールされます。「AutoLoad=1 LoadPkg=0」と設定すると、ファームウェアはチェックされますが、パッケージはチェックされません。ファームウェアをチェックした後、パッケージのチェックが実行されます。ThinOS 8.3 以降、外部パッケージのアップデートの仕組みが変更されました。一部のパッケージはデフォルトとなり、LoadPkg の値に従ってロードされます。ここでは例として RTME を使用します。一部のパッケージでは、追加のパラメータとして AddPkg パラメータを追加する必要があります。たとえば、FR、Horizon、TCX です。AddPkg オプションは、パッケージを追加するためのものです。これは LoadPkg の値に依存します。INI パラメータの使用法の詳細については、『Dell Wyse ThinOS INI Reference Guide』を参照してください。
5 wnos.ini ファイルを保存します。
6 ThinOS クライアントデスクトップで、**システム設定 > 管理サーバ設定 > 全般**と順に進みます。
7 **全般**タブで、FTP サーバまたはディレクトリの IP アドレス、ユーザー名、パスワードを入力します。**ユーザ名**フィールドは「Anonymous」にする必要があり、**パスワード**フィールドはすでに事前設定されています。FTP サーバが Anonymous をサポートしている場合、ユーザー名に **Anonymous** と入力し、事前設定されたパスワードを使用します。サポートしていない場合は、**ユーザ名**および**パスワード**フィールドはブランクのままとします。

   メモ：
   - デフォルトのパスワードがない場合、またはパスワードが変更されている場合は、パスワードを設定する必要があります。たとえば、abe@abc.com。 シンクライアントを工場出荷時のデフォルトにリセットすることもできます。シンクライアントを工場出荷時のデフォルトにリセットすると、デフォルトのパスワードを持つ anonymous（匿名）ユーザーが設定されます。ただし、シンクライアンを再設定する必要があります。
   - DHCP オプションタグ 161 および 162 を使用して、ThinOS クライアント、ファイルサーバおよびパス情報を設定することもできます。DHCP サーバにこれらのオプションを作成し、正しいサーバ情報で設定し、お使いの環境で DHCP サーバのスコープを有効にする必要があります。
8 **OK** をクリックします。
9 シンクライアントをリスタートし、パッケージの自動インストールが完了するまで待機します。

シンクライアントがアップグレードされたことを確認するには、ThinOS デスクトップで、**システム情報 > 全般**と進み、システムバージョンを確認します。

HTTP または HTTPS を使用したファームウェアのインストール

必ず Microsoft Internet Information Services（IIS）および HTTP/HTTPS サービスをインストールして、Windows の PC または Server を設定してください。HTTP または HTTPS サーバをインストールしていない場合は、support.microsoft.com の HTTP または HTTPS サーバの設定方法に関する記事を参照してください。

Web サーバが、ThinOS で使用されるファイルタイプを識別できることを確認します。IIS で 2 つの MIME タイプを作成します。MIME のオプションは、サイト毎に設定する必要があります。デフォルトの IIS では、次のようにインストールします。

1 IIS 管理コンソールを起動します。
2 デフォルトの Web サイトをブラウズし、右クリックをして、**プロパティ**を選択します。
3 **HTTP Headers** タブをクリックし、**MIME Map** セクションで、**File types > New Type** と順に選択します。
4 2 つの MIME タイプを追加します。関連する拡張フィールドには、「.INI」と「.」を使用します。
5 設定を適用し、IIS 管理コンソールを終了します。

IIS をインストールすると、デフォルトディレクトリ **C:¥inetpub¥WWWroot** が作成されますが、これは WWW ルートと呼ばれます。**WWWroot** ディレクトリに、フォルダ **WYSE** とサブフォルダ **wnos** を作成します。 ディレクトリ構造は、**C:\inetpub\wwwroot\WYSE\wnos** となる必要があります。

HTTP または HTTPS サーバを使用した ThinOS ファームウェアのアップグレード：

1 www.dell.com/support にアクセスします。
2 お使いのシンクライアントのモデルに対応する、最新の ThinOS ファームウェアおよび最新の ThinOS パッケージをダウンロードします。ファームウェアとパッケージが圧縮された自己解凍形式（.EXE）または ZIP ファイル形式（.ZIP）の場合は、ファイルを抽出します。
3 抽出したファームウェアとパッケージは、HTTP または HTTPS サーバのそれぞれ **C:\inetpub\wwwroot\WYSE\wnos** フォルダと **C:\inetpub\wwwroot\WYSE\wnos\pkg** に置きます。
4 **C:\inetpub\wwwroot\WYSE\wnos** フォルダに、次の INI パラメータを持つ wnos.ini テキストファイルを（テキストエディターを使用して）作成します。

