Dell Wyse Management Suite

バージョン 2.0 管理者ガイド

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。

March 2020

Rev. A00

目次

1

Wyse Management Suite の紹介

Wyse Management Suite は、Dell Wyse Thin Client を集中的に設定、監視、および最適化できる次世代の管理ソリューションです。クラウドやオンプレミス展開、モバイル アプリケーションを使用する場所を問わない管理オプション、BIOS 設定やポート ロックダウンなどの強化されたセキュリティなどの高度な機能のオプションも提供します。その他の機能には、デバイス検出 / 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、リアルタイムのコマンド、監視、アラート、レポート、およびエンドポイントのトラブルシューティングが含まれます。

トピック：

- Wyse Management Suite バージョン 2.0 の新機能
- Wyse Management Suite のエディション
- Wyse Management Suite の機能マトリックス

Wyse Management Suite バージョン 2.0 の新機能

- ThinOS バージョン 9.0 がサポートされています。
- ThinOS 9.x デバイス用の新しい設定ユーザー インターフェイス。
- ローカルまたはリモートのリポジトリー サーバーでは、ファームウェアおよびパッケージ ファイルをホストするためのオプションがサポートされています。
- ThinOS、ThinLinux、および Windows Embedded Standard オペレーティング システムを実行するシン クライアントに導入できる構成がアップデートされています。
- Wyse Device Agent がバージョン 14.4.3.5 にアップデートされています。
- ファイル リポジトリーのサブネット マッピングがサポートされています。

  メモ: サブネット マッピングは、ThinOS 9.0 デバイスではサポートされていません。
- **登録の検証**を有効にするオプション。グループへのシン クライアントの手動/自動登録を管理者は制御できるようになります。
- ThinOS 9.x デバイス用の**選択グループ**を作成するオプション。
- ThinOS 9.x 設定 UI スキーマのアップグレードがサポートされています。

Wyse Management Suite のエディション

Wyse Management Suite は、以下のエディションで利用できます。

- **Standard (無料)** - Wyse Management Suite の Standard Edition はオンプレミス展開でのみ使用できます。Standard Edition を使用するにはライセンスキーは必要ありません。Standard Edition は小規模および中規模のビジネスに適しています。
- **Pro (有料)** - Wyse Management Suite の Pro Edition は、オンプレミスとクラウド展開の両方で利用できます。Pro Edition を使用するにはライセンスキーが必要です。サブスクリプションベースのライセンスを提供します。Pro ソリューションにより、組織はオンプレミスとクラウドとの間でハイブリッド モデルおよびフローティング ライセンスを採用することができます。Pro のオンプレミスのエディションは、小規模、中規模、および大規模企業に適しています。クラウド展開では、Pro Edition を非企業ネットワーク (ホームオフィス、サードパーティ、パートナー、モバイル Thin Client など) で管理することができます。

  メモ: ライセンスは、クラウドとオンプレミスのインストールの間で簡単にフローティングできます。

  Wyse Management Suite の Pro Edition では、以下も提供します。

  - 重要なアラート、通知を表示し、リアルタイムでコマンドを送信するモバイルアプリケーション。
  - ロール ベースの管理に対応する 2 要素識別と Active Directory 認証により強化されたセキュリティ
  - 詳細なアプリポリシーとレポート作成

  メモ: クラウド サービスは米国およびドイツでホストされます。データレジデンシーに制限のある国のお客様は、クラウドのベースのサービスを利用できない場合があります。

Wyse Management Suite のウェブコンソールは国際化をサポートします。ページの右下隅のドロップダウン メニューから、次のいずれかの言語を選択します。

- 英語

- フランス語
- イタリア語
- ドイツ語
- スペイン語
- 中国語
- 日本語

Wyse Management Suite の機能マトリックス

次の表は、各サブスクリプションタイプでサポートされている機能についての情報を提供します。

表 1. 各サブスクリプションタイプの機能マトリックス

機能	Wyse Management Suite Standard	Wyse Management Suite の Pro プライベートクラウド	Wyse Management Suite の Pro クラウドエディション
Thin Client を管理するための拡張性の高いソリューション	最大 10,000 台のデバイスを利用可能	50,000 台以上のデバイス	100 万台以上のデバイス
ライセンスキー	不要	必須	必須
グループベースの管理	√	√	√
複数レベルのグループと継承	√	√	√
ポリシー管理の設定	√	√	√
オペレーティングシステムのパッチおよび画像の管理	√	√	√
継承後のデバイスレベルでの有効な設定の表示	√	√	√
アプリケーションポリシー管理	√	√	√
アセット、インベントリおよびシステム管理	√	√	√
自動デバイス検出	√	√	√
リアルタイムコマンド	√	√	√
スマートスケジューリング	√	√	√
アラート、イベント、および監査のログ	√	√	√
セキュア通信 (HTTPS)	√	√	√
ファイアウォールの内側にあるデバイスの管理	有限 *	有限 *	√
モバイルアプリケーション	X	√	√
電子メールとモバイルアプリケーションを使用したアラート	X	√	√
アプリケーションのインストールをカスタマイズするためのサポートスクリプト	X	√	√
導入を簡素化して再起動を最少にするためのアプリケーションのバンドル	X	√	√

機能	Wyse Management Suite Standard	Wyse Management Suite の Pro プライベートクラウド	Wyse Management Suite の Pro クラウドエディション
委任管理	X	√	√
デバイス属性に基づいた動的グループの作成と割り当て	X	√	√
2 要素認証	√	√	√
役割ベース管理のための Active Directory の認証。	X	√	√
マルチテナント	X	√	√
エンタープライズグレードのレポート	X	√	√
複数リポジトリ	X	√	√
サポートされるプラットフォーム上のハードウェアポートの有効化 / 無効化	X	√	√
サポートされるプラットフォームでの BIOS の設定	X	√	√
ポリシー設定のエクスポートとインポート	X	√	√
アプリケーション ポリシーへのリポジトリー割り当て	X	√	√
シン クライアントのシャットダウン コマンド	√	√	√
Wyse Management Suite コンソールのタイムアウト	X	√	√
ポリシーの順序	X	√	√
オペレーティング システムに応じてアプリケーションの選択を合理化	√	√	√
エイリアスを設定するオプション	X	√	√
サブネット マッピング	√	√	√
一括アップロード	X	√	√
動的スキーマの設定	√	√	√
登録の検証	√	√	√
ThinOS 用の選択グループ	X	√	√

メモ: * は、セキュアなファイアウォール作業環境でのみ、Wyse Management Suite を使用して、デバイスを管理できることを示します。ファイアウォール設定の範囲外では、Thin Client を管理できません。

