Dell Wyse Thin Client 用 Microsoft Windows 10 IoT Enterprise

管理者ガイド

DELL EMC

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その危険を回避するための方法を説明しています。

警告: 物的損害、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。

2019 - 11

Rev. A09

目次

1

はじめに

Windows 10 IoT Enterprise オペレーティング システムを実行する Dell Wyse Thin Client は、アプリケーション、ファイル、ネットワーク リソースへのアクセスを行います。アプリケーションとファイルは、Citrix Receiver、Microsoft Remote Desktop Connection、VMware Horizon クライアント セッションをホストしているマシンで使用できるようになります。

他のローカルにインストールされたソフトウェアでは、シンクライアントのリモート管理が可能であり、ローカルメンテナンス機能が提供されます。64 ビット Windows と互換性のあるセキュアなユーザーインターフェイスを必要とする環境で、さまざまな周辺機器と機能をサポートするアドオンが他にも数多くあります。詳細については、www.microsoft.com を参照してください。

メモ:

- **Windows 10 IoT オペレーティングシステムは、シンクライアントをインターネットに接続するとアクティブになります。Microsoft アクティベーション サーバがビジー状態の場合は、Windows 10 IoT がアクティブ化されるまで待つ必要があります。アクティベーション ステータスを確認するには、スタート > 設定 > 更新とセキュリティ > ライセンス認証 に移動します。**
- **このガイドに記載されている機能は、職場でのシンクライアントモデルによって異なります。使用しているシン クライアントに適用可能な機能の詳細については、https://support.dell.com/manuals のそれぞれのユーザー ガイドを参照してください。**

テクニカル サポート

テクニカル リソースのセルフサービス ポータル、ナレッジベース文書、ソフトウェア ダウンロード、登録、保証の延長/RMA、リファレンス マニュアル、連絡先情報などにアクセスするには、https://support.dell.com を参照してください。

本書について

このガイドは、Windows 10 IoT Enterprise を実行しているシンクライアント管理者を対象としています。Windows 10 IoT Enterprise 環境の設計と管理に役立つ情報と詳細なシステム構成を提供します。

サポートされる Thin Client

次のリストは、Windows 10 IoT Enterprise で実行されるシンクライアントです。

- Wyse 5470 Thin Client
- Wyse 5470 All-in-One Thin Client
- Wyse 5070 Thin Client (Celeron プロセッサー搭載)
- Wyse 5070 Thin Client (Pentium プロセッサー搭載)
- Wyse 5070 Extended Thin Client (Pentium プロセッサー搭載)
- Wyse 5060 Thin Client
- Wyse 7040 Thin Client
- Latitude 3480 モバイル Thin Client
- Latitude 5280 モバイル Thin Client

メモ: Wyse 7040 Thin Client は Windows 10 IoT Enterprise Threshold 1 オペレーティング システムをサポートし、それ以外のシン クライアントは Windows 10 IoT Enterprise Redstone 1 のオペレーティング システムをサポートします。

2

操作を始める

初めてシンクライアントを起動すると、Quick Start アプリケーションが起動します。このツールは、シンクライアントのソフトウェアとハードウェアの機能を表示します。また、VDI アプリケーション、管理ソフトウェア、およびサポートされている周辺機器についても説明しています。

Quick Start アプリケーションを使用して Wyse Easy Setup アプリケーションをインストールすることもできます。Wyse Easy Setup アプリケーションを使用すると、シン クライアントにすばやく簡単に設定を導入できます。詳細については、「Wyse Easy Setup」を参照してください。

Quick Start アプリケーションを終了すると、ユーザーのデスクトップがデフォルトで表示されます。このツールは後で起動することもできます。

ユーザーまたは管理者としてシンクライアントにログインすることができます。管理者はユーザーアカウントを設定して、自動的にログインできるように、またはログイン資格情報を手動で入力してログインするようにできます。

Wyse Management Suite を使用すると、シンクライアントの設定、監視、管理、および最適化を一元的に行うことができます。詳細については、「Wyse Management Suite の使用」を参照してください。

シン クライアントの使用を開始するには、以下を参照してください。

- 自動および手動ログオン
- シンクライアントを設定する前に
- スタート メニューの使用
- 検索ボックスの使用
- アクションセンターの使用
- アプリケーションをデスクトップにグループ化
- プリンタや外付けデバイスへの接続
- 電源ステータス

自動および手動ログイン

シンクライアントの電源が入ったときまたは再起動のとき、管理者の設定によって、自動ログインしたり、手動で (ユーザーまたは管理者の資格情報を使用して) ログインしたりできます。

詳細については、「ユーザーアカウントを使用したユーザーとグループの管理」を参照してください。

メモ:

- **統合書き込みフィルタ (UWF) を無効にしてから、シンクライアントのパスワードを変更するようにしてください。パスワードの変更後、UWF を必ず有効にしてください。詳細については、「シンクライアントを設定する前に」を参照してください。**
- **パスワードを変更するには、Ctrl+Alt+Delete キーを押して、パスワードの変更 をクリックします。ただし、この機能は ユーザー アカウントには適用されません。**

シンクライアントを起動すると、デフォルトでユーザーのデスクトップに自動的にログインします。

別のユーザーアカウントでログインするには、サインアウトして、ログイン画面で希望するユーザーアカウントをクリックする必要があります。次の資格情報を使用すると、別のユーザーアカウントにログインできます。

- **管理者** - デフォルトのユーザー名は **Admin** で、デフォルトのパスワードは **DellCCCvdi** です (大文字 / 小文字を区別)。
- **ユーザー** - デフォルトのユーザー名は **User** で、デフォルトのパスワードは **DellCCCvdi** です (大文字 / 小文字を区別)。
- **カスタマイズしたユーザー** - カスタマイズしたユーザーアカウントに設定されているユーザー資格情報を入力して、シンクライアントにログインします。

シンクライアントを設定する前に

シンクライアントを設定する前に、シンクライアントを保護する Unified Write Filter と xData Cleanup Manager が設定されていることを確認してください。Unified Write Filter ユーティリティーは、フラッシュ メモリーへの望ましくない書き込みを防止します。xData Cleanup Manager は、不要な情報をクリーンアップしてローカル ディスクに格納されないようにします。

ただし、シンクライアントからログアウトして再起動した後に、変更した設定を管理者が保持できるインスタンスがあります。

デスクトップの使用

初めてシンクライアントにログインすると、管理者による設定が表示されます。

管理者としてログインした場合は、**管理者のデスクトップ** が表示されます。タスクバーの右端にある **通知** アイコンをクリックして、**アクションセンター** ウィンドウを開きます。アクションセンターの詳細については、「アクションセンターの使用」を参照してください。

標準のデスクトップアイコンに加えて、ユーザープリファレンスの設定およびシステム管理のためのリソースの拡張セットが、管理者のコントロールパネルに含まれます。コントロールパネルを開くには、**スタート** > **コントロール パネル** の順に選択します。詳細については、「管理機能」を参照してください。

スタート メニューの使用

スタート メニューから、シンクライアント上のすべてのプログラム、フォルダ、および設定にアクセスできます。スタート メニューには、シンクライアントにインストールされているアプリケーションのリストが含まれます。

メモ: スタート メニューでは、よく使うアプリ の下に頻繁に使用するアプリケーションのリストが表示されます。

検索ボックスの使用

タスクバーの検索ボックスを使用すると、アプリケーション、ファイルまたは設定を検索できます。タスクバーの検索ボックスに検索するものを入力できます。また、シンクライアント全体からファイル、アプリケーション、または設定を検索した結果を確認できます。検索項目に関連するサジェスチョンと検索結果が **ホーム** ウィンドウに表示されます。

メモ: シンクライアント上の特定のファイルを検索するには、ホーム ウィンドウの下部ペインに示される以下の利用可能なフィルタのいずれかを適用し、目的のファイルを検索します。

- **アプリケーションフィルタ**
- **設定フィルタ**
- **ドキュメントフィルタ**
- **フォルダフィルタ**
- **写真フィルタ**
- **ビデオフィルタ**
- **音楽フィルタ**

アプリケーションをデスクトップにグループ化

仮想デスクトップを作成して、お使いのアプリケーションをまとめてグループ化します。タスクバーで、**タスクビュー** アイコンをクリックして、**新しいデスクトップ** で必要なアプリケーションを開きます。

仮想デスクトップ間でアプリケーションを移動するには、**タスクビュー** をクリックして、目的のアプリケーションを特定のデスクトップから別のデスクトップへとドラッグします。

アクションセンターの使用

アクションセンターは、Windows やアプリケーションからの重要な通知をクイックアクションとともにタスクバーに表示します。クイックアクションは、よく使う設定やアプリケーションをすぐに開くことができます。

通知やクイックアクションを表示するには、タスクバーで **アクションセンター** アイコンをクリックします。Windows ロゴ + A キーを押して表示することもできます。

- **通知を表示** — 通知がデスクトップに表示された場合、または **アクションセンター** で通知を表示する場合は、通知を展開して詳細を確認するか、関連アプリケーションを開くことなく対処します。また、通知を選択して画面の右端までドラッグするか、または **閉じる** ボタンをクリックすると、通知をクリアできます。
- **クイックアクション アイコン** — クイックアクション アイコンを使用すると、**すべての設定**と頻繁に使用するアプリケーション（Bluetooth、VPN、など）にアクセスできます。**展開** オプションを選択すると、場所、通知オフ、明るさ、Bluetooth、VPN、バッテリ節約機能、プロジェクト、接続、などの設定やアプリケーションが表示されます。

  アクションセンターの **クイックアクション** オプションを以下に示します。

  - **タブレットモード** — タブレットモードを使用すると、2in1 などのタッチ対応のデバイスを使用する場合や、キーボードやマウスを使いたくない場合に、Windows をさらに手軽で簡単に使えるようになります。タブレットモードをオンにするには、タスクバーで **アクションセンター** アイコンをクリックし、**タブレットモード** を選択します。
  - **接続** — このオプションは、ワイヤレスデバイスや Bluetooth デバイスに接続する場合に使用します。
  - **すべての設定** — Windows 設定を設定する場合に使用します。詳細については、「スタート メニューの使用」を参照してください。
  - **機内モード** — このオプションは、デバイスのワイヤレス通信機能をオフにして、**機内モード** を有効にする場合に使用します。

プリンタや外付けデバイスへの接続

シン クライアント デバイスの USB ポートには、USB インターフェイスのプリンターあるいは USB-パラレル アダプター インターフェイスのプリンターを接続できます。USB ポートに接続する前に、プリンタの USB インストール手順に従います。

プリンタに接続するには、**プリンタの追加** ウィザードを使用してプリンタをシンクライアントデバイスに追加します。詳細については、「プリンタの追加」を参照してください。

外付けデバイスに接続する場合は、シンクライアントデバイスにそのデバイスを追加します。詳細については、「デバイスの追加」を参照してください。

モニターへの接続

シンクライアントモデルに基づいて、外部モニターには次のポートを使用して接続できます。

- HDMI ポート
- VGA ポート
- ディスプレイ ポート
- DVI ポート
- DVI-D ポート
- Type-C ポート

デュアルモニターディスプレイの設定の詳細については、「デュアルモニターディスプレイの設定」を参照してください。

電源ステータス

シンクライアントデバイスの電源ステータスのオプションを変更するには、次に示す手順を実行します。

1. タスクバーで、**スタート** メニューボタンをクリックします。
2. スタートメニューで **電源** をクリックして、次のいずれかのオプションを選択します。
   - **スリープ** — このモードはあまり電力を使用しないため、シンクライアントデバイスは迅速に起動します。
   - **シャットダウン** — 開いているすべてのプログラムを終了して、オペレーティングシステムをシャットダウンする場合に向きます。
   - **再起動** — シンクライアントデバイスの電源がオフになってすぐにオンになります。

   電源ステータスオプションを使用するには、ALT+F4 キーを押して、ドロップダウンリストから希望のオプションを選択します。

   メモ: 自動ログオンが有効になっている場合、シンクライアントは即座にデフォルトユーザーのデスクトップにログインします。

3

アクセス可能なアプリケーション

管理者またはユーザーとしてシンクライアントにログインすると、Windows デスクトップでは **スタート** メニューに特定の拡張機能が表示されます。

次のタスクを実行できます。

- Internet Explorer を使用したインターネットの閲覧
- Dell シンクライアントアプリケーションの使用
- Citrix Receiver セッションサービスの設定
- リモートデスクトップ接続セッションサービスの設定
- VMware Horizon クライアントを使用した仮想デスクトップへの接続
- Ericom PowerTerm Terminal Emulation の使用
- Ericom Connect-WebConnect クライアントの使用
- Windows Media Player
- Wyse Easy Setup

メモ: キーボードの Caps Lock インジケータアプリケーション - Dell キーボードドライバソフトウェア (KM632) は、デスクトップで Caps Lock のステータスインジケータを表示します。シンクライアントにログイン後、Caps Lock キーを押すと、Caps Lock 機能が有効になり、デスクトップにロック記号が表示されます。もう一度 Caps Lock キーを押すと Caps Lock 機能は無効になり、デスクトップにロック解除の記号が表示されます。

Internet Explorer を使用したインターネットの閲覧

Internet Explorer を開くには、次のいずれかの操作を行います。

- **[スタート]** > **[Windows アクセサリ]** > **[Internet Explorer]** の順に選択します。
- デスクトップで **Internet Explorer** アイコンをダブルクリックします。

メモ:

- **ディスクへの書き込みを制限するために、Internet Explorer の設定は工場で行われています。この設定では、使用可能なディスクスペースの容量が制限されるときにそれを使用できません。これらの設定を変更しないことをお勧めします。**
- **Internet Explorer のキャッシュは 100 MB に設定されています。**

Dell シンクライアントアプリケーションの使用

Dell シンクライアントアプリケーションを使用して、シンクライアントデバイスについての一般情報、カスタムフィールド、RAM ディスク、自動ログイン、システムショートカット、およびサポート情報を表示します。

Dell シンクライアントアプリケーション ページにアクセスするには、**スタート** > **Dell シンクライアントアプリケーション** の順に移動します。デスクトップの **Dell シンクライアントアプリケーション** アイコンをクリックして **Dell シンクライアントアプリケーション** にアクセスすることもできます。

左のナビゲーションバーで、次のタブをクリックします。

- **クライアント情報** — シンクライアントデバイスの情報を表示します。
- **QFE** — シンクライアントに適用される Microsoft QFE (以前のホットフィックス) のリストを表示します。
- **インストールされた製品** — シンクライアントにインストールされたアプリケーションのリストを表示します。
- **WDM / WMS パッケージ** — シンクライアントに適用されている WDM および WMS パッケージのリストを表示します。
- **著作権 / 特許権** — 著作権、特許権の情報を表示します。

管理者としてログインすると、**Dell シンクライアントアプリケーション** ページに **カスタムフィールド**、**RAM ディスク**、**自動ログオン**、**システムショートカット**、**バージョン情報とサポート** などのタブが表示されます。

Dell シンクライアントアプリケーション ページには、Energy Star 準拠の Energy Star ロゴ (電子ロゴ) も表示されます。

バージョン情報とサポート タブには、アプリケーションのバージョン、サポートディレクトリ、サポートデータのエクスポート、および HTML ビューに関する情報を表示できます。

詳細については、「管理機能」を参照してください。

メモ: ダイアログボックスに示される情報は、シンクライアントデバイスおよびソフトウェアのリリースによって異なります。ユーザーとしてログインした場合、クライアント情報、QFE、インストール済み製品、WDM/WMS パッケージ、著作権 / 特許権、バージョン情報とサポート といった、数個のタブのみが表示されます。

Citrix Receiver セッションサービスの設定

Citrix Receiver は、ユーザーインタフェースからアプリケーションロジックを分離する、サーバベースのコンピューティングテクノロジです。シン クライアント デバイスにインストールされた Citrix Receiver クライアント ソフトウェアにより、すべてのアプリケーション プロセスがサーバー上で実行されているにもかかわらず、ローカル アプリケーション GUI で対話することができます。

Citrix Receiver セッション サービスは、ターミナル サービスと次のいずれかがインストールされた、Windows Server 2008、Windows Server 2012、または Windows Server 2016 のネットワーク上で使用することができます。

- Citrix 仮想アプリケーションとデスクトップ 7.5
- Citrix 仮想アプリケーションとデスクトップ 7.6
- Citrix 仮想アプリケーションとデスクトップ 7.8
- Citrix 仮想アプリケーションとデスクトップ 7.9
- Citrix 仮想アプリケーションとデスクトップ 7.11
- Citrix 仮想アプリケーションとデスクトップ 7.18

メモ:

Windows Server 2008 R2 を使用している場合、ターミナル サービス クライアント アクセス ライセンス (TSCAL) サーバーにもネットワークでアクセスできる必要があります。サーバにより一時ライセンスが付与され、120 日後に失効します。一時ライセンスの失効後、TSCAL を購入してサーバにインストールします。接続を確立するには一時的または永続的ライセンスが必要です。

Citrix Receiver セッションを設定するには、次の操作を行います。

1. 管理者 としてログインします。
2. 次のいずれかのオプションを使用して Citrix サーバにアクセスします。
   - **スタート** メニューで、**Citrix Receiver** をクリックします。
   - デスクトップで **Citrix Receiver** アイコンをダブルクリックします。