   Autoload=1 loadpkg=1 Addpkg=TCX,FR,horizon

   Autoload=1 オプションによって、強制的にファームウェアのインストール／アップグレードを行うことが可能となります。LoadPkg オプションは、外部パッケージのアップデート方法を指定します。LoadPkg がステートメントにない場合、AutoLoad の値を継承します。

   ベースパッケージと PCoIP パッケージは、ThinOS ファームウェアイメージに統合されています。最新の ThinOS ファームウェアイメージをインストールすると、これらのパッケージの最新バージョンが ThinOS クライアントに自動でインストールされます。「AutoLoad=1 LoadPkg=0」と設定すると、ファームウェアはチェックされますが、パッケージはチェックされません。ファームウェアをチェックした後、パッケージのチェックが実行されます。ThinOS 8.3 以降、外部パッケージのアップデートの仕組みが変更されました。一部のパッケージはデフォルトとなり、LoadPkg の値に従ってロードされます。ここでは例として RTME を使用します。一部のパッケージでは、追加のパラメータとして AddPkg パラメータを追加する必要があります。たとえば、FR、Horizon、TCX です。AddPkg オプションは、パッケージを追加するためのものです。これは LoadPkg の値に依存します。INI パラメータの使用法の詳細については、『Dell Wyse ThinOS INI Reference Guide』を参照してください。
5 wnos.ini ファイルを保存します。
6 ThinOS クライアントデスクトップで、**システム設定 > 管理サーバ設定 > 全般**と順に進みます。
7 **全般**タブで、ファイルサーバまたはディレクトリの IP アドレスを入力します。たとえば、「**https://IPaddress/wyse**」です。

   メモ： DHCP オプションタグ 161 および 162 を使用して、ThinOS クライアント、ファイルサーバおよびパス情報を設定することもできます。DHCP サーバにこれらのオプションを作成し、正しいサーバ情報で設定し、お使いの環境で DHCP サーバのスコープを有効にする必要があります。
8 **OK** をクリックします。
9 シンクライアントをリスタートし、パッケージの自動インストールが完了するまで待機します。

Wyse Management Suite を使用したファームウェアのインストール

Wyse Management Suite にカスタムグループを作成し、ThinOS デバイスをそのグループに割り当てたことを確認します。最新の『Dell Wyse Management Suite 管理者ガイド』を参照してください。
ThinOS クライアントが Wyse Management Suite に登録されたことを確認します。

Wyse Management Suite を使用した ThinOS ファームウェアのアップグレード：

1 www.dell.com/support にアクセスします。
2 お使いのシンクライアントのモデルに対応する、最新の ThinOS ファームウェアおよび ThinOS パッケージをダウンロードします。
3 正しい認証情報を使用して、Wyse Management Suite にログインします。
4 アプリとデートページの OS イメージリポジトリセクションで、**ThinOS** をクリックします。
5 **ファームウェアファイルの追加**をクリックします。

   ファイルの追加ダイアログボックスが表示されます。
6 ダウンロードされたファームウェアファイルをブラウズし、選択します。適切な説明を入力します。
7 **アップロード**をクリックします。

   ThinOS のファームウェアファイルがアップロードされ、そのファームウェアファイルが**アプリとデータ – OS イメージりぽじとり-ThinOS OS** ページに表示されます。
8 お使いの ThinOS のファームウェアファイルに対応するチェックボックスをオンにします。
9 **グループ&設定**ページでカスタムグループを選択し、ポリシーの編集 **> ThinOS** を順にクリックします。

   ThinOS 設定モードの選択画面が表示されます。
10 **詳細設定**をクリックします。

11 **デバイス設定**ペインで、**ファームウェアのアップグレード**をクリックし、**この項目を設定する**をクリックします。
12 **プラットフォームタイプ**ドロップダウンリストで、お使いのシンクライアントのモデルを選択します。
13 **自動導入のためのファームウェア**ドロップダウンリストで、シンクライアントのモデルに対応するファームウェアファイルを選択します。
14 **保存して公開**をクリックします。
シンクライアントが再起動され、ファームウェアのバージョンがアップグレードされます。

Dell Wyse USB Imaging Tool を使用したファームウェアのインストール

Dell Wyse USB Imaging Tool バージョン 3.1.0 を使用して、シンクライアントに ThinOS Merlin のイメージをインストールします。インストール手順の詳細については、downloads.dell.com/wyse/USBFT/3.1.0/の『Dell Wyse USB Imaging Tool version 3.1.0 User's Guide』を参照してください。