2

Wyse Management Suite を開始する

このセクションでは、管理者として管理を始められるように、全般的な機能に関して情報を提供します。また、Wyse Management Suite を使用してシン クライアントを管理する方法について説明します。

トピック：

パブリック クラウドでの Wyse Management Suite へのログイン

Wyse Management Suite コンソールにログインするには、お使いのシステムにサポートされている Web ブラウザーがインストールされている必要があります。Wyse Management Suite コンソールにログインするには、次の操作を行います。

1. Wyse Management Suite のパブリッククラウド（SaaS）エディションには、次のいずれかのリンクを使用してアクセスします。
   - **米国データ センター**：us1.wysmanagermentsuite.com/ccm-web
   - **EU データ センター**：eu1.wysmanagermentsuite.com/ccm-web
2. ユーザー名とパスワードを入力します。
3. **サインイン** をクリックします。

メモ: 初めて Wyse Management Suite コンソールにログインしたとき、新しいユーザーが追加された場合またはユーザーライセンスがアップデートされた場合は、契約条件 ページが表示されます。契約条件を読み、それぞれのチェックボックスを選択し、同意する をクリックします。

メモ: www.wysemanagementsuite.com で Wyse Management Suite の試用版に登録するか、サブスクリプションを購入すると、ログイン資格情報を受け取ります。Wyse Management Suite サブスクリプションは、デルの営業チームまたはローカルのデルパートナーから購入できます。詳細については、www.wysemanagementsuite.com を参照してください。

メモ: パブリッククラウド上で Wyse Management Suite の Pro エディションを使用する際は、外部へのアクセスが可能なリポジトリを DMZ 搭載のサーバ上にインストールする必要があります。また、サーバーの完全修飾ドメイン名（FQDN）をパブリック DNS に登録する必要があります。

パスワードの変更

ログインパスワードを変更するには、管理コンソールの右上にあるアカウントのリンクをクリックしてから、**パスワードの変更** をクリックします。

メモ: 初回ログイン後は、パスワードを変更することをお勧めします。追加の管理者のデフォルト ユーザー名およびパスワードは、Wyse Management Suite のアカウント所有者が作成します。

Wyse Management Suite からのログアウト

管理コンソールからログアウトするには、管理コンソールの右上にあるアカウントのリンクをクリックしてから、**サインアウト** をクリックしてください。

Prerequisites to deploy Wyse Management Suite on the private cloud

Table 2. Prerequisites

Description	10,000 devices or less	50,000 devices or less	120,000 devices or less	Wyse Management Suite – Software repository
Operating system	Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 Standard Supported language pack—English, French, Italian, German, Spanish, Japanese, and Chinese (preview release)			
Minimum disk space	40 GB	120 GB	200 GB	120 GB
Minimum memory (RAM)	8 GB	16 GB	32 GB	16 GB
Minimum CPU requirements	4	4	16	4
Network communication ports	The Wyse Management Suite installer adds Transmission Control Protocol (TCP) ports 443, 8080, and 1883 to the firewall exception list. The ports are added to access the Wyse Management Suite console and to send push notifications to the thin clients. • TCP 443—HTTPS communication • TCP 1883—MQTT communication • TCP 3306—MariaDB (optional if remote) • TCP 27017—MongoDB (optional if remote) • TCP 11211—Memcached • TCP 5172, 49159—End-User Management Software Development Kit (EMSDK)—optional and required only to manage Teradici devices The default ports that are used by the installer may be changed to an alternative port during installation.			The Wyse Management Suite repository installer adds TCP ports 443 and 8080 to the firewall exception list. The ports are added to access the operating system images and application images that are managed by Wyse Management Suite.
Supported browsers	Internet Explorer version 11 Google Chrome version 58.0 and later Mozilla Firefox version 52.0 and later Edge browser on Windows—English only			

- The Overlay Optimizer version 1.0 and installation scripts are provided with the Wyse Management Suite Installer. Administrator must run the scripts to enable the Overlay Optimizer to be made available in Wyse Management Suite.
- The Dell Secure Client version 1.0 installation scripts are provided with the Wyse Management Suite Installer. Administrator must run the scripts to enable the Dell Secure Client to be made available in Wyse Management Suite.

NOTE: `WMS.exe` and `WMS_Repo.exe` must be installed on two different servers. You must install the Wyse Management Suite remote repository for the public cloud. For private cloud, you must install the Wyse Management Suite remote repository and local repository. The software can be installed on a physical or a virtual machine. Also, it is not necessary that the software repository and the Wyse Management Suite server have the same operating system.

管理コンソールの機能エリア

Wyse Management Suite コンソールは、以下の機能領域に分かれています。

- **ダッシュボード** ページは、システムの各機能領域における現在の状態に関する情報を提供します。
- **グループ & 構成** ページでは、デバイス設定の階層グループポリシー管理を採用します。オプションで、グローバルグループポリシーのサブグループを作成して、企業の基準に従ってデバイスを分類することができます。たとえば、ジョブ機能、デバイスタイプなどに基づいて、グループ化できます。

- [**ユーザー**] ページでは、Wyse Management Suite にログインするために、ローカル ユーザーおよび Active Directory からインポートされたユーザーに、グローバル管理者、グループ管理者およびビューアの役割を割り当てることができます。ユーザーは、割り当てられた役割に基づいて、操作を実行するための許可が付与されます。
- **デバイス** ページでは、デバイス、デバイスの種類、デバイス固有の設定の表示および管理ができます。
- **アプリとデータ** ページは、デバイスアプリケーション、オペレーティングシステムイメージ、ポリシー、証明書ファイル、ロゴ、および壁紙イメージを管理できます。
- **ルール** ページでは、自動グループ化およびアラート通知などのルールを追加、編集、有効または無効にすることができます。
- [**ジョブ**] ページでは、再起動、LAN 上でのウェイクアップ、および登録したデバイスで展開する必要のあるアプリケーションまたはイメージ ポリシーなどの、タスクのジョブを作成できます。
- **イベント** ページでは、システムのイベントおよびアラートの表示および監査を行うことができます。
- **ポータル管理** ページでは、ローカルリポジトリ設定、ライセンスサブスクリプション、Active Directory の設定、2 要素認証など、さまざまなシステム設定を行えます。

シンクライアントの設定および管理

- **設定の管理** - Wyse Management Suite はグループとサブグループの階層をサポートします。グループは、システム管理者が定義するルールに基づいて手動または自動で作成できます。マーケティング、セールス、エンジニアリングなど、機能の階層に基づいたグループか、または国/地域、都道府県、市町村など、場所の階層に基づいたグループを構成できます。