   Citrix サーバへのログイン後、**アカウントの追加** ウィンドウが表示されます。
3. **アカウントの追加** ウィンドウで、サーバ IP アドレスを入力します。
4. **次へ** をクリックします。
   - セキュアな接続には、**完全修飾ドメイン名**(FQDN)を入力します。
   - 非セキュアな接続には、IP アドレスを入力します。
5. ユーザーの資格情報を入力し、**ログオン** をクリックします。
   IP アドレスを入力することでアカウントの追加が可能になり、Citrix Receiver の詳細を表示することができます。
6. **はい** をクリックしてから **次へ** をクリックします。
   Citrix Receiver の仮想デスクトップが表示されます。
7. 仮想デスクトップウィンドウで、**Add Apps (+)** > **All Applications** の順に移動します。
   アプリケーションのチェックボックスをオンまたはオフにすることができます。選択したアプリケーションが仮想デスクトップに表示されます。
8. 仮想デスクトップで、**Settings** をクリックして、サーバのアカウントを更新、追加または削除して、ログオフします。

リモートデスクトップ接続セッションサービスの設定

リモートデスクトップ接続は、グラフィカルインタフェースを提供するネットワークプロトコルであり、ネットワーク接続を経由して別のコンピュータへの接続を確立します。

メモ: Windows Server を使用している場合、または Windows Server で Citrix XenApp 5.0 を使用している場合、ターミナル サービスのクライアント アクセス ライセンス (TSCAL) サーバーにもネットワークでアクセスできる必要があります。サーバにより一時ライセンスが付与され、120 日後に失効します。一時ライセンスの失効後、TSCAL を購入してサーバにインストールします。接続を確立するには一時的または永続的ライセンスが必要です。

リモートデスクトップ接続を設定するには、次の手順を実行します。

1. ユーザーまたは管理者としてログインします。
2. [**スタート**] メニューで、[**リモート デスクトップ接続**] をクリックするか、またはデスクトップの [**リモート デスクトップ接続**] アイコンをダブルクリックします。
   [**リモート デスクトップ接続**] ウィンドウが表示されます。
3. [**コンピューター**] ボックスに、コンピューター名またはドメイン名を入力します。
4. 詳細設定オプションを表示するには、[**オプションの表示**] をクリックします。
   a. [**全般**] タブでは、ログイン資格情報の入力、既存の RDP 接続の編集または開始、新規の RDP 接続ファイルの保存などを行えます。
   b. [**画面**] タブでは、リモート デスクトップの画面設定と画面の色を管理します。
      - スライダを動かして、リモートデスクトップのサイズを拡大または縮小します。全画面表示するには、スライダを右方向いっぱいに動かします。
      - ドロップダウンリストから、リモートデスクトップの画面の色を希望に応じて選択します。
      - [**全画面表示の使用時に接続バーを表示する**] チェック ボックスをオンまたはオフにして、全画面モードで接続バーを表示または非表示にします。
   c. [**ローカル リソース**] タブで、リモート デスクトップのオーディオ、キーボード、またはローカル デバイス/リソースの設定を行います。
      - [リモート オーディオ] セクションで、[**設定**] をクリックして詳細なオーディオ設定オプションを選択します。
      - [**キーボード**] セクションで、キーボードの組み合わせを適用する場合と場所を選択します。
      - [**ローカル デバイスとリソース**] セクションでは、リモート セッションで使用するデバイスとリソースを選択します。その他のオプションについては、[**詳細**] をクリックします。
   d. [**エクスペリエンス**] タブで、接続品質に基づいてリモート セッションのパフォーマンスを最適化します。

      メモ:

      統合書き込みフィルターのキャッシュがいっぱいである場合、ウィンドウの [オプションの表示] をクリックしてから [エクスペリエンス] タブのビットマップ キャッシングを無効にできます。
   e. [**詳細設定**] タブで、サーバーが認証に失敗した場合に実行するアクションを選択し、リモート ゲートウェイを経由する接続の設定を行います。
5. [**接続**] をクリックします。
6. リモート セッションに接続するには、[**セキュリティ**] ダイアログ ボックスにログイン資格情報を入力します。
   リモート デスクトップが表示され、[**接続バーを表示する**] を選択した場合は上部に接続バーが表示されます。

VMware Horizon Client を使用した仮想デスクトップへの接続

VMware Horizon Client はローカルにインストールされるソフトウェアアプリケーションであり、View Connection Server と Thin Client オペレーティングシステム間の通信を実行します。Thin Client から一元的にホストされる仮想デスクトップへのアクセスを提供します。VMware セッション サービスは、VMware Horizon 6 以降をインストールした後に、ネットワーク上で使用可能な状態にできます。このサービスは、エンドユーザーに対して単一のプラットフォームを介して、仮想化 / ホストされたデスクトップおよびアプリケーションを提供します。仮想デスクトップに接続するには、VMware Horizon Client ウィンドウを使用します。

VMware Horizon Client ウィンドウを開いて使用するには、次の手順を実行します。

1. ユーザーまたは管理者としてログインします。
2. 次のいずれかのオプションを使用して、VMware Horizon Client ウィンドウにアクセスします。
   - **スタート** メニューで、**VMware** > **VMware Horizon Client** の順にクリックします。
   - デスクトップで **VMware Horizon Client** アイコンをダブルクリックします。

   VMware Horizon Client ウィンドウが表示されます。
3. VMware Horizon Client ウィンドウでは、次のガイドラインを使用します。

a) 新しいサーバ接続を追加するには、VMware Horizon Client ウィンドウで **新規サーバ** オプションをクリックするか、**サーバの追加** アイコンをダブルクリックします。

VMware Horizon Client ダイアログボックスが表示されます。

b) **VMware Horizon Client** ダイアログボックスで、接続サーバのボックスに VMware Horizon Connection Server のホスト名または IP アドレスを入力します。

c) [**接続**] をクリックします。

d) **ログイン** ダイアログボックスで、ユーザー名とログインパスワードをそれぞれのボックスに入力します。

e) **ドメイン** ドロップダウンリストから、サーバが所属するドメインを選択します。

f) **ログイン** をクリックします。

VMware Horizon Client が、選択したデスクトップに接続します。接続の確立後、公開されているデスクトップのリストが表示されます。

g) 特定のアプリケーションまたはデスクトップのアイコンを右クリックしてから、**起動** をクリックして選択したアプリケーションまたはデスクトップに接続します。

VMware Horizon Client の詳細については、www.vmware.com を参照してください。

メモ:

証明書確認モード - 証明書確認モードでは、サーバへの接続が安全であることをクライアントが確認できない場合に、クライアントがどのような処理を行うべきかが決定されます。システム管理者の指示がない限り、この設定は変更しないことをお勧めします。

証明書確認モードにアクセスするには、ウィンドウの右上隅にあるアイコンをクリックし、ドロップダウンリストから SSL を構成 をクリックします。VMware Horizon Client SSL 構成 ダイアログボックスで、必要に応じて次のいずれかのオプションを選択します。

- **信頼されていないサーバに接続しません**
- **信頼されていないサーバに接続する前に、警告を表示します**
- **サーバ ID 証明書を確認しません**

Ericom Connect および WebConnect クライアントの使用

Ericom Connect および WebConnect クライアントは、互換性のある電話またはタブレットから Windows デスクトップおよびアプリケーションへのリモートアクセスを提供します。これは、管理対象ブローカへのアクセス専用です。Ericom Connect および PowerTerm WebConnect の接続は、セキュアゲートウェイをアドレスとして使用します。スタンドアロンまたはネットワーク上のアプリケーションとして、Ericom Connect-WebConnect クライアントにアクセスすることができます。

Ericom Connect および WebConnect クライアントにスタンドアロンアプリケーションとして接続するには、次の手順を実行します。

1. ユーザーまたは管理者としてログインします。
2. **スタート** > **Ericom Connect-WebConnect クライアント** > **Ericom Connect-WebConnect クライアント** の順に選択するか、またはデスクトップの **Ericom Connect-WebConnect クライアント** アイコンをダブルクリックします。
   Ericom AccessPad ログインウィンドウが表示されます。
3. Ericom AccessPad ログインウィンドウで、資格情報を入力し、**ログイン** をクリックします。
   DELL - Ericom アプリケーションゾーン ウィンドウが表示されます。

   メモ: デフォルトでは、Ericom AccessPad ログインウィンドウが表示されます。UI を希望の言語に設定するには、ウィンドウの右下隅にある 地球 アイコンをクリックし、ドロップダウンリストから希望の言語を選択します。
4. DELL - Ericom アプリケーションゾーン ウィンドウに、公開されているアプリケーション (**Blaze デモサーバ**、**RDP デモサーバ**、**Ericom サーバ**、**ペイント** など) が表示されます。
   これらのアプリケーションのいずれかをダブルクリックしてアクセスします。

   サーバサイトから独自のアプリケーションを追加することもできます。
5. デスクトップにショートカットを作成するには、DELL - Ericom アプリケーションゾーン ウィンドウで **オプション** > **デスクトップにショートカットを作成する** の順にクリックします。
6. ログアウトするには、DELL- Ericom アプリケーションゾーン ウィンドウで **ファイル** > **ログアウト** の順にクリックします。

Web ブラウザを介して Ericom Connect-WebConnect クライアントにアクセスするには、次の手順を実行します。

1. **Internet Explorer** アイコンをダブルクリックします。

   Internet Explorer の Web ページが表示されます。

2. URL として `http://serverIP/FQDNWebConnect6.0/AppPortal/Index.asp` を入力し、Ericom Power Term Emulation にアクセスします。

   PowerTerm WebConnect アプリケーションポータル ページが表示されます。
3. **PowerTerm WebConnect アプリケーションポータル** ページで、資格情報とドメイン名を入力します。
4. **ログイン** をクリックします。
5. ログインすると、公開されているデスクトップおよびアプリケーション（**Blaze デモサーバ**、**RDP デモサーバ**、**ペイント** など）が表示されます。

   これらのアプリケーションのいずれかをダブルクリックして、新しい Web ページでアクセスします。

   サーバサイトから独自のアプリケーションを追加することもできます。
6. **PowerTerm WebConnect アプリケーションポータル** ページの左側で **ログアウト** をクリックして、Ericom Power Term WebConnect セッションを終了します。

Ericom PowerTerm Terminal Emulation の使用

Ericom PowerTerm Terminal Emulation を使用して接続を管理するには、次の手順を実行します。

1. 次のオプションのいずれかを使用して、TELNET : PowerTerm InterConnect for thin clients ウィンドウを開きます。
   - デスクトップで **PowerTerm Terminal Emulation** アイコンをダブルクリックします。
   - **スタート** メニューで、**Ericom PowerTerm Terminal Emulation** > **PowerTerm Terminal Emulation** の順にクリックします。
2. **接続** ダイアログボックスで、**セッションタイプ** > **TELNET** の順に選択し、任意の接続を設定します。

Windows Media Player

Windows Media Player は、デジタルメディアファイルを再生するための直観的で使いやすいインタフェースを提供します。デジタルメディアコレクションが整理されて、お気に入りの音楽の CD への書き込み、CD の音楽の抽出、ポータブルデバイスとのデジタルメディアファイルの同期、およびオンラインストアでのデジタルメディアコンテンツの購入が可能になります。詳細については、https://support.microsoft.com にある Windows Media Player のドキュメントを参照してください。

Wyse Easy Setup

Wyse Easy Setup を使用すると、シンクライアントにすばやく簡単に設定を導入できます。

Wyse Easy Setup で実現可能なシナリオ例

- Internet Explorer の設定項目を設定して、専用のブラウザフォーカスクライアントを作成します。
- Citrix、VMware、リモートデスクトッププロトコル（RDP）などの複数のブローカー接続を設定します。
- デバイスを設定して、特定基幹業務用の専用アプリケーションを作成します。

Windows デバイスをロックダウンするためのキオスクモードを作成できます。ユーザーがキオスクモード以外のデバイスの機能またはファンクションにアクセスすることを防止できます。キオスクインタフェースをカスタマイズして、特定の設定へのユーザーアクセスを有効または無効にすることもできます。

詳細については、https://downloads.dell.com/wyse にある Wyse Easy Setup の『管理者ガイド』および『リリースノート』を参照してください。

Overlay Optimizer

Overlay Optimizer は、Microsoft Unified Write Filter（UWF）と動作するソフトウェア コンポーネントです。Overlay Optimizer は書き込みを保護し、デバイスのアップタイムを延ばします。Overlay Optimizer は、Windows 10 IoT Enterprise オペレーティング システムで動作します。

UWF は、RAM オーバーレイに変更を保存してディスクを保護します。アプリケーションがディスクにデータを書き込む際に、書き込みフィルターが RAM オーバーレイに書き込み動作をリダイレクトします。オーバーレイのサイズは事前に設定されており、動的に増加することはできません。オーバーレイ領域が一定期間不足すると、デバイスが再起動します。

Overlay Optimizer は、UWF のオーバーレイ領域とコンテンツを監視します。Overlay Optimizer は書き込みフィルターでのオーバーレイ領域の消費量が多いことを確認すると、使用されていないコンテンツを Overlay Optimizer のディスク オーバーレイに移動します。UWF オーバーレイをクリアすると、デバイスのアップタイムが長くなります。

詳細については、*Overlay Optimizer の各リリース ノート*（https://downloads.dell.com/wyse/）を参照してください。

Dell Secure Client

Dell Secure Client は、Windows ベースのシン クライアント用のセキュリティソフトウェアです。このソフトウェアは、ファイル、フォルダー、レジストリーの除外項目の変更に制限を加えます。

Dell Secure Client の主な機能

Dell Secure Client の主な機能は次のとおりです。

- 書き込みフィルターに含まれるファイル、フォルダー、レジストリーの除外リストを表示します。
- 統合書き込みフィルターに関する Dell Secure Client のステータスを表示します。
- Dell Secure Client サービスはポリシー エンジンとして機能します。ネストされたフォルダーのポリシーを統合し、レジストリー ハイブでも同じように更新します。
- 管理者がユーザー インターフェイスを使用して変更を加えた場合、ユーザーは Dell Secure Client のコマンドライン インターフェイスを使用して、.csv ファイルをポリシーでアップデートすることができます。
- 管理者は Dell Secure Client を使用して、書き込みフィルターで除外されたファイルおよびレジストリーのポリシーを追加、表示、削除することができます。
- ユーザー名、アプリケーション、書き込みフィルター除外リストの各エントリーのアクセス時間に基づいて、ポリシーを追加、削除、表示、変更することができます。

  メモ: ユーザー名とアプリケーション名は必須です。
- ポリシー設定データを.csv または.json 形式でインポートおよびエクスポートできます。
- ポリシーを自己完結型実行可能ファイル(SCE).exe ファイルとしてエクスポートできます。SCE ファイルはポリシー設定を.json 形式でカプセル化したものです。
- 管理者ユーザーインタフェースでは多言語サポートが提供されます。
- シン クライアントの再起動後にユーザーによって追加された Dell Secure Client 設定を保持するためにプロビジョニングを行います。
- ポリシーは、書き込みフィルターを無効にした後でのみ設定できます。
- Dell Secure Client が有効になっている場合、デフォルト ポリシーはすべてのユーザーに適用されます。
- Dell Secure Client ユーザー インターフェイスまたはコマンドライン インターフェイスを使用して、ポリシーをユーザーまたはグループに追加できます。このポリシーは、それぞれのユーザーまたはグループにログインするときに、デフォルト ポリシーとともに適用されます。
- ポリシーは、暗号化された.csv 形式で保存されます。

Dell Secure Client へのアクセス

Dell Secure Client には、次のいずれかの方法でアクセスできます。

- 管理者アカウントを使用する場合：
  1. 管理者 としてログインします。
  2. **スタート** > **Dell** > **DellSecureClient** の順に選択します。
- ユーザーアカウントを使用する場合：
  1. ユーザーとしてログインします。
  2. **スタート** > **Dell** > **DellSecureClient** の順に選択します。

     ユーザーアカウント制御 ウィンドウが表示されます。
  3. 管理者パスワードを入力し、**はい** をクリックします。

Dell Secure Client の設定

Dell Secure Client の設定は、次のいずれかの方法で行うことができます。

- Wyse Management Suite
- ローカル管理者ユーザー インターフェイス - Dell Secure Client GUI

Dell Secure Client ユーザー インターフェイスを使用したポリシーの設定

設定は、Dell Secure Client ユーザー インターフェイスでインポートまたはエクスポートすることができます。

設定のインポート

1. 書き込みフィルターを無効にします。
   シン クライアントが再起動します。
2. 管理者 としてログインします。
3. [Dell Secure Client アプリケーション] をダブルクリックします。
   Dell Secure Client のユーザー インターフェイスが表示されます。
4. [**エクスポート/インポート**] をクリックします。
5. 設定ファイルのパスを入力します。
6. **インポート** をクリックします。
   設定ポリシーは暗号化されて、C:\Program Files\Wyse\DellSecureClient\に.csv ファイルとして保存されます。

設定のエクスポート

1. 書き込みフィルターを無効にします。
   シン クライアントが再起動します。
2. 管理者 としてログインします。
3. [Dell Secure Client アプリケーション] をダブルクリックします。
   Dell Secure Client のユーザー インターフェイスが表示されます。
4. [**エクスポート/インポート**] をクリックします。
5. 設定ファイルのパスを入力します。
6. ファイル形式として、.csv (Dell Secure Client 設定) または.exe (インストール可能パッケージ) オプションを選択します。
7. **エクスポート** をクリックします。
   設定ポリシーは復号化され、エクスポートされます。