  メモ: Pro エディションでは、ルールを追加してグループを作成できます。サブネット、タイムゾーン、場所などのデバイスの属性により、デバイスを既存のグループに割り当てることもできます。

  次の設定をすることもできます。

  - デフォルトポリシーグループで設定されたテナントアカウント内のすべてのデバイスに適用する設定。この設定は、すべてのグループとサブグループが継承するパラメータのグローバル設定です。下位のグループで設定された設定は、親または上位のレベルのグループで設定したものより優先されます。

    たとえば、次のとおりです。

    - デフォルトポリシーグループ (親グループ) のポリシーを設定します。ポリシー設定後に、カスタムグループ (子グループ) のポリシーを確認します。同じセットのポリシーが、子グループにも適用されています。デフォルト ポリシー グループの設定はグローバルなパラメーターであり、すべてのグループおよびサブグループが親グループから継承します。
    - カスタムグループに対して、異なる設定を構成します。カスタム グループは両方のペイロードを受信しますが、デフォルトのポリシー グループ内のデバイスについては、カスタム ポリシー グループに設定されたペイロードを受信しません。
    - カスタムグループに対して、異なる設定を構成します。下位のグループで設定された設定は、親または上位のレベルのグループで設定したものより優先されます。
  - **デバイスの詳細** ページから設定可能な特定のデバイスに対する固有の設定下位レベルのグループなどの設定は、上位レベルのグループでの設定よりも優先されます。

  ポリシーを作成して公開したら、設定パラメータは、サブグループを含むグループ内のすべてのデバイスに導入されます。

  ポリシーを公開してデバイスに伝達されると、変更を行うまで、設定がデバイスに再度送られることはありません。登録された新しいデバイスは、登録された先のグループに有効な設定ポリシーを受信します。これには、グローバル グループ、および中レベルのグループから継承されたパラメーターが含まれます。

  設定ポリシーはすぐに公開され、後で実行するようスケジュールすることはできません。ディスプレイ設定など、一部のポリシーの変更については再起動が強制される場合があります。
- **アプリケーションおよびオペレーティングシステムのイメージ導入** - アプリケーションとオペレーティングシステムイメージのアップデートは、**アプリケーションとデータ** タブから導入できます。アプリケーションは、ポリシーグループに基づいて導入されます。

  メモ: 詳細設定のアプリケーションポリシーを使用すると、要件に応じて現在およびすべてのサブグループにアプリケーションを導入することができます。オペレーティングシステムのイメージは現在のグループのみに導入できます。

  Wyse Management Suite は、標準および詳細設定のアプリケーションポリシーをサポートします。標準のアプリケーションポリシーを使用すると、単一アプリケーションパッケージをインストールできます。アプリケーションのインストール中にデバイスが再起動します。各アプリケーションのインストール前およびインストール後、デバイスを再起動します。詳細設定のアプリケーションポリシーを使用すると、複数のアプリケーションパッケージを 2 回再起動するだけでインストールできます。この機能は Pro エディションでのみ使用可能です。詳細設定のアプリケーション ポリシーは、特定のアプリケーションをインストールするのに必要な、インストール前後のスクリプトもサポートします。

  デバイスを Wyse Management Suite で登録する場合、またはデバイスを新しいグループに移動する場合に、標準および詳細設定のアプリケーションポリシーを設定できます。

  アプリケーションポリシーおよびオペレーティングシステムイメージの Thin Client への導入は、すぐに実行するか、またはデバイスのタイムゾーンやその他の指定されたタイムゾーンに基づいてスケジュールを設定できます。

- **デバイスのインベントリ**- このオプションは **デバイス** タブをクリックすると特定できます。デフォルトでは、このオプションは、システムのすべてのデバイスのページ単位リストを表示します。グループまたはサブグループ、デバイスタイプ、オペレーティングシステムタイプ、ステータス、サブネット、およびプラットフォーム、タイムゾーンなど、さまざまなフィルタ条件を使用して、デバイスのサブセットを表示することを選択できます。

  [**デバイスの詳細**] ページを開くには、このページにリストされているデバイスのエントリーをクリックします。デバイスのすべての詳細が表示されます。

  デバイスの詳細 ページには、デバイスに適用可能なすべての設定パラメータの他、各パラメータが適用されるグループのレベルも表示されます。

  このページでは、**デバイスの例外** ボタンを有効にすることで、該当デバイスに特有の設定パラメータを設定することもできます。このセクションで設定したパラメーターは、グループまたはグローバル レベル (またはその両方) で設定されたいずれのパラメーターよりも優先されます。
- **レポート** - 定義済みフィルターに基づいて、レポートを生成および表示することができます。レポートを生成するには、[**ポータル管理**] ページの [**レポート**] タブをクリックします。
- **モバイルアプリケーション** - モバイルアプリケーションを使用するとアラート通知の受信およびデバイスの管理が可能です。**Dell モバイルエージェント** は Android デバイスで利用できます。モバイル アプリケーションおよび『**Dell モバイル エージェント開始ガイド**』をダウンロードするには、[**ポータル管理**] ページの [**アラートと分類**] タブをクリックします。

3

Wyse デバイスエージェントのインストールまたはアップグレード

本項では、Wyse Management Suite を使用して、Windows Embedded Standard、Linux、ThinLinux デバイスなどの Thin Client で Wyse デバイス エージェントをインストールまたはアップグレードする方法についての情報を提供します。

- **Windows Embedded Standard デバイス** - Wyse デバイス エージェント バージョン 1.4.x は、support.dell.com からダウンロードできます。次のいずれかの方法を使用して、Windows Embedded Standard デバイスに Wyse デバイス エージェントをインストールまたはアップグレードすることができます。
  - Wyse デバイスエージェントを手動でインストール
  - Wyse Management Suite アプリケーションポリシーの使用による Wyse デバイスエージェントのアップグレード

  メモ: 最新バージョンの Wyse デバイス エージェントの.exe ファイルをダブル クリックして、Wyse デバイス エージェントを手動でアップグレードすることもできます。

  メモ: Wyse Device Agent は、KB3033929 が使用可能な場合にのみ、Windows Embedded Standard 7 オペレーティング システムにインストールできます。
- **Linux および ThinLinux デバイス** - Wyse デバイスエージェントは、Wyse Management Suite を使用して Linux および ThinLinux デバイスでインストールまたは アップグレードできます。詳細については、「ThinLinux 上および Linux クライアントでの Wyse デバイスエージェントのインストールまたはアップグレード」を参照してください。

トピック：

- Windows Embedded デバイスへの Wyse デバイス エージェントの手動インストール
- Wyse Management Suite アプリケーションポリシーの使用による Wyse デバイスエージェントのアップグレード
- ThinLinux 上および Linux クライアントでの Wyse デバイスエージェントのインストールまたはアップグレード

Windows Embedded デバイスへの Wyse デバイス エージェントの手動インストール

このタスクについて

Wyse デバイス エージェントを Windows Embedded デバイスに手動でインストールするには、次の操作を行います。

手順

1. `WDA.exe` ファイルを Thin Client にコピーします。
2. `WAD.exe` ファイルをダブルクリックします。
3. **はい** をクリックします。

   メモ: 古いバージョンの Wyse デバイスエージェントまたは HAgent がデバイス上にインストールされている場合に警告メッセージが表示されます。
4. **グループのトークン** フィールドで、グループトークンを入力します。これはオプションのフィールドです。
   このステップを省略するには、**次へ** をクリックします。Wyse デバイスエージェントのユーザーインタフェースに、グループトークンの詳細を後で入力することができます。
5. **リージョン** ドロップダウンリストから、Wyse Management Suite のパブリッククラウドサーバの地域を選択します。
   インストールが正常に行われると、Wyse Management Suite のパブリッククラウドサーバは、Wyse Management Suite コンソールに自動的にデバイスを登録します。

Wyse Management Suite アプリケーションポリシーの使用による Wyse デバイスエージェントのアップグレード

前提条件

Wyse デバイス エージェントのアップグレードには、Wyse Management Suite アプリケーションを使用することが推奨されます。Wyse Management Suite のプライベートクラウドのセットアップでは、Windows Embedded Standard 用の最新の Wyse デバイスエージェントパッケージがローカルリポジトリで使用できます。パブリック クラウド、またはプライベート クラウド上のリモート リポジトリーを使用している場合は、`WDA.exe` ファイルをリポジトリー内の `thinClientApps` フォルダーにコピーします。

手順

1. `WDA.exe` ファイルをリポジトリーにコピーした後、[**アプリとデータ**] に移動し、このパッケージを使用して標準アプリケーション ポリシーを作成します。「Thin Client に対する標準アプリケーション ポリシーの作成および導入」を参照してください。

   メモ: 高度なアプリケーションポリシーは、Wyse デバイスエージェント 14.x 以降のみでサポートされています。14.x から Wyse デバイス エージェントをアップグレードするときには、標準のアプリケーション ポリシーを使用することが推奨されます。Wyse デバイスエージェントを 14.x から最新のバージョンにアップグレードするために高度なアプリケーションポリシーを使用することもできます。

2. [**ジョブ**] ページに移動し、Wyse デバイス エージェントをアップグレードするジョブをスケジュールします。

   メモ: Windows Embedded Standard Wyse デバイス エージェントをバージョン 13.x からバージョン 14.x にアップグレードする場合、リポジトリー プロトコルとして HTTP を使用することが推奨されます。

   インストールに成功した後、ステータスがサーバに送信されます。

ThinLinux 上および Linux クライアントでの Wyse デバイスエージェントのインストールまたはアップグレード

前提条件

- ThinLinux バージョン 2.0、イメージ バージョン 2.0.14、Wyse デバイス エージェント バージョン 3.0.7 で、Wyse デバイス エージェントを Dell Wyse 3040 Thin Client にインストールするには、`wda3040_3.0.10-01_amd64.deb` ファイルをインストールして、次に `wda_3.2.12-01_amd64.tar` ファイルをインストールする必要があります。
- Linux Thin Client 用に、プラットフォーム ユーティリティー アドオンと Wyse デバイス エージェント アドオンをインストールする必要があります。ThinLinux Thin Client 用に `wda_x.x.x.tar` ファイルをインストールできます。

このタスクについて

次のオプションのいずれかを使用して、アドオンをインストールまたは実行することができます

- INI パラメータの使用
- アドオンマネージャ
- RPM コマンド

手順

1. パブリッククラウド、またはプライベートクラウド上でリモートリポジトリを使用している場合は、RPM ファイルを、`thinClientApps` フォルダにコピーします。デフォルトでは、Linux および ThinLinux クライアントの最新の Wyse デバイス エージェントとプラットフォーム ユーティリティー RPM は、ローカル リポジトリーで使用できます。
2. **ジョブ** ページに進み、ジョブをスケジュールしてプラットフォームのユーティリティのアドオンをアップグレードします。
   プラットフォームユーティリティのアドオンが Thin Client で正常にインストールされるまで待機する必要があります。

メモ: プラットフォームのアドオンを先にインストールしてから、Wyse デバイスエージェントのアドオンをインストールします。最新の Wyse デバイスエージェントは、最新のプラットフォームユーティリティのアドオンをインストールしてからインストールする必要があります。

3. ジョブ ページで、ジョブをスケジュールして、クライアントの Wyse デバイスエージェントをアップグレードします。

メモ: Linux クライアントは、Wyse デバイス エージェントのアドオン バージョン 2.0.11 をインストールした後に再起動します。

4

Wyse Management Suite を使用した新しいデバイスの登録と設定

Wyse Management Suite を使用した新しい Windows Embedded Standard デバイスの登録と設定

手順

1. シン クライアントへの Wyse デバイス エージェントのインストール - 「Wyse デバイス エージェントのインストールまたはアップグレード」を参照してください。
2. Wyse Management Suite へのシン クライアントの登録 - 「Wyse Device Agent を使用した Windows Embedded Standard Thin Client の Wyse Management Suite への登録」を参照してください。

   メモ: また次のいずれかの方法でデバイスを登録できます。

   - **DHCP オプション タグの使用 - 「DHCP オプション タグの使用によるデバイスの登録」を参照してください。**
   - **DNS SRV レコードの使用 - 「DNS SRV レコードの使用によるデバイスの登録」を参照してください。**

   メモ: [登録の検証] オプションが有効になっている場合、手動または自動検出されたデバイスは、[デバイス] ページで [登録の検証保留中] 状態になります。テナントは、[デバイス] ページで 1 台または複数のデバイスを選択して、登録を検証することができます。デバイスは検証された後、目的のグループに移動されます。デバイスの検証方法の詳細については、「登録の検証」を参照してください。
3. 目的のグループにデバイスを追加します (オプション)。「グループ管理および設定」を参照してください。
4. 次のいずれかのオプションを使用して、Thin Client を設定します。
   - [**グループと設定**] ページの使用 - 「Windows Embedded Standard ポリシー設定の編集」を参照してください。
   - [**デバイス**] ページの使用 - 「デバイスの管理」を参照してください。