CSV 形式

出力.csv ファイルは次の形式です。

表 1. .csv 形式

ポリシータイプ	ファイル/フォルダー	アプリ	NT アカウント	時間範囲 (オプション)
ファイル (F)	C:\Temp\Sample.txt	C:\Windows\System32\notepad.exe	ユーザー	0700-1900
フォルダー	C:\Temp\	C:\Program Files\Windows NT\Accessories\Wordpad.exe	ユーザー	0700-1900
ファイル (F)	C:\Temp\Sample2.txt	C:\Windows\System32\notepad.exe	Admin1	
フォルダー	C:\Program Files\Windows Defender	C:\Windows\System32\mspaint.exe	システム	
レジストリー	HKLM\SOFTWARE\WOW6432Node\3DMAX	C:\Program Files (x86)\AutoCAD\audtocadx86.exe	ユーザー	
レジストリー	HKLM\SOFTWARE\WOW6432Node\3DMAX	C:\Program Files (x86)\AutoCAD\audtocadx86.exe	Admin1	
レジストリー	HKLM\SOFTWARE\WOW6432Node\Dell\CommandUpdate	C:\Program Files\Dell\Command	システム	

ポリシータイプ	ファイル/フォルダー	アプリ	NT アカウント	時間範囲 (オプション)
		Monitor\dataeng\bin\dsm_sa_datmgr64.exe		
レジストリー	HKLM\SOFTWARE\WOW6432Node\Dell\CommandUpdate	C:\Program Files\Dell\Command Monitor\dataeng\bin\dsm_sa_datmgr64.exe	Admin2	0900-1000

JSON 形式

出力.json ファイルは、次の形式になります。


```
{
  "deviceElements": null,
  "deviceElementsV2": null,
  "fullConfiguration": false,
  "shouldSendRemoteCommand": false,
  "isJailBroken": false,
  "compliantStatus": 0,
  "configCompliantStatus": 0,
  "passcodeCompliant": true,
  "encryptionCompliantStatus": 1,
  "computeJailbreak": true,
  "isCaValidationOn": false,
  "personInfoLean": null,
  "lastUpdatedAt": 1534142918777,
  "passcodeProfileDescription": null,
  "deviceQueryId": null,
  "deviceQueryStatus": null,
  "configurations": {
    "contentProvider": null,
    "description": null,
    "configSettings": [
      {
        "targetOS": null,
        "configName": "rcDellSecureClientSettings",
        "configItems": [
          {
            "itemKey": "rcDellSecureClientSettings",
            "itemValue": [
              [
                {
                  "itemKey": "policyType",
                  "itemValue": "file",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "location",
                  "itemValue": " C:\\Program Files\\AutoCAD ",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "application",
                  "itemValue": " C:\\Program Files\\AutoCAD\\audtocadx64.exe ",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "user",
                  "itemValue": " User ",
                  "itemValueExtra": null,
                  "valueType": "STRING"
```

```
                },
                {
                  "itemKey": "duration",
                  "itemValue": "0700-1900",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                }
              ],
              [
                {
                  "itemKey": "policyType",
                  "itemValue": "registry",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "location",
                  "itemValue": "    HKEY_LOCAL_MACHINE\\SOFTWARE\\WOW6432Node\\3DMAX ",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "application",
                  "itemValue": " C:\\Program Files (x86)\\AutoCAD\\audtocadx86.exe",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "user",
                  "itemValue": "User ",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "duration",
                  "itemValue": "0700-1900",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                }
              ]
            ],
            "itemValueExtra": null,
            "valueType": "JSON"
          }
        ],
        "contentVersion": "2.3.0"
      }
    ]
  },
  "allowUnregistration": true,
  "businessRuleInfo": null,
  "currentBiosAdminPassword": null,
  "mqttUrl": "tcp://10.150.38.10:1883",
  "wmsUrl": "https://brl-hackthon-win12R2:443/ccm-web",
  "heartbeatIntervalInMins": 0,
  "checkInIntervalInHours": 0,
  "groupToken": null,
  "personalDeviceSettings": null,
  "wmsVersion": "4.3.0",
  "maxCheckinIntervalInHours": 0
}
```


自己解凍ファイル

自己解凍形式の.exe 出力ファイルは、.json 形式のポリシー設定ファイルから構成されています。自己解凍形式の.exe ファイルは、設定ファイルを入力とするインポート コマンドで `dscmgr` 値を呼び出します。

このファイルは、Wyse Management Suite の高度なアプリケーション ポリシーを用いて、複数のクライアントで設定をインポートするために使用できます。また、ポリシーをインポートすると、成功コードも返されます。

設定の導入

複数のシンクライアントに設定を導入するには、次の 2 つの方法があります。

- Dell Secure Client ユーザー インターフェイス
- Wyse Management Suite

コマンドラインオプション

表 2. コマンドラインオプション

コマンド ライン	説明
`dscmgr /help` または `dscmgr ?`	このコマンドは、Dell Secure Client の [**ヘルプ**] メニューを表示するために使用します。
`dscmgr /init [Mode]`	このコマンドは、Dell Secure Client をアプリケーション ハッシュまたはアプリケーション パスモードで起動するために使用します。アプリケーション モードがデフォルトのモードで、値を入力しなければデフォルトのモードが選択されます。 [Mode] - アクセスを有効にする、またはブロックするモードを入力します。アプリケーションのバイナリ ハッシュまたはアプリケーション パスを使用できます。このパラメーターはオプションです。
`dscmgr /getappauthenticationmode`	このコマンドは、適用されたアプリケーション認証モードを表示します。
`dscmgr /addpolicy <Path of the file, folder, or registry key> <Local Windows Username> <Application Name> [Time Duration] [Policy Type]`	このコマンドは、Dell Secure Client にポリシーを追加するために使用します。このコマンドは、シン クライアントを再起動した後に有効になります。 `Path of the file, folder, or registry key` - Dell Secure Client が変更を監視するファイル、フォルダー、またはレジストリー キーです。入力されたパスは、UWF 除外リストで使用できる必要があります。 `Local Windows Username` - Dell Secure Client にアクセスを提供するリソースのユーザー名を入力します。 `Application Name` - リソースに対する変更が有効になるアプリケーション名を入力します。 `Time Duration` - 変更を有効にする時間の長さを入力します。このパラメーターはオプションです。値を入力しない場合は、いつでもポリシーを変更できます。 `Policy Type` - ポリシーのタイプを指定します。値はファイルまたはレジストリーのみです。このパラメーターはオプションです。 たとえば、`dscmgr /addpolicy C:\Users\Administrator\Test.txt Administrator C:\Windows\System32\notepad.exe 0900-1100` というコマンドを実行すると、午前 9 時から 11 時の間にメモ帳を使用して `C:\Users\Administrator\Test.txt` を変更することができます。 **メモ: このコマンドを使用するには、書き込みフィルターを無効にする必要があります。**
`dscmgr /removepolicy <Path of File or Folder or Registry Key> <Local Windows Username> <Application Name> [Time Duration]`	このコマンドは、Dell Secure Client からポリシーを削除するために使用します。このコマンドは、シン クライアントを再起動した後に有効になります。

コマンド ライン	説明
	`Path of the file, folder, or registry key` - Dell Secure Client が変更を監視するファイル、フォルダー、またはレジストリー キーです。入力されたパスは、UWF 除外リストで使用できる必要があります。 `Local Windows Username` - Dell Secure Client にアクセスを提供するリソースのユーザー名を入力します。 `Application Name` - リソースに対する変更が有効になるアプリケーション名を入力します。 `Time Duration` - 変更を有効にする時間の長さを入力します。このパラメーターはオプションです。値を入力しない場合は、いつでもポリシーを変更できます。 `Policy Type` - ポリシーのタイプを指定します。値はファイルまたはレジストリーのみです。このパラメーターはオプションです。 たとえば、`dscmgr /removepolicy C:\Users \Administrator\Test.txt Administrator C:\Windows\System32\notepad.exe 0900-1100` というコマンドを実行すると、午前 9 時から 11 時の間にメモ帳を使用して `C:\Users\Administrator\Test.txt` にアクセスすることができなくなります。 **メモ: このコマンドを使用するには、書き込みフィルターを無効にする必要があります。**
`dscmgr /enabledsc`	このコマンドは、Dell Secure Client を有効にするために使用します。このコマンドは、シン クライアントを再起動した後に有効になります。 **メモ: このコマンドを使用するには、書き込みフィルターを無効にする必要があります。**
`dscmgr /disabledsc`	このコマンドは、Dell Secure Client を無効にするために使用します。このコマンドは、シン クライアントを再起動した後に有効になります。 **メモ: このコマンドを使用するには、書き込みフィルターを無効にする必要があります。**
`dscmgr /exportpolicy <File Path>`	このコマンドは、Dell Secure Client からファイルにポリシーをエクスポートするために使用します。 `File Path` - ポリシーをエクスポートするファイルのパスを入力します。ファイル拡張子は.json または.csv である必要があります。ファイルが存在しない場合は、新しいファイルが作成されます。ファイルが存在する場合は、ファイルの内容が更新されます。 **メモ: このコマンドを使用するには、書き込みフィルターを無効にする必要があります。**
`dscmgr /importpolicy <File Path>`	このコマンドは、ファイルから Dell Secure Client にポリシーをインポートするために使用します。ファイルには、`/addpolicy` コマンドで言及された、有効なポリシーのセットが必要です。このコマンドは、シン クライアントを再起動した後に有効になります。 `File Path` - ポリシーをインポートするファイルのパスを入力します。ファイル拡張子は.json または.csv である必要があります。 **メモ: このコマンドを使用するには、書き込みフィルターを無効にする必要があります。**

コマンド ライン	説明
`dscmgr /exportinstallablepackage <Folder Path>`	このコマンドは、ポリシーを Dell Secure Client が使用する自己解凍式実行ファイルとしてエクスポートするために使用します。このファイルを使用すれば、複数のデバイスに同じポリシーを展開することができます。 `Folder Path` - ポリシーをエクスポートするファイルのパスを入力します。そのフォルダーに `DefaultDSCPolicy.exe` ファイルが作成されます。 **メモ: このコマンドを使用するには、書き込みフィルターを無効にする必要があります。**
`dscmgr /getdscstate`	このコマンドは、Dell Secure Client の現在の状態を表示するために使用します。Dell Secure Client が有効な場合は **1**、無効な場合は **0** が表示されます。

ログファイルの生成と表示

ログファイルには、Dell Secure Client のイベントのレコードがあります。このセクションでは、ログファイルを生成して表示する手順について説明します。

1. `C:\Program Files\Wyse\WyseLoggingLevel.ini` に移動します。
2. `[LoggingLevel] DSCSVC` パラメーターを 4 に更新します。
   別の Dell Secure Client のコンポーネントのログファイルは `C:\Wyse\WDA\DellSecureClient` で確認できます。

ヒントとベストプラクティス

このセクションでは、Dell Secure Client で効果的に作業するためのベスト プラクティスとヒントを紹介します。

- Dell Secure Client を有効にして設定する前に、UWF オーバーレイが RAM に設定されていることを確認してください。
- Dell Secure Client ユーザー インターフェイスを設定する前に、書き込みフィルターを無効にすることをお勧めします。
- 書き込みフィルターの除外リストを保護するため、Dell Secure Client を無効にしないことをお勧めします。
- ポリシーは、Dell Secure Client ユーザー インターフェイスの [**書き込みフィルター除外**] フィールドのそれぞれのフォルダーに表示されます。

エラーコード

表 3. エラーコード

エラーコード	説明
localInvalidFileError	Dell Secure Client 設定をエクスポートするための有効なファイルパスを選択します。
localExportFormatMsg	エクスポート形式を選択します。
cliPolicyExistsErrorMsg	ポリシーが存在します。
cliPolicyDoesntExist	ポリシーが存在しません。
cliInvalidPolicy	設定のポリシーが無効です。
cliIgnorePolicy	ポリシーを無視します。
cliInvalidFileExtension	無効なファイル拡張子が入力されました。
localEnterAppPath	アプリケーションパスを入力します。
localEditSuccess	編集に成功しました。
localFinishAddEditMsg	メッセージの追加または編集を完了します。
localExceptionInConfigMsg	設定ファイルのポリシーに無効な例外値があります。

エラーコード	説明
localWriteFilterEnabledWarning	Dell Secure Client の状態とポリシーを変更するには、書き込みフィルターを無効にする必要があります。
localInvalidData	インデックスに無効なデータが入力されました。
localAbortEditMsg	編集を中止します。
cliErrorDSCSate	Dell Secure Client の状態の問い合わせ中にエラーが発生しました。
localCorruptFileErrorMsg	設定ファイルが破損している可能性があります。次回の起動時にファイルが破損していた場合は、デフォルトのポリシーが適用されます。
cliPolicyLocationErrorMsg	UWF 除外リストにポリシーの場所が見つかりません。
cliInvalidCommandErrorMsg	無効なコマンドです。Dell Secure Client で使用可能なコマンドのリストを表示するには、`dscmgr help` と入力します。
cliInvalidCommand	無効なコマンドです
cliErrorConfigFileRead	設定ファイルの読み取り中にエラーが発生しました。
localAddPolicyErrorMsg	必須フィールドが入力されていないため、ポリシーを追加できません。

4

管理機能

管理者 は、管理者グループのメンバであるユーザー用に作成されたデフォルトのユーザープロファイルです。

管理者としてログインする方法については、「自動および手動ログオン」を参照してください。シンクライアントデバイスに管理者としてログインすると、コントロールパネル で特定の主要な拡張機能にアクセスできます。

コントロールパネル にアクセスするには、タスクバーで **スタートメニュー** > **コントロールパネル** の順にクリックします。

管理者として以下の機能を実行できます。

- 管理ツールの使用
- TPM と BitLocker の使用
- カスタムフィールドの使用
- RAM ディスクのサイズの設定
- 自動ログオンの有効化
- システムのショートカットの使い方
- SCCM コンポーネントの表示および設定
- デバイスの追加
- プリンタの追加
- デュアルモニターディスプレイの設定
- サウンド ダイアログボックスの使い方
- 地域と言語の設定
- ユーザーアカウントを使用したユーザーとグループの管理
- Windows Defender の使用
- Windows Defender Advanced Threat Protection (ATP) の使用
- Threat Defense
- Endpoint Security Suite Enterprise
- CAD ツールの使用
- Wyse Device Agent の設定
- Citrix HDX RealTime Media Engine の設定

管理ツールの使用

管理ツール ウィンドウにアクセスするには、**スタート** > **コントロールパネル** > **管理ツール** の順にクリックします。

管理ツールを使用して、次のタスクを実行できます。

- コンポーネントサービスの設定
- サービスの管理

コンポーネントサービスの設定

コンポーネントサービス、イベントビューアー、およびローカルサービスにアクセスして設定するには、**コンポーネントサービス** コンソールを使用します。

詳細については、https://support.microsoft.com の『*Windows 10 の管理ツール*』を参照してください。

イベントの表示

Windows やその他のプログラムからの監視およびトラブルシューティングのメッセージを表示するには、イベントビューアー ウィンドウを使用します。

コンポーネントサービス コンソールで、**コンソールルート** ツリーから **イベントビューアー** アイコンをクリックします。お使いのコンピュータで発生したイベントのすべてのログの概要が表示されます。詳細については、https://support.microsoft.com で『*イベント ビューアー*』を参照してください。

サービスの管理

シンクライアントデバイスにインストールされたサービスを表示および管理するには、**サービス** ウィンドウを使用します。**サービス** ウィンドウを開くには、**スタート** > **コントロール パネル** > **管理ツール サービス** の順に選択します。

1. **コンポーネント サービス** コンソールで、コンソール ツリーの **サービス** アイコンをクリックします。
   サービスのリストが表示されます。
2. 実行するサービスを選択して、右クリックします。開始、停止、一時停止、再開、再起動、の各操作を実行できます。
   ドロップダウン リストから、スタートアップの種類 を選択できます。
   - 自動 (遅延した開始)
   - 自動
   - 手動
   - 無効

   詳細については、https://support.microsoft.com の『*コンポーネント サービス管理*』を参照してください。

   メモ: サービスの管理中は書き込みフィルターが無効になっていることを確認します。

TPM と BitLocker の使用

信頼済みプラットフォーム モジュール (TPM) — 基本的なセキュリティ関連の機能を提供するマイクロチップで、主に暗号化キーを使用します。

BitLocker ドライブ暗号化 (BDE) — ボリューム全体を暗号化することでデータを保護する全ディスク暗号化機能です。デフォルトでは、128 ビット キーを持つ暗号ブロック連鎖 (CBC) モードで AES 暗号化アルゴリズムを使用します。このアルゴリズムは Elephant diffuser と組み合わされて、ディスク暗号化固有のセキュリティがさらに強化されます。

Windows 10 IoT Enterprise では、BitLocker 暗号化デバイスでの sysprep がサポートされません。この制限があるため、デバイスの暗号化、sysprep の実行、およびイメージのプルを行えません。この問題を解決するには、TPM スクリプトを追加または修正する必要があります。sysprep(プル)の実行前にデバイスは暗号化してはいけません。デバイスの暗号化は、`C:\Windows\setup\tools\` にある `TPM_enable.ps1` スクリプトを使用する POST プッシュスクリプトによって処理されます。この POST プッシュスクリプトは、sysprep スクリプトの後、UWF を有効にする前に入れる必要があります。クライアントの暗号化に使用される PIN は、引数としてスクリプトに渡される必要があります。

TPM と BitLocker を使用したフラッシュ メモリの暗号化

前提条件

フラッシュ メモリが以前に暗号化されている場合は、次の手順に沿って TPM をクリアします。

1. BIOS モードに入ります。
2. TPM 設定で、**TPM ステータスの変更** を **クリア** に設定してから、設定を適用します。
3. デバイスを再起動し、BIOS モードにもう一度入ります。
4. **TPM ステータスの変更** を **有効化とアクティブ化** に設定します。

TPM と BitLocker を使用してフラッシュ メモリを暗号化するには、次の手順に従います。

1. **BIOS** メニューから TPM を有効にします。
2. イメージング ソリューションに基づいて、スクリプトの TPM 関連部分を変更します。
3. 以下の行をコメント解除して、`C:\Windows\Setup\CustomSysprep\Modules\Post_CustomSysprep.psm1` の CustomFICore イメージング メソッドの TPM 暗号化の PIN を更新します。
   - `#cd C:\windows\setup\Tools\TPM\`
   - `#.\TPM_enable.ps1 -pin 1234`
4. 以下の行をコメント解除して、`C:\Windows\Setup\ConfigMgrSysprep\Modules\Admin_ConfigMgrSysprep.psm1` の SCCM プッシュの TPM 暗号化の PIN を更新します。
   - `#cd C:\windows\setup\Tools\TPM\`
   - `#.\TPM_enable.ps1 -pin 1234`
5. 以下の行をコメント解除して、`Post_CustomSysprep.psm1` の非工場出荷時環境 (WDM、WSI、USB イメージング ソリューション) の TPM 暗号化の PIN を更新します。
   - `#cd C:\windows\setup\Tools\TPM\`

- `#.\TPM_enable.ps1 -pin 1234`

Bluetooth 接続の設定

シンクライアントデバイスに Bluetooth 機能がある場合、他の Bluetooth 対応デバイスと共に使用することができます。

メモ: 設定を保持するには、統合書き込みフィルター (UWF) を無効にして、Application Launch Manager と xData Cleanup Manager を設定します。詳細については、「シンクライアントを設定する前に」を参照してください。

Bluetooth 接続を設定するには、https://support.microsoft.com の『*Bluetooth デバイスに接続する*』を参照してください。

ワイヤレスローカルエリアネットワークの設定

ワイヤレスローカルエリアネットワーク設定を構成するには、シンクライアントデバイスでワイヤレスサポートが許可されている場合は、**新しい接続またはネットワークのセットアップ** ウィンドウを使用します。

ワイヤレス ローカル エリア ネットワークの設定項目を設定するには、https://support.microsoft.com で、『*ワイヤレス ネットワークをセットアップする*』を参照してください。

カスタムフィールドの使用

Wyse Device Manager (WDM) および Wyse Management Suite (WMS) で使用するための設定文字列を入力するには、**カスタムフィールド** ダイアログボックスを使用します。設定文字列には、場所、ユーザー、管理者、その他の情報を含めることができます。

WDM および Wyse Management Suite サーバで使用できる情報を入力するには、次の手順を実行します。

1. 管理者 としてログインします。
2. **スタート** > **Dell Thin Client Application** の順に移動します。
   Dell Thin Client Application ウィンドウが表示されます。
3. 左のナビゲーションバーで、**カスタムフィールド** をクリックします。
4. カスタムフィールドのボックスにカスタムフィールド情報を入力し、**適用** をクリックします。

   カスタムフィールド情報は Windows レジストリに転送されて、WDM/WMS サーバで使用可能になります。

注意:

情報を永久的に保存するには、統合書き込みフィルター (UWF) を必ず無効 / 有効にしてください。詳細については、「シンクライアントを設定する前に」を参照してください。

メモ:

カスタムフィールド情報の詳細については、www.dell.com/support で WDM および WMS のドキュメントを参照してください。

RAM ディスクのサイズの設定

RAM ディスクは、一時的なデータの保存場所として使用される揮発性メモリです。管理者の判断で、RAM ディスクを他のデータの一時的な保存場所として使用することもできます。詳細については、「ファイルの保存とローカルドライブの使用」を参照してください。

RAM ディスクには、次の項目が保存されます。

- ブラウザの Web ページのキャッシュ
- ブラウザ履歴
- ブラウザの Cookie
- ブラウザのキャッシュ
- インターネット一時ファイル
- 印刷スプール
- ユーザーおよびシステムの一時ファイル

RAM ディスクのサイズを設定するには、次の操作を行います。

1. 管理者としてログインします。

2. **スタート** > **Dell シンクライアントアプリケーション** の順に移動します。
   Dell シンクライアントアプリケーション ウィンドウが表示されます。
3. 左のナビゲーションバーで、**RAM ディスク** をクリックします。
4. **RAM ディスクのサイズ** フィールドで、設定する RAM ディスクのサイズを入力または選択し、**適用** をクリックします。

   RAM ディスクのサイズを変更した場合、変更を有効にするにはシステムを再起動するよう求められます。

   メモ:

   情報を永久的に保存するには、統合書き込みフィルター (Unified Write Filter (UWF)) を無効にしてください。詳細については、「シンクライアントを設定する前に」を参照してください。

自動ログオンの有効化

ユーザーのデスクトップへの自動ログオンは、シンクライアントデバイス上ではデフォルトで有効に設定されています。自動ログオンを有効または無効にし、デフォルトのユーザー名、パスワード、ドメインを変更するには、自動ログオン機能を使用します。

自動ログオンを有効 / 無効にするには、次の操作を行います。

1. 管理者としてログインします。
2. **Start (スタート)** > **Dell Thin Client Application (Dell Thin Client アプリケーション)** の順に移動します。
   Dell Thin Client Application (Dell Thin Client アプリケーション) ウィンドウが表示されます。
3. 左のナビゲーションバーで、**Auto Logon** (自動ログオン) をクリックします。
4. 管理者ログオンページから開始するには、**Default User Nam** (デフォルトユーザー名) フィールドに `Admin` と入力します。

   メモ: デフォルトでは、Enable Auto Logon (自動ログオンを有効にする) チェックボックスが選択されます。

5. デフォルトの管理者、選択ユーザー、その他のアカウントで Logon (ログオン) ウィンドウから開始する場合は、**Enable Auto Logon** (自動ログオンを有効にする) チェックボックスをクリアします。

   注意: 情報を永久的に保存するには、統合書き込みフィルタ (UWF) を無効 / 有効にしてください。詳細については、「シンクライアントを設定する前に」を参照してください。

   メモ:

   自動ログインが有効になっていて、現在のデスクトップからログオフすると、ロック画面が表示されます。ロック画面上の任意の場所をクリックすると、Logon (ログオン) ウィンドウが表示されます。このウィンドウから、管理者またはユーザーアカウントにログインします。

システムのショートカット

システムのショートカット ページを使用すると、**スタート** メニューまたはコントロールパネルを介して移動することなく、一部のアプリケーション、ディレクトリ、ファイル、およびフォルダに直接にアクセスできます。

1. 管理者としてログインします。
2. **スタート** > **Dell シンクライアントアプリケーション** の順に移動します。
   Dell シンクライアントアプリケーション ウィンドウが表示されます。
3. 左のナビゲーションバーで、**システムのショートカット** をクリックします。
   システムのショートカット 領域には、次のショートカットが表示されます。
   - 管理ツール
   - すべてのコントロールパネル項目
   - システムディレクトリ
   - プログラムファイル
   - 一時フォルダ
   - マイドキュメント
   - 最近アクセスしたファイル
   - Dell シンクライアントアプリケーションフォルダ
   - アプリケーションデータフォルダ
4. フォルダ / ファイル / アプリケーションのそれぞれにアクセスするには、いずれかのショートカットをクリックします。

SCCM コンポーネントの表示および設定

シンクライアントデバイスにインストールされている SCCM コンポーネントを表示および設定するには、[**Configuration Manager のプロパティ**] ダイアログボックスを使用します。

Configuration Manager のプロパティ ダイアログボックスを開くには、次の手順を実行します。

1. 管理者としてログインします。
2. **[スタート]** > **[コントロール パネル]** > **[構成マネージャー]** の順に選択します。
   Configuration Manager のプロパティ ダイアログボックスが表示されます。

[**Configuration Manager のプロパティ**] ダイアログボックスの使用方法の詳細については、support.dell.com/manuals にある『*Managing Windows-based Dell Wyse Thin Clients using System Center Configuration Manager Administrator's Guide*』を参照してください。

System Center Configuration Manager Client LTSB 2016

Microsoft System Center Configuration Manager (SCCM) を使用すると、企業のコンプライアンスと制御を維持しながら、生産的である必要があるデバイスとアプリケーションを強化できます。Microsoft SCCM は、物理的、仮想、およびモバイルのクライアントを単体で管理できる統合インフラストラクチャによる企業のコンプライアンスと制御を達成しました。

これらのジョブの実行を簡単にするためのツールや改善策も提供しています。SP1 では、PC とモバイルデバイスを管理するための Windows Intune との統合が提供されます。クラウドおよびオンプレミスからの統合も、単一の管理コンソールからの統合も可能です。詳細については、support.dell.com/manuals の『*Managing Windows-based Dell Wyse Thin Clients using System Center Configuration Manager Administrator's Guide*』を参照してください。

デバイスとプリンタ

デバイスおよびプリンタを追加するには、Devices and Printers (デバイスとプリンター) ウィンドウを使用します。

注意: 設定をクリーンアップせずにおくには、Unified Write Filter (UWF) を無効 / 有効にして、Application Launch Manager と xData Cleanup Manager を設定します。詳細については、「シンクライアントを設定する前に」を参照してください。

シンクライアントにデバイスまたはプリンタを追加するには、次の手順を実行します。

1. 管理者としてログインします。
2. **Start (スタート)** > **Control Panel (コントロールパネル)** > **Devices and Printers (デバイスとプリンター)** の順に選択します。
   Devices and Printers (デバイスとプリンター) ウィンドウが表示されます。

プリンタの追加

シンクライアントにプリンタを追加するには、次の手順を実行します。

1. コントロールパネルの **Devices and Printers** (デバイスとプリンター) アイコンをクリックします。
   Devices and Printers (デバイスとプリンター) ウィンドウが表示されます。
2. **Add a Printer** (プリンタの追加) ウィザードを開いて使用するには、**Add a Printer** (プリンタの追加) をクリックします。

   Add a Printer (プリンタの追加) ウィザードのセッションが開始します。

   Dell Open Print Driver は、他の内蔵プリントドライバと一緒にシンクライアントにインストールされています。すべてのテキストおよび画像をローカルプリンタに印刷するには、製造元が提供するドライバを説明書の手順に沿ってインストールします。

   Citrix Receiver、リモートデスクトップ接続 または **VMware Horizon Client** アプリケーションからネットワークプリンタへの印刷は、サーバ上のプリンタドライバを使用して実現されます。

   サーバのプリンタドライバを使用した、**Citrix Receiver、リモートデスクトップ接続** または **VMware Horizon Client** アプリケーションからローカルプリンタへの印刷により、プリンタからすべてのテキストおよび画像の機能が使用可能になります。次の手順を使用して、サーバにプリンタドライバを、シンクライアントにテキスト専用ドライバをインストールします。

   a) **Add a local printer** (ローカルプリンタを追加します) をクリックして、**Next** (次へ) をクリックします。
   b) **Use an existing port** (既存のポートを使用) をクリックし、リストからポートを選択して **Next** (次へ) をクリックします。
   c) プリンタのメーカーとモデルを選択して **Next** (次へ) をクリックします。
   d) プリンタの名前を入力して **Next** (次へ) をクリックします。

e) **Do not share this printer**（このプリンタを共有しない）を選択して **Next**（次へ）をクリックします。
f) テストページを印刷するかどうかを選択して **Next**（次へ）をクリックします。
g) **Finish**（完了）をクリックしてインストール作業を終了します。

このオプションを選択した場合は、インストール後にテストページが印刷されます。

デバイスの追加

シンクライアントにデバイスを追加するには、次の手順を実行します。

1. コントロールパネルの **デバイスとプリンター** アイコンをクリックして、**デバイスとプリンター** ウィンドウを開きます。
2. **デバイスの追加** ウィザードを開いて使用するには、**デバイスの追加** をクリックします。
   デバイスの追加 ウィザードのセッションが開始します。ウィザードを使用して、シンクライアントに任意のデバイスを追加することができます。

マルチモニターディスプレイの設定

画面の解像度 ウィンドウを使用して、デュアルモニター対応のシンクライアントデバイスでデュアルモニターの設定を行えます。

画面の解像度 ウィンドウを開くには、次の手順を実行します。

1. 管理者としてログインします。
2. **スタート** > **コントロールパネル** > **ディスプレイ** > **ディスプレイの設定の変更** の順に選択します。
   画面の解像度 ウィンドウが表示されます。画面解像度の設定方法の詳細については、www.microsoft.com を参照してください。

   マルチモニターのセットアップ方法の詳細については、support.dell.com から「*Windows 10 でマルチモニターをセットアップする方法*」を参照してください。

オーディオおよびオーディオデバイスの管理

オーディオおよびオーディオデバイスを管理するには、**サウンド** ダイアログボックスを使用します。

オーディオおよびオーディオデバイスを管理するには、管理者としてログインして **サウンド** ダイアログボックスを開きます。

サウンド ダイアログボックスの使い方

オーディオデバイスを管理するには、**サウンド** ダイアログボックスを使用します。

サウンド ダイアログボックスを開くには、次の手順を実行します。

1. **スタート** > **コントロールパネル** > **サウンド** の順に選択します。

   サウンド ダイアログボックスが表示されます。
2. 以下のタブを使用して、サウンド関連の設定を行います。
   - **再生** — 再生デバイスを選択してその設定を変更します。
   - **録音** — 録音デバイスを選択してその設定を変更します。
   - **サウンド** — Windows またはプログラムのイベント用に、既存または変更したサウンドテーマを選択します。
   - **通信** — シンクライアントを使用して通話を発信または受信しているときに、各種のサウンドの音量を調整するオプションをクリックします。
3. **適用**、**OK** の順にクリックします。

メモ:

- **パワード スピーカーを使用することをお勧めします。**
- **タスクバーの通知領域の 音量 アイコンを使用して音量を調節することもできます。**

地域の設定

キーボードと Windows の表示言語を含む地域フォーマットを選択するには、**地域** ダイアログボックスを使用します。

地域の形式を選択するには、次の手順を実行します。

1. 管理者としてログインします。

2. **スタート** > **コントロール パネル** > **地域** の順に選択します。
   地域 ダイアログボックスが表示されます。
3. **形式** タブで、言語、日付と時刻の形式を設定します。
   形式をカスタマイズするには、以下の手順を実行します。
   a) **追加の設定** をクリックします。
      形式のカスタマイズ ウィンドウが表示されます。
   b) 設定をカスタマイズして、**OK** をクリックします。
4. **適用**、**OK** の順にクリックします。
5. **場所** タブで、特定の場所を選択して、ニュースや天気などの追加情報を表示します。
6. **管理** タブで、Unicode をサポートしていないプログラムで表示されるよう言語を変更し、その設定をコピーします。

ユーザーアカウントの管理

ユーザーおよびグループを管理するには、**ユーザーアカウント** ウィンドウを使用します。

ユーザーアカウント ウィンドウを開くには、次の手順を実行します。

1. 管理者としてログインします。
2. **スタート** > **コントロール パネル** > **ユーザーアカウント** の順に選択します。

   ユーザーアカウント ウィンドウの使用方法については、「ユーザーアカウントを使用したユーザーとグループの管理」を参照してください。

Windows Defender の使用

お使いのコンピュータをスキャンして、スパイウェアやマルウェアから保護するには、**Windows Defender** ダイアログボックスを使用します。

Windows Defender ウィンドウを開くには、次の手順を実行します。

1. 管理者としてログインします。
2. **スタート** > **コントロール パネル** > **Windows Defender** の順に選択します。

   Windows Defender ウィンドウが表示されます。**ホーム** タブで、スキャンオプションを選択して **今すぐスキャン** をクリックします。

シンクライアントデバイスを設定および管理するには、**設定** タブでマルウェア対策ソフトウェアの設定を使用できます。

Windows Defender は、Windows に含まれているスパイウェア対策ソフトウェアで、シンクライアントの電源投入時に自動的に実行されます。スパイウェア対策ソフトウェアを使用すると、スパイウェアやその他の潜在的に望ましくないソフトウェアからデバイスを保護するのに役立ちます。スパイウェアは、インターネットへの接続時にはいつでも、ユーザーに気づかれないままデバイスにインストールされる可能性があります。CD、DVD、またはその他のリムーバブルメディアを使用していくつかのプログラムをインストールすると、お使いのコンピュータにスパイウェアが感染するおそれがあります。スパイウェアも、インストール時だけではなく予期しない時間に実行するようにプログラムされている可能性があります。

メモ: Windows Defender は毎月第 2 日曜日の午前 1:00 に自動的に更新されます。

Windows Defender Advanced Threat Protection

Windows Defender Advanced Threat Protection (ATP) は、企業がネットワーク上の高度な攻撃を検出、調査し、その攻撃に対応することを支援する新しいサービスです。

Windows Defender ATP は、Windows Defender、AppLocker、および Device Guard など、エンドポイント上にある既存の Windows セキュリティテクノロジと共に動作します。また、Windows Defender ATP は、サードパーティのセキュリティソリューションやアンチマルウェア製品と協調して動作します。詳細については、docs.microsoft.com の『*Windows Defender Advanced Threat Protection*』マニュアルを参照してください。

Threat Defense

Dell Data Protection | Threat Defense Agent (Cylance 提供) は、マルウェアがコンピュータに影響を与える前に検出してブロックします。Cylance は、マルウェアの識別に数学的アプローチを使用しています。これは、事後対応型のシグニチャ、信頼ベースのシステム、サンドボックスではなく、機械学習手法を使用しています。Dell Data Protection | Threat Defense は、オペレーティングシステム内のマルウェアの可能性のあるファイルの実行形式を分析します。