Wyse Management Suite を使用した新しい ThinOS 8.x デバイスの登録と設定

手順

1. Thin Client のデスクトップのメニューから、**[システム セットアップ]** > **[一元設定]** の順に移動します。
   一元設定 ウィンドウが表示されます。
2. 管理者が対象グループに対して設定した **グループ登録キー** を入力します。
3. [**WMS の詳細設定の有効化**] チェック ボックスを選択します。
4. [**WMS サーバー**] フィールドに、Wyse Management Server の URL を入力します。
5. ライセンスのタイプに基づき、CA 検証を有効または無効にします。パブリック クラウドの場合、[**CA 検証を有効にする**] チェック ボックスを選択します。プライベート クラウドの場合、Wyse Management Suite サーバーに既知の認証局の証明書をインポート済みであれば、[**CA 検証を有効にする**] チェック ボックスを選択します。

   プライベートクラウドで CA 検証オプションを有効にするには、同じ自己署名証明書を ThinOS デバイスにもインストールする必要があります。自己署名証明書を ThinOS デバイスにインストールしていない場合は、[**CA 検証を有効にする**] チェック ボックスを選択しないでください。登録後に、Wyse Management Suite を使用して証明書をデバイスにインストールしてから、CA 検証オプションを有効にしてください。
6. 設定を確認するには、**キーの検証** クリックします。

メモ: キーが検証されない場合は、入力したグループキーと WMS サーバの URL を確認してください。記載されたポートがネットワークでブロックされていないことを確認します。デフォルト ポートは 443 と 1883 です。

7. OK をクリックします。

メモ: [登録の検証] オプションが有効になっている場合、手動または自動検出されたデバイスは、[デバイス] ページで [登録の検証保留中] 状態になります。テナントは、[デバイス] ページで 1 台または複数のデバイスを選択して、登録を検証することができます。デバイスは検証された後、目的のグループに移動されます。デバイスの検証方法の詳細については、「登録の検証」を参照してください。

デバイスが、Wyse Management Suite に登録されました。

8. Wyse Management Suite にログインします。
9. 目的のグループにデバイスを追加します (オプション)。「グループ管理および設定」を参照してください。
10. 次のいずれかのオプションを使用して、Thin Client を設定します。
    - [グループと設定] ページの使用 -「ThinOS ポリシー設定の編集」を参照してください。
    - [デバイス] ページの使用 -「デバイスの管理」を参照してください。

Wyse Management Suite を使用した新しい ThinOS 9.x デバイスの登録と設定

手順

1. Thin Client のデスクトップのメニューから、[システム セットアップ] > [一元設定] の順に移動します。
   一元設定 ウィンドウが表示されます。
2. 管理者が対象グループに対して設定した**グループ登録キー**を入力します。
3. [**WMS の詳細設定の有効化**] チェック ボックスを選択します。
4. [**WMS サーバー**] フィールドに、Wyse Management Server の URL を入力します。
5. ライセンスのタイプに基づき、CA 検証を有効または無効にします。パブリッククラウドの場合、**CA 検証を有効にする** チェックボックスを選択してください。プライベートクラウドの場合、周知の認証局から Wyse Management Suite サーバに証明書をインポート済みであれば、**CA 検証を有効にする** チェックボックスを選択してください。

   プライベートクラウドで CA 検証オプションを有効にするには、同じ自己署名証明書を ThinOS デバイスにもインストールする必要があります。自己署名証明書を ThinOS デバイスにインストールしていない場合は、[**CA 検証を有効にする**] チェック ボックスを選択しないでください。登録後に、Wyse Management Suite を使用して証明書をデバイスにインストールしてから、CA 検証オプションを有効にしてください。
6. 設定を確認するには、**キーの検証** クリックします。

メモ: キーが検証されない場合は、入力したグループキーと WMS サーバの URL を確認してください。記載されたポートがネットワークでブロックされていないことを確認します。デフォルト ポートは 443 と 1883 です。

アラートウィンドウが表示されます。

7. OK をクリックします。
8. [一元設定] ウィンドウで [OK] をクリックします。

メモ: また次のいずれかの方法でデバイスを登録できます。

- DHCP オプション タグの使用 -「DHCP オプション タグの使用によるデバイスの登録」を参照してください。
- DNS SRV レコードの使用 -「DNS SRV レコードの使用によるデバイスの登録」を参照してください。

メモ: [登録の検証] オプションが有効になっている場合、手動または自動検出されたデバイスは、[デバイス] ページで [登録の検証保留中] 状態になります。テナントは、[デバイス] ページで 1 台または複数のデバイスを選択して、登録を検証することができます。デバイスは検証された後、目的のグループに移動されます。デバイスの検証方法の詳細については、「登録の検証」を参照してください。

デバイスが、Wyse Management Suite に登録されました。

9. Wyse Management Suite にログインします。
10. 目的のグループにデバイスを追加します (オプション)。「グループ管理および設定」を参照してください。
11. 次のいずれかのオプションを使用して、Thin Client を設定します。
    - [グループと設定] ページの使用 -「ThinOS 9.x ポリシー設定の編集」を参照してください。
    - [デバイス] ページの使用 -「デバイスの管理」を参照してください。

Wyse Management Suite を使用した新しい Linux または ThinLinux デバイスの登録と設定

手順

1. シン クライアントへの Wyse デバイス エージェントのインストール - 「Wyse デバイス エージェントのインストールまたはアップグレード」を参照してください。
2. Wyse Management Suite へのシン クライアントの登録 - 「Wyse デバイス エージェントを使用した Linux/ThinLinux シン クライアントの Wyse Management Suite への登録」を参照してください。

   メモ: また次のいずれかの方法でデバイスを登録できます。

   - **DHCP オプション タグの使用 - 「DHCP オプション タグの使用によるデバイスの登録」を参照してください。**
   - **DNS SRV レコードの使用 - 「DNS SRV レコードの使用によるデバイスの登録」を参照してください。**

   メモ: [登録の検証] オプションが有効になっている場合、手動または自動検出されたデバイスは、[デバイス] ページで [登録の検証保留中] 状態になります。テナントは、[デバイス] ページで 1 台または複数のデバイスを選択して、登録を検証することができます。デバイスは検証された後、目的のグループに移動されます。デバイスの検証方法の詳細については、「登録の検証」を参照してください。
3. 目的のグループにデバイスを追加します (オプション)。「グループ管理および設定」を参照してください。
4. 次のいずれかのオプションを使用して、Thin Client を設定します。
   - [**グループと設定**] ページの使用 - 「ThinLinux ポリシー設定の編集」または「Linux ポリシー設定の編集」を参照してください。
   - [**デバイス**] ページの使用 - 「デバイスの管理」を参照してください。