Endpoint Security Suite Enterprise

Dell Endpoint Security Suite Enterprise バージョン 10.1 の Advanced Threat Prevention の要素がサポートされています。この機能は Wyse 5070 Thin Client、Wyse 5470 Thin Client、Wyse 5470 All-in-One Thin Client でのみサポートされています。

Endpoint Security Suite Enterprise は、ビジネスデータ、システム、および評価に対してデータセキュリティを提供します。このスイートでは、高度な脅威防御、エンタープライズクラスの暗号化、すべての集中管理を単一のコンソールで実行できる統合クライアントが提供されます。統合されたコンプライアンスレポートと柔軟な電子メール通知を使用して、すべてのエンドポイントのコンプライアンスを簡単に実施、証明することができます。

C-A-D ツール

C-A-D ツールを使用すると、管理者は VDI アプリケーションの Ctrl+Alt+Del キーの組み合わせを、VDI アプリケーションの Ctrl+Alt+Del 画面を表示するようにマッピングできます。C-A-D ツールが有効になっている場合、すべての VDI アプリケーションに Ctrl+Alt+Del キーの組み合わせを使用できます。また、リモートセッション (リモートデスクトップ、Citrix、VMware の各セッションなど) では、Win+L や Ctrl+Alt+Delete キー機能も使用できます。

以下に、C-A-D ツールでサポートされる各種の VDI アプリケーションにマップされているキーを示します。

- Citrix - Ctrl+F1
- RDP - Ctrl+Alt+End
- VMware - Ctrl+Alt+Insert

メモ: C-A-D ツールは、Citrix セッションで Citrix Virtual Apps and Desktops (旧 Citrix XenDesktop) に対しては機能しませんが、Citrix 仮想アプリでのみ機能します。

C-A-D ツールは、デフォルトでは無効に設定されています。

Wyse Device Agent

Wyse Device Agent (WDA) は、すべてのシンクライアント管理ソリューション向けの統合エージェントです。WDA をシンクライアントにインストールすると、Dell Wyse Device Manager (WDM)、および Dell Wyse Management Suite (WMS) によって管理可能になります。詳細については、support.dell.com/manuals の『*Dell Wyse Device Agent Release Notes*』(Dell Wyse Device Agent リリースノート) を参照してください。

メモ: Wyse Device Manager を使用して、Wyse 5070 Thin Client、Wyse 5470 Thin Client、Wyse 5470 All-in-One Thin Client を管理することはできません。

Citrix HDX RealTime Media Engine

Microsoft Lync 用の **Citrix HDX RealTime Optimization Pack** は拡張性に優れたソリューションを提供します。XenDesktop および XenApp 環境で Microsoft Lync を経由して、Linux、Mac および Windows デバイスのユーザーにリアルタイムのオーディオ / ビデオ会議機能と VoIP エンタープライズテレフォニーを提供します。HDX RealTime Optimization Pack は、既存の Microsoft Lync インフラストラクチャを適用し、デバイスでネイティブに実行されている他の Microsoft Lync エンドポイントと相互運用できます。

詳細については、Citrix のマニュアルを参照してください。

オペレーティングシステムイメージのマニフェストファイルの表示およびエクスポート

マニフェストファイルは、オペレーティングシステムイメージに関するメタデータを含む XML ドキュメントです。現在および工場出荷時のマニフェストファイルを比較すると、シンクライアントでの変更を見つけることができます。次の 2 つのタイプのマニフェストファイルは、データコレクションのソースに基づいています。

表 4. マニフェストファイル

マニフェストのソース	インストール済み製品	QFE	ドライバ
現在のマニフェスト	はい	はい	はい
工場出荷時のマニフェスト	はい	はい	はい

現在および工場出荷時のマニフェストファイルでインストール済み製品、QFE、およびドライバの詳細を比較して、インストール済みアプリケーション、QFE、およびドライバそれぞれに関して、シンクライアントでの変更を見つけることができます。

メモ: **インストール済み製品は、シンクライアントにインストールされているすべてのアプリケーションを示しています。**

オペレーティングシステムイメージの現在のマニフェスト情報の表示とエクスポート

1. 管理者としてログインします。
2. **スタート** > **コントロールパネル** > **Dell Wyse Software Manifest Utility** の順に選択します。
3. **サポートデータのエクスポート** をクリックします。
   データは、デフォルトのパス C:/Users/Public/Public Documents/Wyse にエクスポートされます。

   メモ:

   カスタムパス を選択したり必要なフォルダを参照したりして、カスタムフォルダにデータをエクスポートすることもできます。
4. **サポートディレクトリ** をクリックします。
   DellTCASupportInfo フォルダが表示されます。

   サポートディレクトリには、シンクライアントの現在のマニフェスト情報のアプリケーション、ドライバ、および QFE が含まれています。

オペレーティングシステムイメージの工場出荷時のマニフェスト情報の表示

1. 管理者としてログインします。
2. C:\Windows\Setup\Tools に移動します。
   BuildContent フォルダには、シンクライアントの工場出荷時のマニフェストが含まれています。
3. オペレーティングシステムイメージのマニフェストの情報を表示します。
   - 出荷時に工場でインストールされた製品の情報を表示するには、**アプリ** > **InstalledProducts xml ファイル** に移動します。
   - 出荷時に工場でインストールされた QFE の情報を表示するには、**Qfe** > **QFE xml ファイル** に移動します。
   - 現在インストールされているドライバのマニフェスト情報を表示するには、**ドライバ** > **Drivers xml ファイル** に移動します。

メモ:

- **Dell Wyse Software Manifest Utility によって生成された InstalledProducts、QFE、および Drivers の .xml ファイル (現在のマニフェスト情報設定) と、<drive C>\Windows\Setup\Tools\BuildContent フォルダにある .xml ファイル (工場出荷時のマニフェスト情報設定) を比較して、インストール済みのアプリケーションと QFE に関する変更を見つけることができます。**
- **サポートデータ と ビルドコンテンツ データは、トラブルシューティングの際にサポートチームと共有できます。**

Dell ドッキング ステーション WD19

Dell ドッキング ステーション WD19 は、USB Type-C ケーブル インターフェイスで、すべての電子デバイスをシン クライアントにリンクするデバイスです。シン クライアントをドッキングステーションに接続すると、コンピューターに接続しなくても、すべての周辺機器 (マウス、キーボード、ステレオスピーカー、外付けハード ドライブ、大画面ディスプレイ) にアクセスできます。

Wyse 5470 Thin Client は、Dell ドッキング ステーション WD19 をサポートします。

詳細については、support.dell.com/manuals にある『*Dell ドッキング ステーション WD19 ユーザーズ ガイド*』および『*Microsoft Windows 10 IoT Enterprise for Dell Wyse 5470 Thin Client Release Notes*』を参照してください。

5

追加の管理者ユーティリティおよび設定情報

ここでは、管理者が利用できるユーティリティおよび設定についての追加情報を提供します。

- 自動的に起動するユーティリティ
- ログオフ、再起動、およびシャットダウンによる影響を受けるユーティリティ
- 統合書き込みフィルターの使用
- Application Launch Manager の使用
- xData Cleanup Manager の使用
- ファイルの保存およびローカルドライブの使用
- ネットワークドライブのマッピング
- ドメインへの参加
- Net および Tracert ユーティリティの使用
- ユーザーアカウントを使用したユーザーとグループの管理
- シンクライアントのコンピュータ名の変更

自動的に起動するユーティリティ

次のユーティリティは、システムの電源を入れるか、シンクライアントにログインすると、自動的に起動します。

- **統合書き込みフィルター** — システムに電源を入れると、統合書き込みフィルターユーティリティが自動的に起動します。タスクバーの通知領域にあるアイコンによって、統合書き込みフィルターのステータス（アクティブまたは非アクティブ）が示されます。詳細については、「統合書き込みフィルター（UWF）の使用」を参照してください。

  メモ: Dell Wyse 書き込みフィルターのアイコンおよび機能は現在サポートされていますが、Microsoft のマニュアル（www.microsoft.com を開いて統合書き込みフィルターのマニュアルに移動）に記載されているように、UWF を使用することをお勧めします。

- **Application Launch Manager** — Application Launch Manager（ALM）バージョン 1.0 を使用すると、サービスの起動、ユーザーのログオフ、またはセッションゼロのシステムのシャットダウンなどの事前定義されたイベントに基づいて、アプリケーションを起動できます。また、このようなアプリケーションを使用して、簡単なトラブルシューティングに必要なマルチレベルログを設定することもできます。
- **xData Cleanup Manager** — xData Cleanup Manager（xDCM）バージョン 1.0 は、無関係な情報がローカルディスクに保存されないようにします。xDCM を使用すると、情報の一時的なキャッシュに使用されるディレクトリを自動的にクリーンアップできます。クリーンアップは、サービスのスタートアップ、ユーザーのログオフ、またはシステムシャットダウンのいずれかによってトリガされます。クリーンアップはユーザーの目に見えず、完全に設定可能です。
- **VNC サーバ** — シンクライアントにログインすると、Windows VNC サーバユーティリティが自動的に起動します。VNC によって、シンクライアントデスクトップにリモートからアクセスして管理やサポートを行えます。詳細については、「TightVNC を使用したシンクライアントのシャドーイング」を参照してください。

ログオフ、再起動、およびシャットダウンによる影響を受けるユーティリティ

次のユーティリティは、シンクライアントデバイスのログオフ、再開、およびシャットダウンにより影響を受けます。

- **統合書き込みフィルター** — システムに電源を入れると、統合書き込みフィルターユーティリティが自動的に起動します。Microsoft のドキュメントに記載されているように、UWF を使用することをお勧めします。詳細については、www.microsoft.com を開いて、統合書き込みフィルターのマニュアルを参照してください。
- **Application Launch Manager** — Application Launch Manager（ALM）バージョン 1.0 を使用すると、サービスの起動、ユーザーのログオフ、またはセッションゼロのシステムのシャットダウンなどの事前定義されたイベントに基づいて、アプリケーションを起動できます。また、このようなアプリケーションを使用して、簡単なトラブルシューティングに必要なマルチレベルログを設定することもできます。
- **xData Cleanup Manager** — xData Cleanup Manager（xDCM）バージョン 1.0 は、無関係な情報がローカルディスクに保存されないようにします。xDCM を使用すると、情報の一時的なキャッシュに使用されるディレクトリを自動的にクリーンアップできま

す。クリーンアップは、サービスのスタートアップ、ユーザーのログオフ、またはシステムシャットダウンのいずれかによってトリガされます。クリーンアップはユーザーの目に見えず、完全に設定可能です。

- **電源管理** — モニターセーバーはモニターへのビデオ信号を切断し、指定したアイドル時間の経過後にモニターを省電力モードにすることができます。電源設定にアクセスするには、**[スタート]** > **[コントロール パネル]** > **[電源オプション]** の順に選択します。
- **Wake-on-LAN** — この機能では、使用している LAN に接続されているすべてのシンクライアントを検出し、ボタンをクリックするだけで起動できるようにします。たとえば、シャットダウンされた、またはスタンバイ状態のデバイスでイメージのアップデートおよびリモート管理機能を実行できます。この機能を使用するには、シンクライアントの電源が入っている必要があります。

統合書き込みフィルター

統合書き込みフィルター (UWF) は、ストレージメディアを保護するセクタベースの書き込みフィルターです。UWF は、書き込み試行を仮想オーバーレイにリダイレクトし、保護されたボリュームへの書き込み試行を中断します。これによってデバイスの安定性と信頼性が向上し、それによってソリッドステートドライブのような書き込みメディアの損耗が低減されます。UWF では、オーバーレイは、保護対象ボリュームに対する変更を保存する仮想ストレージ領域です。ファイルシステムが保護対象セクタを変更しようとする場合は、UWF が保護対象ボリュームのセクタをオーバーレイにコピーし、そのオーバーレイが変更されます。アプリケーションがそのセクタから読み取ろうとする場合、UWF はオーバーレイからデータを返します。システムからはボリュームに書き込んだように見えますが、ボリュームは変更されていません。詳細については、www.microsoft.com で統合書き込みフィルターのマニュアルを参照してください。

注意: 書き込みフィルターをオンにした状態で保持できない場合(定期的なメンテナンスやアプリケーション / ドライバのインストールまたはアップグレードを除く)、フラッシュ / SSD ストレージが早期に摩耗し、保証が無効になります。

次に、UWF によってフィルタリングから除外されているデフォルトのファイルフォルダを示します。

- C:\Users\Admin\AppData\LocalLow
- C:\Users\User\AppData\LocalLow
- C:\Program Files\Windows Defender
- C:\Program Files (x86)\Windows Defender
- C:\Windows\WindowsUpdate.log
- C:\Windows\Temp\MpCmdRun.log
- C:\Windows\system32\spp
- C:\ProgramData\Microsoft\Windows Defender
- C:\program files\Wyse\WDA\Config
- C:\Users\Public\Documents\Wyse
- C:\Wyse\WCM\ConfigMgmt
- C:\Wyse\WCM
- C:\Wyse\WDA

次に、UWF によってフィルタリングから除外されているデフォルトのレジストリを示します。

- HKLM\SYSTEM\CurrentControlSet\Control\WNT\DWCADTool
- HKLM\Software\Wyse\ConfigMgmt
- HKLM\SOFTWARE\Microsoft\Windows Defender
- HKLM\SYSTEM\CurrentControlSet\Control\WNT\UWFSvc
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\HomeGroup
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList
- HKLM\SYSTEM\WPA

注意: 常に適切な書き込みフィルターを使用し、Windows ページファイルの使用方法の指示に従ってください。当該の指示にはたとえば、通常の使用時には必ず書き込みフィルターを有効にしておき、イメージのアップグレード、セキュリティパッチの適用、レジストリの変更、アプリケーションのインストールが必要な場合にのみ、管理者が一時的にフィルターを無効にする、などの指示が含まれています。こうしたタスクが完了したら直ちに、書き込みフィルターを再度有効にする必要があります。その他の指示としては、シンクライアントの通常使用時は、Windows ページファイル機能を決して有効にしないことなどの指示があります。通常の使用時に書き込みフィルタをオフにしたり、Windows ページファイルを有効にしたりして、Dell Wyse Windows Embedded Thin Client の操作を行うと、フラッシュ/SSD ストレージの消耗が早まり、パフォーマンスが低下して、製品の寿命が縮まります。デルは、これらの指示に従わなかったために適切に動作しなくなった、いかなるシンクライアントデバイスまたはコンポーネントに対しても、保証、サポート、修理、または交換の責任を負いません。

統合書き込みフィルターの使用

UWF を使用するようにシンクライアントデバイスを設定するには、次の手順を実行します。

1. 管理者としてログインします。
   ユーザーのデスクトップへの自動ログオンが有効になっている場合は、ユーザーのデスクトップからログオフして、管理者としてログインします。
2. 統合書き込みフィルターを無効にするには、デスクトップの **Dell Wyse WF 無効** アイコンをダブルクリックします。
   このアイコンは、フィルターを無効にしてシステムを再起動します。
3. シンクライアントデバイスを必要に応じて設定します。
4. シンクライアントデバイスの設定後、統合書き込みフィルタを有効にするには、デスクトップの **Dell Wyse WF 有効** アイコンをダブルクリックします。
   このアイコンは、フィルターを有効にしてシステムを再起動します。これで、シンクライアントデバイスに対する設定が保存され、シンクライアントの再起動後も維持されます。

システムが起動すると、統合書き込みフィルター (UWF) ユーティリティが自動的に起動します。

保護されているボリューム上の特定のファイルまたはフォルダをファイル除外リストに追加して、これらのファイルおよびフォルダが UWF によってフィルタリングされないようにすることができます。ファイルまたはフォルダがボリュームの除外リストにある場合、そのファイルやフォルダへのすべての書き込みが UWF フィルタリングをバイパスし、保護されたボリュームに直接書き込まれ、デバイスの再起動後も維持されます。

実行時にファイルまたはフォルダの除外を追加または削除するには、管理者としてログインする必要があります。また、新しい除外が有効になるようにデバイスを再起動する必要があります。

統合書き込みフィルターのコマンドラインオプションの実行

統合書き込みフィルターの制御に使用できる、複数のコマンド行があります。コマンドラインの引数は組み合わせることはできません。

統合書き込みフィルターのコマンドラインオプションについては、次のガイドラインを使用します。また、**実行** ボックスにコマンドを入力して昇格した権限で コマンドプロンプト ウィンドウを開いた場合にもコマンドを使用できます。

表 5. 統合書き込みフィルターのコマンドラインオプションの実行

コマンドラインオプション	説明
`uwfmgr`	このコマンドラインツールは、統合書き込みフィルター (UWF) の設定を構成および取得します。使用できるコマンドラインオプションがない場合は、コマンドヘルプが表示されます。
`uwfmgr filter enable`	このコマンドラインは、次回のシステム再起動後に、統合書き込みフィルターを有効にします。統合書き込みフィルターが有効な場合、統合書き込みフィルターステータス アイコンは緑です。
`uwfmgr filter disable`	このコマンドラインオプションは、次回のシステム再起動後に、統合書き込みフィルターを無効にします。無効になっている間は、統合書き込みフィルターステータス アイコンは赤のままです。
`uwfmgr file commit C: <ファイルパス>`	このコマンドラインは、統合書き込みフィルターで保護されているボリュームに対してオーバーレイ対象として指定したファイルへの変更をコミットします。このコマンドを使用するには、管理者レベルの許可が必要です。 <file> パラメータは、ボリュームとパスを含む完全修飾名である必要があります。`uwfmgr.exe` は、<file> パラメータに指定されたボリュームを使用して、そのファイルに対するファイル除外リストを含むボリュームを特定します。ボリューム名とファイルパスの間には単一スペースを入れます。たとえば、ファイル `C:\Program Files\temp.txt` をコミットする場合、コマンドは `uwfmgr commit C: \Program Files\temp.txt` となります。

コマンドラインオプション	説明
uwfmgr file add-exclusion C: <ファイルまたはディレクトリへのパス>	このコマンドラインは、指定したファイルを、統合書き込みフィルターで保護されているボリュームのファイル除外リストに追加します。統合書き込みフィルターは、次回のシステム再起動後に、フィルタリング対象からのファイルの除外を開始します。 たとえば、レジストリのディレクトリ HKLM\SYSTEM\WPA を追加する場合、コマンドは UWFmgr.exe registry add-exclusion HKLM\SYSTEM\WPA となります。
uwfmgr file remove-exclusion C: <ファイルまたはディレクトリのパス>	このコマンドラインは、指定したファイルを、統合書き込みフィルターで保護されているボリュームのファイル除外リストから削除します。統合書き込みフィルターは、次回のシステム再起動後に、フィルタリング対象からのファイルの除外を停止します。
uwfmgr overlay get-config	このコマンドラインは、統合書き込みフィルターのオーバーレイの構成設定を表示します。現在および次の両方のセッションに関する情報を表示します。
uwfmgr registry /?	このコマンドラインは、レジストリキーの除外のための構成設定を表示します。

メモ: コマンドプロンプト ウィンドウを開いて uwfmgr ? または uwfmgr help と入力すると、使用可能なすべてのコマンドが表示されます。コマンドの詳細については、uwfmgr help <command> を使用してください。たとえば、コマンド volume の詳細を表示するには、uwfmgr help volume のように入力します。

注意:

- **管理者はファイルセキュリティを使用して、これらのコマンドの望ましくない使用を防ぐ必要があります。**
- **別のフラッシュ動作の進行中は、ディスクにデータをフラッシュしないでください。**

デスクトップアイコンを使用した書き込みフィルターの有効化と無効化

統合書き込みフィルターを有効または無効にするには、書き込みフィルターの有効化 / 無効化 デスクトップアイコンも使用できます。タスクバーのタスクトレイにあるアイコンの色により、統合書き込みフィルターのアクティブ (緑) または非アクティブ (赤) のステータスが示されます。

- **Dell Wyse WF 有効 アイコン (緑)** - このアイコンをダブルクリックすると、統合書き込みフィルターが有効になります。このユーティリティは、uwfmgr のフィルター有効化のコマンドラインと同様の動作をします。ただし、このアイコンをダブルクリックすると、システムはすぐに再起動され、統合書き込みフィルターが有効になります。統合書き込みフィルターが有効な場合、タスクバーのタスクトレイの統合書き込みフィルターのステータスアイコンは緑です。
- **Dell Wyse WF 無効 アイコン (赤)** - このアイコンをダブルクリックすると、統合書き込みフィルターが無効になります。このユーティリティは、uwfmgr のフィルター無効化のコマンドラインオプションと同様の動作をします。ただし、このアイコンをダブルクリックすると、すぐにシステムが再起動します。統合書き込みフィルターが無効の場合、タスクバーの通知領域の統合書き込みフィルターのステータスアイコンは赤です。

書き込みフィルターコントロールの設定

UWF コントロールの設定を表示および管理するには、**統合書き込みフィルターコントロール** ダイアログボックスを使用します。ダイアログボックスを開くには、管理者タスクバーのタスクトレイにある UWF アイコンをダブルクリックします。

UWF コントロール設定時には、一部のフィールドが使用不可になっています。設定中に使用可能なフィールドのリストから選択することができます。

Dell Wyse 統合書き込みフィルターコントロール ダイアログボックスには以下が含まれます。

- **UWF ステータス**
  - **現在のステータス** - 統合書き込みフィルターのステータスを示します。ステータスは、有効または無効のいずれかです。

- **起動コマンド** - 起動コマンドのステータスを示します。UWF_ENABLE は UWF が次のセッションでは有効になっていることを意味し、UWF_DISABLE は次のセッションでは UWF が無効になっていることを意味します。
- **UWF によって使用される RAM** - メガバイト (MB) と割合で、統合書き込みフィルターに割り当てられている RAM の量を示します。**現在のステータス** が無効になっている場合、UWF に割り当てられる RAM は常にゼロ (0) です。
- **UWF キャッシュに使用される RAM の量** - 現在のセッションで統合書き込みフィルターキャッシュに割り当てられている RAM の量をメガバイト (MB) で示します。
- **警告 #1(%)** - 現在のセッションでメモリ不足警告メッセージがユーザーに表示される UWF キャッシュの割合値を示しています。
- **警告 #2 (%)** - 重要なメモリの警告メッセージがユーザーに表示される UWF キャッシュの割合値を示しています。

- **UWF キャッシュ設定**
  - **UWF キャッシュに使用される RAM の量** - 次のセッションで統合書き込みフィルターキャッシュとして使用される RAM の量を MB で示します。この値は 256 MB ~ 2048 MB の範囲内である必要があります。この値が使用可能な RAM の 50 % を超えていないことを、必要以上に確認されます。
- **UWF 警告設定**
  - **警告 #1(%)** - メモリ不足警告メッセージがユーザーに表示される UWF キャッシュの割合値を示しています (デフォルト値 = 80、最小値 = 50、最大値 = 80)。
  - **警告 #2 (%)** - 重要なメモリの警告メッセージがユーザーに表示される UWF キャッシュの割合値を示しています。メモリのレベルが警告レベル 2 を超えると、システムが自動的に再起動します (デフォルト値 = 90、最小値 = 55、最大値 = 90)。
- **UWF を有効にする** — 統合書き込みフィルターを有効にできます。シンクライアントデバイスを再起動するように要求されます。変更を保存するには、シンクライアントを再起動します。統合書き込みフィルターを有効にするためにシステムが再起動した後、デスクトップの統合書き込みフィルターのステータスアイコンが緑色に変わります。
- **UWF を無効にする** — 統合書き込みフィルターを無効にできます。シンクライアントデバイスを再起動するように要求されます。変更を保存するには、シンクライアントを再起動します。統合書き込みフィルターを無効にした後は、デスクトップのタスクトレイの統合書き込みフィルターのステータスアイコンが赤色に変わり、統合書き込みフィルターはシステムの再起動後も無効のままとなります。
- **デフォルト** - UWF キャッシュ設定 領域、および UWF 警告設定 領域をリセットしてデフォルト値に設定します。
- **ファイルコミット 領域**
  - **ファイルパス** - 基盤となるメディアに対してファイルの追加、削除およびコミットを行えます。システムはシンクライアントデバイスを再起動しません。変更はただちにコミットされます。

    メモ: ファイルがコミットされていない場合は、リストからファイルパスを削除します。
- **現在のセッションの除外リスト**
  - **ファイル / ディレクトリパス** -

    次のセッションに対する、除外リストへのファイルやフォルダの追加と削除が行えます。現在のセッションの除外リスト と表示されているペインに列挙されているファイルやディレクトリは、現在のセッションでの更新内容が維持されます。次のセッションの除外リスト と表示されるペインに列挙されるファイルやディレクトリは、次のセッションにて更新された内容が維持される対象です。システムはシンクライアントを再起動せず、管理者がシンクライアントデバイスを手動で再起動するまで変更はコミットされません。

Application Launch Manager

Application Launch Manager (ALM) バージョン 1.0 を使用すると、サービスの起動、ユーザーのログイン / ログオフ、システムのシャットダウンなどシステムアカウントで事前定義されたイベントに基づいて、アプリケーションを起動できます。また、`DebugLog.xml` ファイルを使用して、トラブルシューティングに必要なマルチレベルログを設定することもできます。

また、コマンドラインインターフェイスを使用して、ALM 構成ファイルにアプリケーション構成ノードを追加または削除することもできます。

ALM CLI ツール

ALM CLI ツールを使用して、ALM 設定ファイル `ApplicationLaunchConfig.xml` のアプリケーション設定ノードを追加または削除できます。このツールは、ALM アプリケーションのインストールパスにあります。デフォルトでは、このツールは `%Systemdrive%\Program Files\ALM` にあります。

ALM を使用したノードの構成

次のオプションとパラメータを使用して、`ApplicationLaunchConfig.xml` でアプリケーションノードを構成できます。

表 6. ノードを構成するためのオプション

オプション	説明
Add -Application	アプリケーションノードを追加するオプション。
Remove -Application	アプリケーションノードを削除するオプション。

表 7. ノードを構成するためのパラメータ

パラメータ	Values
Name:<アプリケーション名>	[アプリケーション名]
Path:<アプリケーションのパス>	[アプリケーションパス]
Arguments:<アプリケーションの起動時に設定情報を指定>	[引数]
Event:<コマンドを実行するためのイベント>	USER_LOGOFF SVC_STARTUP ON_SHUTDOWN USER_LOGIN

xDCM を使用したノード構成の例

表 8. xDCM を使用したノード構成の例

シナリオ	コマンド
ClientServiceEngine サービスによって使用されているアプリケーションノードを追加して、システムからログオフするときに TestApp.exe に引数 -t を指定して実行します。	ALM.exe -Add -Application -Name:ExampleApp -Path:C:\Windows\System32\TestApp.exe -Arguments:"-t" -Event: USER_LOGOFF
ExampleApp アプリケーションからアプリケーションノードを削除します。	ALM.exe -Remove -Application -Name: ExampleApp

メモ:

- **ALM.exe を使用して ApplicationLaunchConfig.xml に新しいアプリケーションエントリを追加するには、一意の名前を指定する必要があります。**
- **ALM アプリケーションでは、3 種類の実行イベントの値 (USER_LOGOFF、SVC_STARTUP、および ON_SHUTDOWN) のみがサポートされています。イベントごとに、これらの値のうちいずれか 1 つだけを追加できます。**

xData Cleanup Manager

xData Cleanup Manager (xDCM) バージョン 1.0 は、無関係な情報がローカルディスクに保存されないようにします。xDCM を使用すると、情報を一時的にキャッシュするために使用されるディレクトリを自動的にクリーンアップできます。クリーンアップは、サービスのスタートアップ、ユーザーのログオフ、またはシステムシャットダウンのいずれかによってトリガされます。

また、トラブルシューティングに必要なマルチレベルログを設定することもできます。アプリケーションプログラミングインターフェイス (API) を使用して、ファイルやフォルダをクリーンアップしたり、xDCM を有効または無効にしたりできます。また、コマンドラインインターフェイスを使用して、xDCM 構成ファイルに構成ノードを追加または削除することもできます。

メモ:

- **既存の NetXclean.ini 設定は、新しい xDataCleanupConfig.xml に移植されています。**
- **xData Cleanup Manager のコンテンツは、デフォルトでクリーンアップされます。**

xDCM CLI ツール

xDCM CLI ツールを使用して、xDCM 設定ファイル XdataCleanupConfig.xml の設定ノードを追加または削除できます。このツールは、xDCM アプリケーションのインストールパスにあります。デフォルトでは、このツールは %systemdrive%\Program Files\XDCM にあります。

xDCM を使用したノードの構成

次のオプションとパラメータを使用して、XdataCleanupConfig.xml でアプリケーションノードを設定できます。

表 9. ノードを構成するためのオプション

オプション	説明
追加	フォルダクリーンアップノードを追加するオプション。
削除	フォルダクリーンアップノードを削除するオプション。

表 10. ノードを構成するためのパラメータ

パラメータ	Values
CleanupType:<クリーンアップノードのタイプ>	フォルダ ファイル レジストリ
Name:<クリーンアップノードの名前>	[フォルダ / ファイル / レジストリ名]
Path:<クリーンアップノードのパス>	[フォルダ / ファイル / レジストリパス]
PathExclusions:<削除から除外されるパス (Path1,Path2)/ NULL>	[パス / NULL]
Event:<コマンドを実行するためのイベント>	USER_LOGOFF SVC_STARTUP ON_SHUTDOWN
CleanType:<クリーンアップのタイプ>	DIR_DELETE DIR_EMPTY
CleanFrom:<メモリの種類>	ディスク オーバーレイ

xDCM を使用したノード構成の例

表 11. xDCM を使用したノード構成の例

シナリオ	コマンド
DiskCleanup 要素の下の XdataCleanupConfig.xml にフォルダクリーンアップノードを追加します。	XDCM.exe -Add -CleanupType:Folder -Name:Notepad -Path:C:\Windows\Security -PathExclusions:"C:\Windows\Security\database, C:\Windows\logs" -Event: USER_LOGOFF -CleanType:DIR_EMPTY -CleanFrom:Disk
XdataCleanupConfig.xml の **OverlayCleanup** 要素の **Notepad** の下にあるファイルクリーンアップノードを削除します。	XDCM.exe -Remove -CleanupType:File -Name:Notepad -CleanFrom:Overlay

メモ:

- **UWF が無効になっているときにシンクライアントからログオフすると、ClientServiceEngine サービスがフォルダのクリーンアップノードを使用して、ディレクトリ C:\Windows\Security 内のコンテンツをクリーンアップします。また、このディレクトリの内容が削除されると、C:\Windows\Security\database フォルダと C:\Windows\logs フォルダの内容が (除外パスに追加されたため) 削除されます。**
- **XDCM.exe を使用して XdataCleanupConfig.xml に新しいアプリケーションエントリを追加するには、一意の名前を指定する必要があります。**

- **エントリを追加するコマンドを実行しているとき、そのフォルダパスは既存のエントリと比較されます。パスがすでに使用可能な場合は、除外パスのみが既存のフォルダエントリに追加されます。**

ログファイルのキャプチャ

DebugLog.xml ファイルを設定して、さまざまな種類のアプリケーションのログを収集できます。ログレベルを変更すると、特定のタイプのログを取得できます。ログファイルは、C:\Windows\Logs\<Application name>\Logs に作成されます。

メモ: デフォルトでは、アプリケーションのログは作成されません。

DebugLog XML ファイルの設定

デバッグ設定エディタ (DCE) コンソールアプリケーションを使用して、デバッグ設定 XML ファイルを設定できます。このツールを使用して、デバッグ設定ファイルをコミット、除外、または変更できます。

デバッグ設定ファイルをコミット、除外、または変更するには、デバッグ設定エディタで次のコマンドを入力します。

- ファイルをコミットしてログファイルを取得する — DebugConfigEditor.exe -CommitLog -Path "DebugLog.xml"。このコマンドは、Debug.xml に記載されているパスに存在するファイルをコミットします。
- Debug.xml に記載されているフォルダからログの収集を除外する — DebugConfigEditor.exe -ExcludeLog -Path "DebugLog.xml"。
- さまざまなタイプのログを収集するように Debug.xml ファイルを設定する — DebugConfigEditor.exe -UpdateConfig -Path "DebugLog.xml" -LogPath "Path of Log File" -LogFileName "Name of log File" -LogLevel "logLevel"。

  次の表に、使用できるさまざまな LogLevel 値の説明を示します。

表 12. LogLevel の値

値	説明
0	ログは取得されません。
1	エラーログが取得されます。
2	警告ログが取得されます。
3	エラーログおよび警告ログが取得されます。
4	情報ログが取得されます。
7	すべてのログが取得されます。

ファイルの保存およびローカルドライブの使用

シンクライアントは、一定量のディスク領域に組み込まれたオペレーティングシステムを使用します。保持したいファイルは、シンクライアント上ではなくサーバ上に保存することをお勧めします。

注意: ディスク領域のドライブ C に書き込むというアプリケーション設定に注意してください。デフォルトでは、これらのアプリケーションは、ローカルシステムのドライブ C にキャッシュファイルを書き込みます。ローカルドライブに書き込む必要がある場合は、ドライブ Z を使用するようにアプリケーションの設定を変更します。「ユーザーアカウントを使用したユーザーとグループの管理」に記載されているデフォルトの構成設定では、工場出荷時にインストールされたアプリケーションによるドライブ C への書き込みを最小限に抑えています。

ドライブ Z

ドライブ Z は、シンクライアントのオンボードの不揮発性メモリ (Dell Wyse RAM ディスク) です。保持しておきたいデータの保存にはこのドライブを使用しないことをお勧めします。

ローミングプロファイルを含む Z ドライブの使用の詳細については、「ドメインへの参加」を参照してください。

ドライブ C

ドライブ C は、オンボードの不揮発性のフラッシュメモリです。ドライブ C には書き込まないことをお勧めします。ドライブ C に書き込むと、空きディスク領域が減少します。ドライブ C の空きディスク容量が 500 MB 未満まで減少すると、シンクライアントは不安定になります。

メモ: 500 MB のディスク容量を未使用領域として空けておくことを強くお勧めします。空きディスク容量が 500 MB まで減少すると、シン クライアントは修復不可能な損傷を受けるため、認定サービスセンターに連絡して修理を依頼する必要があります。

統合書き込みフィルターを有効にすると、ディスクが損傷から保護され、キャッシュが上書きされた場合にエラーメッセージが表示されます。ただし、このメッセージが表示されると、統合書き込みフィルター キャッシュのファイルをフラッシュできなくなり、キャッシュ内にあるシン クライアントの設定変更はすべて失われます。統合書き込みフィルターのキャッシュに書き込まれる項目、または、統合書き込みフィルターが通常の動作時に無効になった場合に直接ディスクに書き込まれる項目には、以下のものがあります。

- お気に入り
- 作成された接続
- 接続の削除 / 編集

ネットワークドライブのマッピング

管理者は、ネットワークドライブをマッピングできます。ネットワーク ドライブをマッピングし、シン クライアント デバイスを再起動した後にもそのマッピングを保持するには、https://support.microsoft.com で『*ネットワーク ドライブの割り当て*』を参照してください。