Wyse Management Suite を使用した新しい Wyse Software Thin Client の登録と設定

手順

1. シン クライアントへの Wyse デバイス エージェントのインストール - 「Wyse デバイス エージェントのインストールまたはアップグレード」を参照してください。
2. Wyse Management Suite へのシン クライアントの登録 - 「Wyse デバイスエージェントを使用した Wyse Software Thin Client の Wyse Management Suite への登録」を参照してください。

   メモ: また次のいずれかの方法でデバイスを登録できます。

   - **DHCP オプション タグの使用 - 「DHCP オプション タグの使用によるデバイスの登録」を参照してください。**
   - **DNS SRV レコードの使用 - 「DNS SRV レコードの使用によるデバイスの登録」を参照してください。**

   メモ: [登録の検証] オプションが有効になっている場合、手動または自動検出されたデバイスは、[デバイス] ページで [登録の検証保留中] 状態になります。テナントは、[デバイス] ページで 1 台または複数のデバイスを選択して、登録を検証することができます。デバイスは検証された後、目的のグループに移動されます。デバイスの検証方法の詳細については、「登録の検証」を参照してください。
3. 目的のグループにデバイスを追加します (オプション)。「グループ管理および設定」を参照してください。
4. 次のいずれかのオプションを使用して、Thin Client を設定します。
   - [**グループと設定**] ページの使用 - 「Wyse Software Thin Client ポリシー設定の編集」を参照してください。
   - [**デバイス**] ページの使用 - 「デバイスの管理」を参照してください。

5

Wyse Management Suite ダッシュボード

ダッシュボード ページでは、システムのステータスおよびシステム内で実行された最近のタスクを見ることができます。特定のアラートを表示するには、**アラート** セクションのリンクをクリックします。[**ダッシュボード**] ページでは、デバイスの概要も表示できます。

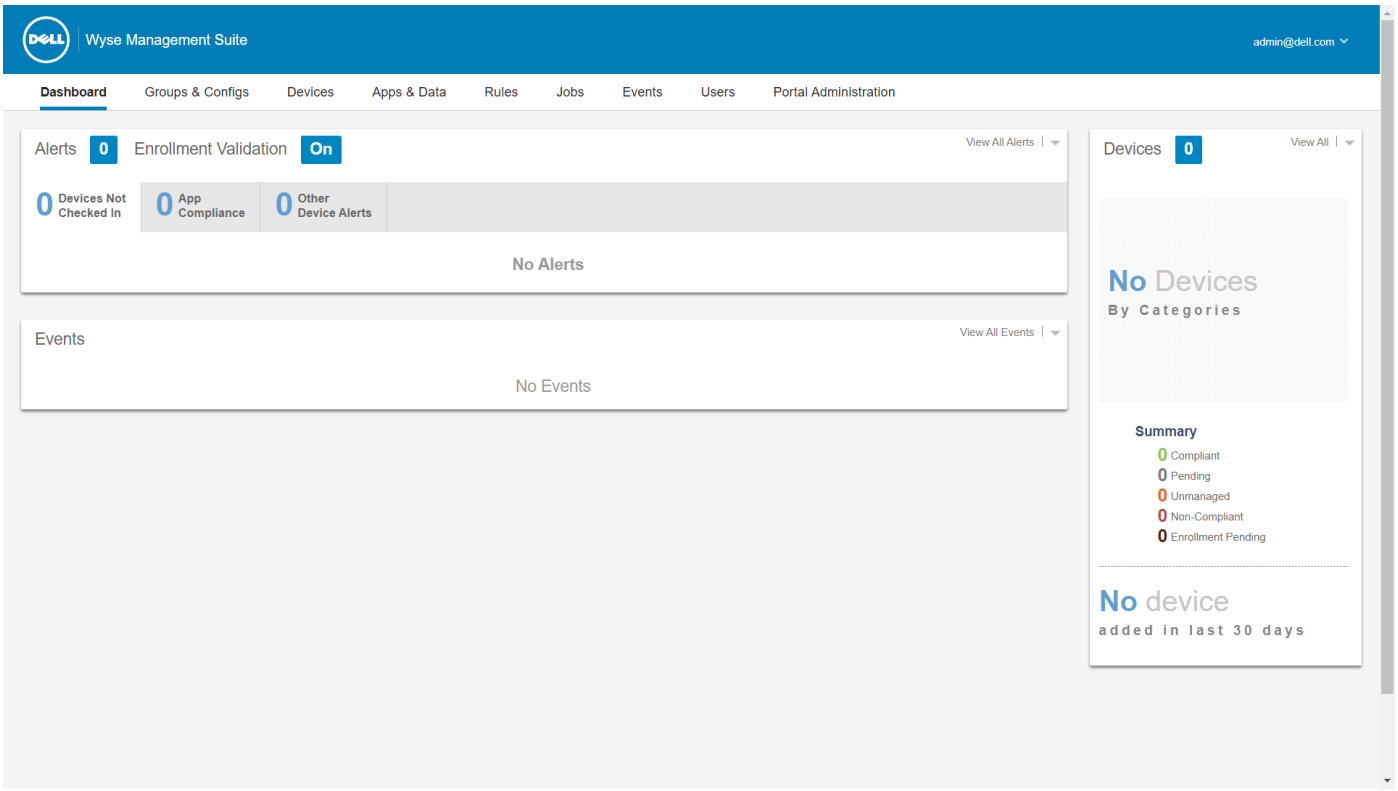


図 1. ダッシュボード

トピック：

- アラートの表示
- イベントリストの表示
- デバイスステータスの表示
- 登録の検証を有効にする
- ユーザープリファレンスの変更
- オンラインヘルプへのアクセス
- パスワードの変更
- 管理コンソールからのログアウト

アラートの表示

アラート セクションには、すべてのアラートの概要が表示されます。

手順

1. **ダッシュボード** をクリックします。
   アラートの概要が表示されます。
2. **すべてのアラートを表示** をクリックします。

次の属性が [**イベント**] ページに表示されます。

- **デバイスはチェックインしていません**
- **アプリのコンプライアンス**
- **その他のデバイスアラート**

イベントリストの表示

イベント セクションには、最近数日内に発生したイベントの概要が表示されます。

手順

1. **ダッシュボード** をクリックします。
   インポートの概要が表示されます。
2. **すべてのイベントを表示** をクリックします。
   イベント ページが開いて、すべてのイベントのリストが表示されます。