ドメインへの参加

シンクライアントをドメインに参加させるか、ローミングプロファイルを使用することにより、ドメインに参加することができます。

ドメインに参加するには、次の手順を実行します。

1. 管理者としてログインします。
2. **スタート** > **コントロール パネル** > **システム** の順に選択します。
   システム ウィンドウが表示されます。
3. **コンピュータ名、ドメインおよびワークグループの設定** セクションで、**設定の変更** をクリックします。
   システムのプロパティ ダイアログボックスが表示されます。
4. **変更** オプションをクリックして、ドメインまたはワークグループを変更します。
   a) **ドメイン** をクリックします。
      コンピュータ名 / ドメインの変更 ダイアログボックスが表示されます。
   b) 任意のドメインを入力します。
   c) **OK** をクリックします。
5. シンクライアントデバイスをドメインに参加させるには、**ネットワーク ID** をクリックします。
   ドメインまたはワークグループへの参加 ウィザードが表示されます。ウィザードの最初のページでは、お使いのネットワークを示すオプションを選択します。
   - ビジネスネットワーク — シンクライアントがビジネスネットワークの一部であり、仕事で他のクライアントへの接続に使用する場合、このオプションをクリックします。
     a. **次へ** をクリックします。
     b. 企業ネットワークがドメインで使用可能かどうかに基づいてオプションを選択します。
        オプション **ドメインを使用しているネットワーク** を選択した場合は、次の情報を入力します。
        - ユーザー名
        - パスワード
        - ドメイン名

        オプション **ドメインを使用していないネットワーク** を選択した場合は、**ワークグループ** を入力してから **次へ** をクリックします。

        メモ: ワークグループ名がわからない場合も、次へ をクリックします。
     c. 変更を適用するには、コンピュータを再起動する必要があります。**終了** をクリックします。

        メモ: コンピュータを再起動する前に、開いているファイルを保存し、すべてのプログラムを閉じます。
   - ホームネットワーク — シンクライアントがホームクライアントであり、ビジネスネットワークの一部でない場合は、このオプションをクリックします。変更を適用するには、コンピュータを再起動する必要があります。**終了** をクリックします。

注意: ログオン時にプロファイルをダウンロードすることによってキャッシュやフラッシュメモリがオーバーフローする場合があるので、ドメインにシンクライアントデバイスを参加させるときは特に注意が必要です。

シンクライアントデバイスをドメインに参加させるときは、統合書き込みフィルターを無効にしてシンクライアントデバイスにドメイン情報を永続的に保存できるようにしてください。情報はドメイン参加後の再起動時にシンクライアントに書き込まれるので、統合書き込みフィルターは次の再起動まで無効のままにしてください。この統合書き込みフィルターは、Active Directory ドメインに参加するときに重要です。統合書き込みフィルターを有効または無効にする手順の詳細については、「シンクライアントを設定する前に」を参照してください。

ドメイン変更を永続的にするには、次の手順を実行します。

a) 統合書き込みフィルターを無効にします。
b) ドメインに参加します。
c) シンクライアントを再起動します。
d) 統合書き込みフィルターを有効にします。

メモ:

書き込みフィルター有効化 アイコンを使用して書き込みフィルターを有効にすると、シンクライアントは自動的に再起動します。

ローミングプロファイルの使用

C ドライブにローミングプロファイルを書き込むことにより、ドメインに参加できます。プロファイルのサイズを制限する必要があります。また、プロファイルは、シンクライアントデバイスの再起動時に失われます。ローミングプロファイルを正常にダウンロードし正しく機能させるためには、ローミングプロファイル用に十分なディスク容量が必要です。場合によっては、ローミングプロファイル用の容量を確保するためにソフトウェアコンポーネントの削除が必要になります。

Net および Tracert ユーティリティの使用

Net および Tracert ユーティリティは、管理用途で使用できます。たとえば、IP ネットワーク上でのパケット経路決定などに使用できます。

これらのユーティリティの詳細については、www.microsoft.com を参照してください。

ユーザーアカウントを使用したユーザーとグループの管理

ユーザーアカウントおよびグループを作成・管理して、詳細なユーザープロファイルのプロパティを設定するには、**ユーザーアカウント** ウィンドウを使用します。デフォルトでは、新しいユーザーは **ユーザー** グループのメンバーとなるだけで、ロックダウンされていません。管理者として、ユーザーの属性およびプロファイル設定を選択できます。

この項では、以下の項目に関するクイックスタートガイドラインを提供します。

- ユーザーアカウントの作成
- ユーザーアカウントの編集
- ユーザープロファイルの設定

メモ: ユーザーアカウント ウィンドウの使用方法については、ウィザードを通じて提供される ヘルプ アイコンおよびサンプルへのリンクをクリックしてください。たとえば、Windows のヘルプとサポート ウィンドウを使用すると、ユーザープロファイルやユーザーグループなどの項目を検索できます。これらの項目の作成および管理の詳細な手順へのリンクを取得します。

ユーザーアカウントの作成

管理者のみが、VNC を使ってローカルまたはリモートからユーザーアカウントを作成できます。ただし、ローカルフラッシュまたはディスク容量の制限から、シンクライアントデバイス上の追加のユーザー数は最小限に抑えるべきです。

注意: 情報を永久的に保存するには、統合書き込みフィルター (UWF) を必ず無効にしてください。

1. 管理者としてログインします。
2. **スタート** > **コントロールパネル** > **ユーザーアカウント** の順に選択します。
3. **ユーザーアカウント** ウィンドウで、**別のアカウントの管理** をクリックします。
   アカウントの管理 ウィンドウが表示されます。

4. PC 設定の **新規ユーザーの追加** をクリックします。
   PC 設定 ウィザードが起動します。このウィザードを使用してユーザーアカウントを作成します。
5. 標準ユーザーおよび管理者の作成後、作成したユーザーが **アカウントの管理** ウィンドウに表示されます。**手順 3** を参照してください。

ユーザーアカウントの編集

「ユーザーアカウントの管理」で説明されているように、**ユーザーアカウント** ウィンドウを開きます。

標準のユーザーまたは管理者のアカウントのデフォルトの設定を編集するには、次の手順を実行します。

1. **ユーザーアカウント** ウィンドウで、**別のアカウントの管理** をクリックします。
   アカウントの管理 ウィンドウが表示されます。
2. 必要に応じて変更するには、**ユーザー** を選択します。
   アカウントの変更 ウィンドウが表示されます。ここで、記載されているリンクを使用して変更を行います。

ユーザープロファイルの設定

「ユーザーアカウントの管理」で説明されているように、**ユーザーアカウント** ウィンドウを開きます。

注意:

- **デフォルトでは、すべてのアプリケーションが C ドライブにキャッシュを作成するように設定されています。統合書き込みフィルターキャッシュのオーバーフローを避けるため、アカウントのプロファイルに事前に設定されていたように RAM ディスク (ドライブ Z) にキャッシュを作成することをお勧めします。**
- **新規および既存のユーザーが使用できる他のアプリケーションは、ディスク容量が限られているため、ローカルファイルシステムには書き込めないように設定することをお勧めします。工場出荷時にインストールされたアプリケーションの構成設定を変更するときには、特に注意することをお勧めします。**

シンクライアントに保存されているデフォルト管理者とユーザーのプロファイルを設定するには、次の手順を実行します。

1. **ユーザーアカウント** ウィンドウで、**詳細ユーザープロファイルのプロパティの設定** をクリックします。

   ユーザープロファイル ダイアログボックスが表示されます。
2. ウィザードを通じて提供される Microsoft のドキュメントで説明されているように、**種類の変更**、**削除**、**コピー先** などのコマンドボタンを使用します。

シンクライアントのコンピュータ名の変更

管理者は、シンクライアントのコンピュータ名を変更することができます。コンピュータ名の情報とターミナルサービスクライアントアクセスライセンス (TSCAL) は、統合書き込みフィルタの状態 (有効または無効) に関係なく保持されます。これにより、特定のコンピュータ識別情報が保持され、シンクライアントのイメージの管理が容易になります。

シンクライアントデバイスのコンピュータ名を変更するには、次の手順を実行します。

1. 管理者としてログインします。
2. **スタート** > **コントロールパネル** > **システム** の順に選択します。
   システム ウィンドウが表示されます。
3. **コンピュータ名、ドメイン、およびワークグループ設定** セクションで、**設定の変更** をクリックします。
   システムのプロパティ ダイアログボックスが表示されます。
4. **変更** をクリックして、コンピュータ名を変更します。
5. **コンピュータ名** ウィンドウで、**コンピュータ名** フィールドにシンクライアントデバイスの名前を入力して **OK** をクリックします。
6. 確認 ダイアログボックスで、**OK** をクリックして変更を適用するために再起動します。
7. **閉じる** をクリックし、**今すぐ再起動** をクリックして変更を適用します。

6

システム管理

シンクライアントデバイスの環境を維持するために、ローカルおよびリモートのシステム管理タスクを実行できます。そのようなタスクには以下があります。

- シンクライアントの BIOS 設定へのアクセス
- 統合拡張可能ファームウェアインタフェース (UEFI) とセキュアブート
- Wyse Management Suite の使用
- ポートとスロット
- Tight VNC (サーバおよびビューア) を使用したシンクライアントのシャドーイング

シンクライアントの BIOS 設定へのアクセス

シンクライアント BIOS 設定にアクセスするには、次の手順を実行します。

1. システムの起動中に、Dell ロゴが表示されたら F2 キーを押します。
   BIOS 設定 画面が表示されます。
2. 必要に応じて BIOS 設定を変更します。
3. 変更を保存して終了します。

統合拡張可能ファームウェアインターフェイスとセキュアブート

統合拡張可能ファームウェアインタフェース (UEFI) は、ソフトウェアの相互運用性と BIOS のアドレス制限を改善するように設計された標準ファームウェアインタフェースです。UEFI は、基本入出力システム (BIOS) に取って代わるように設計されています。

セキュアブートは、UEFI ベースのクライアントの機能であり、起動シーケンス中に不正なソフトウェアがクライアントで実行されるのを防止することでクライアントのセキュリティを高めます。起動中に読み込まれるオペレーティングシステム (OS) も含めて、各ソフトウェアに有効な署名があることを確認します。

シンクライアントデバイスでは、UEFI とセキュアブートが有効になっています。この機能により、BIOS モードに入って、セキュアブートを無効化してレガシー起動モードへ変更し、**USB からの起動** オプションを有効にしない場合、USB キーからは起動できません。

DOS USB キーからの起動

次の表に、サポートされているシンクライアントデバイスの DOS USB キーから起動するためのガイドラインを示します。

表 13. DOS USB キーからの起動

シンクライアント	シンクライアントを起動するためのガイドライン
• Wyse 5020 Thin Client (Win10 IoT) (D90Q10) • Wyse 7020 Thin Client (Win10 IoT) (Z90Q10) • Wyse 7020 高速グラフィックス Thin Client (Win10 IoT) (Z90QQ10) • Wyse 5060 Thin Client	DOS USB キーからシンクライアントを起動するには、次の手順を実行します。 1. システムの起動中に、Wyse ロゴが表示されたら `Delete` キーを押します。 BIOS **設定** 画面が表示されます。 2. **セキュアブート** を **無効** に設定します。 3. **起動モード** を **レガシー** に設定します。 4. **USB からの起動** を **有効** に設定します。 5. 変更を保存して終了します。

シンクライアント	シンクライアントを起動するためのガイドライン
	6. ポップアップメニューで、使用する USB キーを選択し、**通常**の起動を選択します。

UEFI USB キーからの起動

次の表に、サポートされているシンクライアントデバイスの UEFI USB キーから起動するためのガイドラインを示します。

表 14. UEFI USB キーからの起動

サポートされる Thin Client	シンクライアントを起動するためのガイドライン
• Wyse 5020 Thin Client (Win10 IoT) (D90Q10) • Wyse 7020 Thin Client (Win10 IoT) (Z90Q10) • Wyse 7020 高速グラフィックス Thin Client (Win10 IoT) (Z90QQ10)	UEFI USB キーからシンクライアントを起動するには、次の手順を実行します。 1. システムの起動中に、Wyse ロゴが表示されたら `Delete` キーを押します。 BIOS **設定** 画面が表示されます。 2. **セキュアブート** を **無効** に設定します。 3. **USB からの起動** を **有効** に設定します。 4. 変更を保存して終了します。 5. ポップアップメニューで、使用する USB キーを選択し、**通常**の起動を選択します。
• Wyse 5470 Thin Client • Wyse 5470 All-in-One Thin Client • Wyse 5060 Thin Client • Wyse 7040 Thin Client • Latitude 3480 モバイル Thin Client • Latitude 5280 モバイル Thin Client	UEFI USB キーからシンクライアントを起動するには、次の手順を実行します。 1. システムの起動中に、Dell ロゴが表示されたら `F2` キーを押します。 BIOS **設定** 画面が表示されます。 2. **セキュアブート** を **無効** に設定します。 3. **システム設定** > **USB 設定** の順にクリックして、**USB 起動サポートを有効にする** チェックボックスを選択します。 4. 変更を保存して終了します。 5. システムの起動中に `F12` キーを押し、起動メニューの USB キー を選択します。 **メモ: セキュアブートが 無効 に設定されている場合は、Windows 10 IoT Enterprise (WIE10) 64 ビットデバイスを起動できます。ただし、セキュリティの観点からはこの方法はお勧めできません。**

起動可能な UEFI USB キーの作成

起動可能な UEFI USB を作成するには、次の手順を実行します。

1. 実行可能な UEFI シェルを取得します。
2. そのファイルを `bootx64.efi` としてクライアントに保存します。
3. USB キーを `FAT32` でフォーマットします。
4. その USB キーに、`\efi\boot` ディレクトリを作成します。
5. `bootx64.efi` ファイルを USB キーの `\efi\boot` ディレクトリにコピーします。
   これで、起動可能な UEFI USB キーが作成されました。

Dell Wyse Management Suite の使用

Wyse Management Suite は、Dell Wyse Thin Client を一元で設定、監視、管理、最適化するための次世代管理ソリューションです。高い機能性、パフォーマンス、使いやすさを誇る新しい Suite では、Thin Client の導入および管理を簡単に行うことができます。ク

ラウドやオンプレミスでの導入、モバイルアプリケーションによる場所を問わない管理、BIOS 設定やポートロックダウンなどのセキュリティの向上など、最新機能オプションも備えています。その他にも、デバイスの検出 / 登録、資産 / インベントリ管理、設定管理、オペレーティングシステム / アプリケーションの導入、リアルタイムコマンド、監視、アラート、レポート、エンドポイントのトラブルシューティングなどの機能があります。

Dell Wyse Management Suite の詳細については、dell.com/support/manuals を参照してください。

メモ: Windows 10 IoT Enterprise オペレーティングシステムを実行しているデバイスを Wyse Management Suite に登録するには、dell.com/support/manuals の『*Wyse Device Agent を使用した Wyse Management Suite への Windows Embedded Standard シンクライアントの登録*』を参照してください。

ポートとスロット

シンクライアントデバイスには、ポートとスロットが多数あります。職場でのシンクライアントデバイスのポートおよびスロットの詳細については、dell.com/support でそれぞれの『クイックスタートガイド』を参照してください。

ポート経由でサービスを提供するには、シンクライアントデバイスに適切なドライバまたはソフトウェアをインストールします。

メモ:

- **デルのウェブサイトから、無料またはライセンス料を支払って使用できる他のサービスおよびアドオンをインストールできます。**
- **シンクライアントデバイスを設定して、Bluetooth 対応の周辺機器を使用できます。詳細については、「Bluetooth 接続の設定」を参照してください。**

TightVNC — サーバおよびビューアー

シンクライアントデバイスを遠隔地から設定するには、TightVNC (サーバおよびビューアー) を使用します。TightVNC の主な目的は、サポートおよびトラブルシューティングです。

TightVNC を、シンクライアントデバイスにローカルでインストールします。インストール後は、リモートデバイスからシンクライアントをシャドーイング、操作および監視できます。

TightVNC サーバは、シンクライアントデバイスの再起動時にサービスとして自動的に起動します。TightVNC サーバの初期化も、この手順で サービス ウィンドウを使用して制御できます。

TightVNC サーバ ウィンドウを開くには、次の手順を実行します。

1. 管理者としてログインします。
2. **スタートメニュー** > **TightVNC** > **TightVNC サーバ** の順にクリックします。

メモ:

- **TightVNC Web サイトから TightVNC ビューアーを利用できます。**
- **TightVNC はコンポーネントとして WDM ソフトウェアに含まれます。**
- **TightVNC ビューアーは、シャドーイングするマシンまたはリモートマシンに事前にインストールする必要があります。**
- **サービスのステータスを永続的に保存する場合は、現在のシステムのセッション中に統合書き込みフィルターのファイルをフラッシュしてください。**

TightVNC — 前提条件

TightVNC サーバをリモートマシンにインストールする前に、シンクライアントデバイスにアクセスするには次の情報を知っておく必要があります。

- シャドーイング、操作、監視するシンクライアントデバイスの IP アドレスまたは有効な DNS 名。
- シャドーイング、操作、監視するシンクライアントデバイスのプライマリパスワード。

メモ:

- **シンクライアントデバイスの IP アドレスを取得するには、タスクバーの TightVNC アイコン上にポインタを移動します。**
- **TightVNC サーバを設定する際、デフォルトパスワードは DELL です。**

TightVNC を使用したシンクライアントのシャドーイング

TightVNC サーバは、シンクライアント起動時のサービスとして自動的に起動します。サービス ウィンドウを使用して、TightVNC サーバサービスを開始 / 停止することもできます。