デバイスステータスの表示

[**表示**] セクションには、デバイス ステータスの概要が表示されます。

手順

1. **ダッシュボード** をクリックします。
   デバイスの概要が表示されます。
2. **すべてを表示する** をクリックします。
   デバイス ページに、登録済みのすべてのデバイスのリストが表示されます。**概要** セクションには、次のデバイスステータスカテゴリに基づいたデバイスの数が表示されます。
   - **準拠**
   - **保留中**
   - **管理対象外**
   - **非準拠**
   - **登録保留中**

登録の検証を有効にする

[**登録の検証**] を有効にすると、グループへのシン クライアントの手動/自動登録を管理者が制御できるようになります。

手順

1. **ダッシュボード** をクリックします。
2. [**登録の検証**] オプションの横にある [**オン/オフ**] ボタンをクリックします。
   [**ポータル管理**] ページの [**その他の設定**] オプションにリダイレクトされます。
3. [**登録の検証**] オプションを有効または無効にします。

ユーザープリファレンスの変更

アラート通知、ポリシー設定、ページ サイズなどのユーザー プリファレンスを変更できます。

手順

1. **ダッシュボード** ページの右上隅にある ログイン ドロップダウンメニューをクリックします。
2. **ユーザープリファランス** をクリックします。
   ユーザープリファレンス ウィンドウが表示されます。
3. **アラート** をクリックし、電子メールおよびモバイルアプリケーションからの通知にアラートタイプ (重要、警告、情報) を割り当てるために適切なチェックボックスを選択します。
4. **ポリシー** をクリックして、**ThinOS ウィザードモードを使用するかどうかを確認する** チェックボックスを選択すると、ThinOS ポリシーを設定するたびに、**ThinOS 設定モードの選択** ウィンドウが表示されます。

5. **ページサイズ** をクリックし、**ページあたりの項目数** テキストボックスに 10 ~ 100 の数字を入力します。このオプションを使用すると、各ページに表示される項目数を設定できます。

オンラインヘルプへのアクセス

手順

1. **ダッシュボード** ページの右上隅にある ログイン ドロップダウンメニューをクリックします。
2. **WMS ヘルプ** をクリックします。
   Wyse Management Suite のサポート ページが表示されます。

パスワードの変更

手順

1. **ダッシュボード** ページの右上隅にある ログイン ドロップダウンメニューをクリックします。
2. **パスワードの変更** をクリックします。
   パスワードの変更 ウィンドウが表示されます。
3. 現在のパスワードを入力します。
4. 新しいパスワードを入力します。
5. 確認のために新しいパスワードを再入力します。
6. **パスワードの変更** をクリックします。

管理コンソールからのログアウト

手順

1. **ダッシュボード** ページの右上隅にある ログイン ドロップダウンメニューをクリックします。
2. **サインアウト** をクリックします。

6

グループ管理および設定

グループ & 設定 ページでは、デバイスの設定に必要なポリシーを定義できます。グローバルグループポリシーのサブグループを作成し、要件に応じてデバイスを分類できます。たとえば、ジョブ機能やデバイスタイプなどに基づいてデバイスをグループ化できます。

各グループについて、次のオペレーティングシステム用のポリシーを定義できます。

- **ThinOS**
  - **ThinOS**
  - **ThinOS 9.x**
- **WES**
- **Linux**
- **ThinLinux**
- **Teradici**
- **Wyse Software Thin Client**

デバイスは、作成された順序でポリシーを継承します。デフォルト ポリシー グループで指定された設定が、デフォルト ポリシー グループに記載されたすべてのポリシーのデフォルト設定として適用されます。グループでは、そのグループに存在するすべてのデバイスに、デフォルト設定としてデフォルト ポリシー グループがあります。

デバイスの詳細 ページで、グループ内のデバイスのグループの例外を作成し、グループのデフォルトとは異なるポリシーのサブセットを用意することができます。

設定されている場所の詳細および特定のアセットの設定（グローバル、グループ、およびデバイスレベル）はページに表示されます。例外を作成するオプションはこのページで利用できます。**例外** 設定は、選択したデバイスにのみ適用されます。

メモ:

下位レベルのポリシーを変更すると、箇条書きの記号がポリシーの横に表示されます。この記号は、ポリシーが、上位レベルのポリシーをオーバーライドすることを示します。たとえば、システムの個人設定、ネットワーキング、セキュリティ などです。ポリシーを変更する場合は、アスタリスク（*）がポリシーの横に表示されます。この記号は、未保存または未発行の変更があることを示します。発行する前にこの変更を確認するには、保留中の変更の表示 リンクをクリックします。

ポリシーの設定が異なるレベルの間で優先される必要がある場合、最下位レベルのポリシーが優先されます。

ポリシーの設定後、Thin Client に変更が通知されます。変更は、Thin Client の設定後すぐに反映されます。

メモ: Windows Embedded Standard の BIOS 設定などの特定の設定では、変更を有効にするには再起動が必要です。ただし、ThinOS のほとんどの設定では、変更を反映させるのにデバイスを再起動する必要があります。