1. 管理者としてログインします。
2. **スタート** > **コントロール パネル** > **管理ツール** > **サービス** の順に移動してから、**TightVNC サーバ** を選択します。
3. **スタート** > **TightVNC** の順に選択して TightVNC サーバ機能を使用することもできます。

   リモートマシンからシンクライアントをシャドーイングするには、以下の操作を行います。

   a) TightVNC ビューアーがインストールされているリモートマシンで **新しい Tight VNC 接続** ダイアログボックスを開きます。
   b) シャドーイング、操作、監視するシンクライアントの IP アドレスまたは有効な DNS 名を入力します。
   c) **OK** をクリックします。
   VNC 認証 ダイアログボックスが表示されます。
   d) シャドーイングするシンクライアントの **パスワード** を入力します。これは、シャドーイングするシンクライアントのプライマリパスワードです。
   e) **OK** をクリックします。

   リモートマシンの別のウィンドウに、シャドーイング、操作、または監視する対象のシンクライアントが管理者用に表示されます。リモートマシンのマウスとキーボードを使用して、ローカルでの操作時と同様にシンクライアントを操作します。

シンクライアントでの TightVNC サーバのプロパティの設定

1. **TightVNC サーバ設定 (オフライン)** ダイアログボックスを開くには、**スタート** > **TightVNC** > **TightVNC サーバ - オフライン設定** の順に移動します。
   TightVNC サーバ設定 (オフライン) ダイアログボックスが表示されます。
2. **サーバ** タブで、**プライマリパスワード** を設定します。シンクライアントのシャドーイング時にはこのパスワードを使用します。デフォルトのプライマリパスワードは `Wyse` です。
3. **サーバ** タブで、次のチェックボックスを選択します。
   - 受信接続を受け付ける
   - VNC 認証を必要とする
   - ファイル転送の有効化
   - デスクトップの壁紙を非表示にする
   - タスクトレイにアイコンを表示する
   - Web クライアントに Java Viewer を使用する
   - 使用可能な場合にミラードライバを使用する
   - 透過ウィンドウのキャプチャ
4. 次のチェックボックスは空白のままにします。
   - リモート入力イベントをブロック
   - ローカルアクティビティでリモート入力をブロック
   - クライアントセッション中にローカル入力をしない
5. **メインサーバポート** ボックスで、5900 を選択または入力します。
6. **Web アクセスポート** ボックスで、5800 を選択または入力します。
7. **画面ポーリングサイクル** ボックスで、1000 を選択または入力します。
8. **OK** をクリックします。

メモ: セキュリティ上の目的から、シン クライアントを受け取ったらすぐにプライマリー パスワードを変更すること、さらに管理者のみが使用するようにすることをお勧めします。

7

ネットワークアーキテクチャとサーバ環境

この項には、シンクライアントのネットワークおよびセッションサービスを提供するために必要なネットワークアーキテクチャとエンタープライズサーバ環境に関する情報が含まれます。この項の内容：

- ネットワークサービスの設定方法について
- 動的ホスト構成プロトコル（DHCP）の使用
- DHCP オプション
- ドメインネームシステム（DNS）の使用
- Citrix Studio について
- VMware Horizon View Manager サービスについて

ネットワークサービスの設定方法について

シンクライアントに提供されるネットワークサービスには、DHCP、FTP ファイルサービス、DNS などがあります。使用環境での可用性に応じて、ネットワークサービスを構成、設計、および管理できます。

次のものを使用して、ネットワークサービスを設定できます。

- 動的ホスト構成プロトコル（DHCP）
- ドメインネームシステム（DNS）

動的ホスト構成プロトコルの使用

シンクライアントは、IP アドレスとネットワーク構成を動的ホスト構成プロトコル（DHCP）サーバから取得するように初期設定されています。DHCP サーバは、DHCP アップグレードプロセスによって IP アドレスおよびネットワーク構成にアクセスするための FTP サーバの IP アドレスまたは DNS 名、およびソフトウェアの FTP ルートパスの場所を `Microsoft.msi` 形式で提供します。

シンクライアントの設定およびアップグレードには、DHCP を使用することをお勧めします。これにより、複数のシンクライアントでこれらの設定をローカルに行う時間と手間を軽減できます。DHCP サーバを使用できない場合は、固定 IP アドレスを割り当てることができます。固定 IP アドレスはデバイスごとにローカルに入力する必要があります。

DHCP サーバは、WMS サーバの IP アドレスも提供できます。

DHCP オプション

次の表にリストされている DHCP オプションは、シンクライアントによって受け入れられます。

表 15. 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
3	ルーター	オプションですが推奨されています。シンクライアントが別のサブネット上のサーバと対話する必要がない限り、これは必須ではありません。
6	ドメインネームサーバ（DNS）	オプションですが推奨されています
12	ホスト名	オプション
15	ドメイン名	オプションですが推奨されています
43	ベンダークラス固有の情報	オプション
50	要求された IP	必須
51	リース時間	必須

オプション	説明	メモ
52	オプションの過負荷	オプション
53	DHCP メッセージタイプ	必須
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	DHCP メッセージの最大サイズ	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	必須
59	T2 (リバインド) 時間	必須
61	クライアント識別子	常に送信されます
155	プロキシサーバの IP アドレスまたは名前	オプション
156	接続に使用するログオンユーザー名	オプション
157	接続に使用するドメイン名	オプション
158	接続に使用するログオンパスワード	オプション
159	接続用コマンドライン	オプション
160	接続用作業ディレクトリ	オプション
163	SNMP トラップサーバの IP アドレスリスト	オプション
164	SNMP 設定コミュニティ	オプション
165	リモートデスクトップ接続の起動公開アプリケーション	オプション
168	仮想ポートのサーバ名	オプション
165	Wyse Management Suite サーバの URL オプションタグ	オプション
166	MQTT サーバの URL オプションタグ	オプション
167	Wyse Management Suite CA 検証サーバの URL オプションタグ	オプション
199	Wyse Management Suite グループトークンサーバの URL オプションタグ	オプション

メモ: DHCP サーバの設定の詳細については、www.microsoft.com を参照してください。

ドメインネームシステムの使用

シンクライアントデバイスは、企業イントラネットで利用可能なドメインネームシステム (DNS) サーバ上で登録されている有効な DNS 名を受け付けます。シンクライアントデバイスは、ネットワーク上の DNS サーバに名前を照会して、対応する IP アドレスに翻訳します。DNS を使用すると、IP アドレスではなく登録した DNS 名でホストにアクセスできます。

Windows Server 2000 およびそれ以降の各 Windows DNS サーバはすべてダイナミック DNS (DDNS) を装備しており、サーバはすべて DNS サーバに動的に登録されます。DNS ドメインの DHCP エントリおよびサーバの場所情報については、「動的ホスト構成プロトコル (DHCP) の使用」を参照してください。

Citrix Studio について

Citrix Studio は、パーソナライズされたデスクトップおよびアプリケーションの設定および管理を可能にするソフトウェアプログラムです。Citrix Studio は、すべてのデバイスおよびネットワークにわたって簡単なエンドユーザーコンピューティング体験を提供しながら、パフォーマンスの最適化、セキュリティの向上、パーソナライズの向上を実現します。

メモ: **Citrix Studio のインストールおよび設定の詳細については、Citrix ウェブサイト を参照してください。**

Citrix Studio は、次のタスクを実行することができる各種のウィザードから構成されます。

- 仮想アプリケーションの公開
- サーバまたはデスクトップオペレーティングシステムのグループの作成
- アプリケーションおよびデスクトップのユーザーへの割り当て
- ユーザーのリソースへのアクセスの許可
- 権限の割り当てと転送
- Citrix ライセンスの取得と追跡
- StoreFront の設定

使用可能なすべての仮想デスクトップアプリケーション (VDA) は、Studio にリストされます。VDA リストから、公開するアプリケーションを選択します。Studio に表示される情報は、コントローラの ブローカーサービス から受信されます。

VMware Horizon View Manager について

VMware View は企業クラスの仮想デスクトップマネージャであり、承認されたユーザーを集中管理された仮想デスクトップにセキュアに接続します。VMware View は完全なエンドツーエンドのソリューションを提供し、これによって制御性と管理容易性が向上し、使い慣れたデスクトップエクスペリエンスが実現されます。クライアントソフトウェアは、集中管理された仮想デスクトップ、バックエンドの物理システム、またはターミナルサーバにユーザーをセキュアに接続します。

メモ: **View Manager のインストールおよび設定の詳細については、VMware ウェブサイトを参照してください。**

VMware View には、次の主要コンポーネントが含まれます。

- **View Connection Server** — クライアント接続の仲介として機能するソフトウェアサービス。受信したリモートデスクトップユーザーの要求を認証して、適切な仮想デスクトップ、物理デスクトップまたはターミナルサーバに転送します。
- **View Agent** — すべてのゲスト仮想マシン、物理システム、またはターミナルサーバ上にインストールされているソフトウェアサービス。View Manager はこのソフトウェアを管理します。エージェントは、リモートデスクトップ接続の監視、仮想印刷、リモート USB のサポート、およびシングルサインオンなどの機能を提供します。
- **View Client** — ローカルにインストールされているソフトウェアアプリケーション。View Connection Server と通信することにより、ユーザーは Microsoft のリモートデスクトップ接続を使用してデスクトップに接続可能となります。
- **View Portal** — View Client とよく似ていますが、Web ブラウザを介して View ユーザーインターフェイスを提供します。これは、複数のオペレーティングシステムとブラウザでサポートされます。
- **View Administrator** — Web ブラウザを介して View の管理を提供します。View 管理者は、このコンポーネントを使用して以下を行います。

  - 構成設定を管理します。
  - 仮想デスクトップと、Windows のユーザーおよびグループのデスクトップの資格を管理します。

  View Administrator は、ログイベントを監視するインタフェースも提供しており、View Connection Server と共にインストールされます。
- **View Composer** — View Manager が、集中管理された単一のベースイメージから複数のリンククローンデスクトップを迅速に展開できるように、Virtual Center サーバには **View Composer** ソフトウェアサービスがインストールされます。

8

USB イメージングツールを使用した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は、シンクライアントに Windows 10 IoT Enterprise ファームウェアをインストールするプロセスです。

Dell Wyse USB Imaging Tool バージョン 3.2.0 を使用して、シンクライアントに Windows 10 IoT Enterprise 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、https://downloads.dell.com/wyse/の『*Dell Wyse USB イメージング ツール バージョン 3.2.0 ユーザーズ ガイド*』を参照してください。

9

FAQ（よくある質問）

Skype for Business のインストール方法

シンクライアントに Skype for Business をインストールするには、次の手順を実行します。

1. 管理者としてログインします。
2. 統合書き込みフィルターを無効にします。
3. Skype for Business スタンドアロン（64 ビット）を https://support.microsoft.com からダウンロードします。
4. .exe ファイルをダブルクリックして、**実行** をクリックします。
5. インストール完了後、**閉じる** をクリックします。
6. Skype for Business を起動します。
7. 使用許諾契約書の画面で、**同意する** をクリックします。
8. 統合書き込みフィルターを有効にします。

詳細については、https://support.office.com の『*Skype for Business をインストールする*』を参照してください。

スマートカードリーダーのセットアップ方法

スマートカードリーダーをセットアップするには、次の手順を実行します。

1. 管理者としてログインします。
2. 統合書き込みフィルターを無効にします。
3. 使用したいスマートカードアプリケーションをダウンロードします。
4. ローカルドライブにファイルを解凍します。
5. スマートカードの入ったスマートカードリーダーを接続して、**設定** をクリックします。
6. インストールが完了したら、Citrix または VMware セットアップの接続を確立する場合は、サーバ証明書をインストールします。
7. 統合書き込みフィルターを有効にします。
8. Citrix、VMware、RDP などの優先 VDI セッションに接続します。

USB リダイレクトの使用方法

USB リダイレクトを使用すると、シンクライアントの USB ポートに外部デバイスを接続し、そのデバイスに対してリモートデスクトップまたはアプリケーションを使用してアクセスできます。

Citrix Virtual Apps and Desktops（旧 Citrix XenDesktop）環境で、USB リダイレクトを設定できます。詳細については、support.citrix.com の『*Citrix Generic USB Redirection Configuration Guide*』（Citrix 汎用 USB リダイレクト構成ガイド）を参照してください。

また、View Virtual Desktop セッションで、USB デバイスを使用および管理するオプションを設定できます。詳細については、www.vmware.com の『*USB Device Redirection, Configuration, and Usage in View Virtual Desktops*』（View Virtual Desktops での USB デバイスのリダイレクト、構成、および使用方法）を参照してください。

Windows 10 IoT Enterprise オペレーティングシステムイメージのキャプチャおよびプッシュの方法

次のいずれかの方法を使用して、Windows 10 IoT Enterprise オペレーティングシステムイメージをキャプチャおよびプッシュできます。

- Wyse Management Suite
- Microsoft System Center Configuration Manager（SCCM）
- USB イメージングツール

Wyse Management Suite および SCCM の詳細については、https://support.dell.com/manuals でそれぞれのガイドを参照してください。

USB イメージング ツールの詳細については、https://downloads.dell.com/wyse の『*Dell Wyse USB イメージング ツール ユーザーズ ガイド*』を参照してください。

10

トラブルシューティング

キーボードのカスタマイズの問題

デフォルトでサポートされていないキーボード言語をカスタマイズするには、次の手順を実行します。

1. `C:\Windows\system32\oobe` に移動します。
2. `oobe.xml` ファイルと、関連するサブディレクトリを削除します。
3. sysprep.xml ファイルを手動でカスタマイズし、キーボード、ロケールなどをそれぞれの言語に設定します。
4. .xml ファイルを手動で展開するか、SCCM またはカスタム Sysprep を使用して展開します。

キーボード、ロケール、タイムゾーン、国などすべての環境設定が適用されます。

メモリの問題の解決

Dell Wyse Windows Embedded シンクライアントの **メモリ不足** エラーのトラブルシューティングを行うには、次のいずれかのツールを使用して、メモリ要件を特定して調整します。

- Windows タスクマネージャー
- 統合書き込みフィルター
- ファイルエクスプローラ

メモ: エラー ダイアログボックスの名前は、メモリの問題の原因を識別するために役立ちます。

Windows タスクマネージャーの使用

1. 管理者としてログインします。
2. Ctrl+Alt+Delete キーを押します。
3. **タスクマネージャ**をクリックします。

   タスクマネージャウィンドウが表示されます。
4. **詳細**をクリックします。
5. **パフォーマンス** タブをクリックし、システムメモリリソースを分析します。
6. より多くのメモリを使用しているプログラムを終了します。

統合書き込みフィルターの使用

1. 管理者としてログインします。
2. システムトレイの UWF アイコンをダブルクリックします。
3. **FBWF キャッシュに使用される RAM の量 (MB)** オプションを設定します。

ファイルエクスプローラの使用

ファイルエクスプローラを使用して、Z: (RAMDisk) ドライブのサイズを確認できます。更新された値を表示するには、アプリケーションを最新表示に更新する必要があります。

ブルー スクリーン エラー (BSOD) の問題

エラー コード「`CRITICAL PROCESS DIED`」を伴うブルー スクリーン エラー (BSOD) が、Apacer ソリッドステート ドライブを搭載し、Windows 10 IoT Enterprise バージョン 10.03.06.10.18.00 を実行している Wyse 5070 Thin Client で見られます。この問題を解決するには、AHCI インターフェイスを使用してシン クライアントに接続されたストレージ デバイスのリンク電源管理モードを無効にする必要があります。

メモ: この問題は、バージョン 10.03.06.10.18.00 より以降の Windows 10 IoT Enterprise イメージ ビルドでは解決しており、従ってレジストリー エントリーを手動で適用する必要はありません。

レジストリー ファイルを使用してリンク電源管理モードを無効にするには、次の手順に従います。

1. 管理者としてログインします。
2. 統合書き込みフィルターを無効にします。

   システムが再起動します。
3. 管理者として再度ログインします。
4. メモ帳を開き、次の構文を入力します。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\storahci\Parameters\Device]
"SingleIO"=hex(7):2a,00,00,00
"NoLPM"=hex(7):2a,00,00,00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings
\0012ee47-9041-4b5d-9b77-535fba8b1442\0b2d69d7-a2a1-449c-9680-
f91c70521c60\DefaultPowerSchemeValues\381b4222-f694-41f0-9685-ff5bb260df2e]
"ACSettingIndex"=dword:00000000
"DCSettingIndex"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings
\0012ee47-9041-4b5d-9b77-535fba8b1442\0b2d69d7-a2a1-449c-9680-
f91c70521c60\DefaultPowerSchemeValues\8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c]
"ACSettingIndex"=dword:00000000
"DCSettingIndex"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings
\0012ee47-9041-4b5d-9b77-535fba8b1442\0b2d69d7-a2a1-449c-9680-
f91c70521c60\DefaultPowerSchemeValues\a1841308-3541-4fab-bc81-f71556f20b4a]
"ACSettingIndex"=dword:00000000
"DCSettingIndex"=dword:00000000
```

5. ファイルを.reg ファイルとして保存します。
6. [**スタート**] をクリックします。
7. 検索フィールドに「cmd」と入力します。
8. [**コマンド プロンプト**] を右クリックします。
9. [**管理者として実行**] をクリックします。

   [**ユーザー アカウント制御**] ウィンドウが表示されます。
10. [**はい**] をクリックします。

    権限が昇格されたコマンド プロンプト ウィンドウが表示されます。
11. reg import <file path of the registry file>コマンドを実行します。
12. 統合書き込みフィルターを有効にします。