ポリシーは、次の優先順位で実行されます。

- グローバル
- グループ
- デバイス

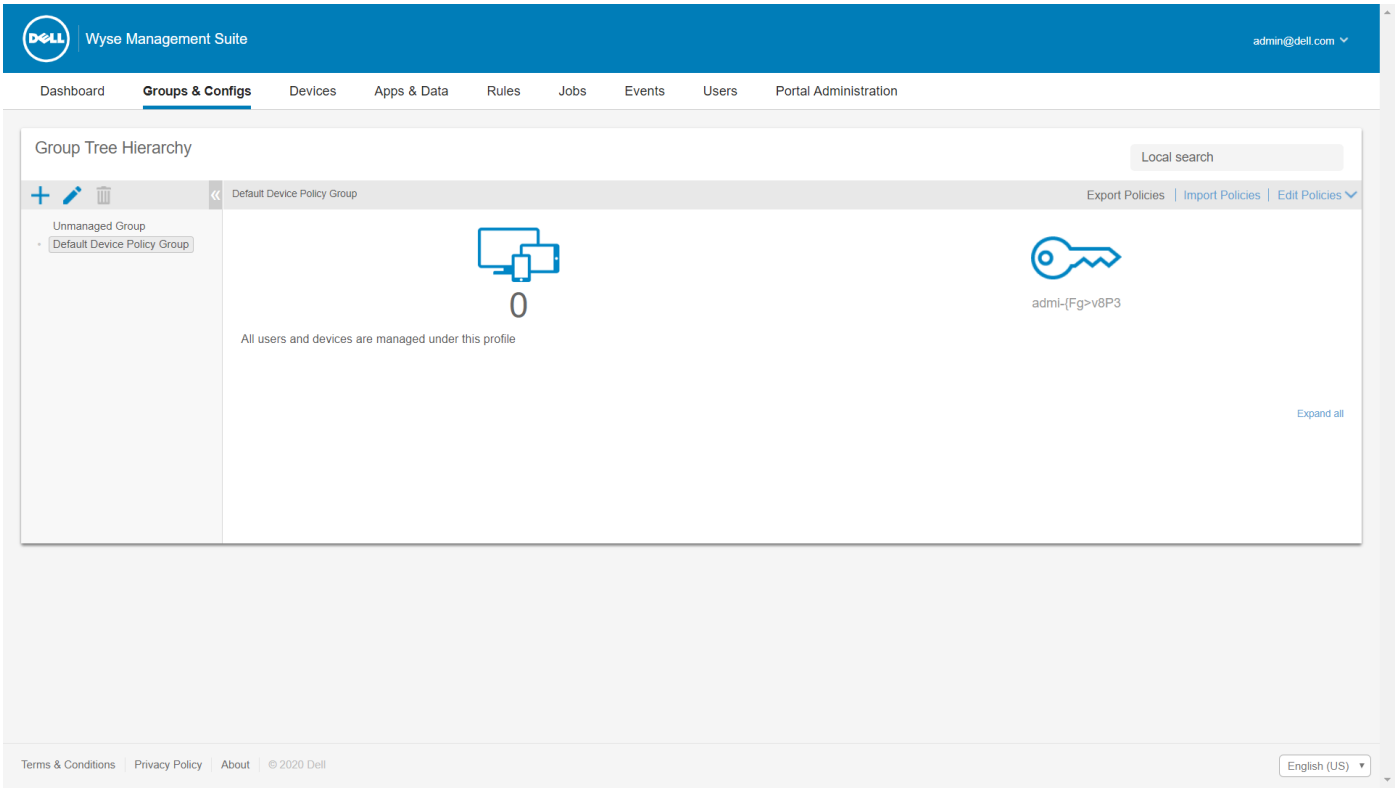


図 2. グループと設定

トピック：

- デフォルトのデバイス ポリシー グループの作成
- 管理対象外グループの編集
- グループの削除
- ThinOS 選択グループの削除
- グローバルレベルポリシーの設定
- グループレベルポリシーの設定
- デバイスレベルのポリシーの設定
- グループ ポリシーのエクスポート
- グループ ポリシーのインポート
- ThinOS ポリシー設定の編集
- ThinOS 9.x ポリシー設定の編集
- Windows Embedded Standard ポリシー設定の編集
- Linux ポリシー設定の編集
- ThinLinux ポリシー設定の編集
- Wyse Software Thin Client ポリシー設定の編集
- Cloud Connect のポリシー設定の編集

デフォルトのデバイス ポリシー グループの作成

グローバル デバイス グループ ポリシーのグループを作成し、要件に応じてデバイスを分類できます。

手順

1. [**グループ&設定**] ページで、[**デフォルト デバイス ポリシー グループ**] オプションをクリックします。
2. ＋をクリックします。
3. [**新規グループの追加**] ダイアログ ボックスで、**グループ名**と**説明**を入力します。

メモ: **ThinOS デバイスの親選択グループを作成するには、[これは ThinOS 選択グループの親です] オプションを選択します。詳細については、「ThinOS 選択グループの作成」を参照してください。**

4. **登録** タブで、グループトークン の下の **有効** チェックボックスをオンにします。
5. グループトークンを入力します。
6. [**管理**] タブで、このグループの管理を担当しているグループ管理者の名前を選択します。**使用可能なグループ管理者** ボックスでグループを選択し、右矢印をクリックして **割り当てられたグループ管理者** ボックスに移動します。[**割り当てられたグループ管理者**] から [**使用可能なグループ管理者**] に 1 つのグループを移動する場合は、その逆を実行します。このステップはオプションです。
7. **保存** をクリックします。

   グループ & 設定 ページに利用できるグループのリストが追加されます。

   メモ: **各グループの [グループと設定] ページで利用可能なグループ トークンを入力すると、グループにデバイスを登録できます。**

ThinOS 選択グループの作成

手順

1. [**グループ&設定**] ページで、[**デフォルト ポリシー グループ**] オプションをクリックします。
2. ＋をクリックします。
3. [**新規グループの追加**] ダイアログ ボックスで、**グループ名**と**説明**を入力します。
4. [**これは ThinOS 選択グループの親です**] オプションを選択します。
5. このグループの管理を担当するグループ管理者の名前を選択します。**使用可能なグループ管理者** ボックスでグループを選択し、右矢印をクリックして **割り当てられたグループ管理者** ボックスに移動します。[**割り当てられたグループ管理者**] から [**使用可能なグループ管理者**] に 1 つのグループを移動する場合は、その逆を実行します。このステップはオプションです。
6. **保存** をクリックします。

   グループ & 設定 ページに利用できるグループのリストが追加されます。

   作成した親グループにサブ グループを追加するには、[**グループ&設定**] ページで親グループをクリックし、「デバイス ポリシー グループの作成」で説明されている手順に従います。

   メモ: **親選択グループの下には、10 個の子選択グループを作成でき、デバイスを子選択グループに登録できます。**

   メモ: **他のオペレーティング システムに対して、プロファイルを設定できます。作成されたプロファイルは、他のカスタム グループと同じです。**

ThinOS 選択グループの編集

手順

1. [**グループ&設定**] ページに移動して、編集する ThinOS 選択グループをクリックします。
2. 鉛筆をクリックします。
3. **デフォルトポリシーグループの編集** ダイアログボックスで、**グループ名** や **説明** などを編集します。
4. [**管理**] タブで、このグループの管理を担当しているグループ管理者の名前を選択します。**使用可能なグループ管理者** ボックスでグループを選択し、右矢印をクリックして **割り当てられたグループ管理者** ボックスに移動します。[**割り当てられたグループ管理者**] から [**使用可能なグループ管理者**] に 1 つのグループを移動する場合は、その逆を実行します。このステップはオプションです。
5. **保存** をクリックします。

デフォルト ポリシー グループの編集

手順

1. [**グループ&設定**] ページに移動し、デフォルト ポリシー グループを選択します。

2. をクリックします。
3. **デフォルトポリシーグループの編集** ダイアログボックスで、**グループ名** や **説明** などを編集します。
4. [**登録**] タブで、グループ トークンを編集します。

   メモ: デバイス登録画面で利用可能なグループトークンを入力すると、グループにデバイスを登録できます。
5. **保存** をクリックします。

管理対象外グループの編集

管理対象外グループに属するデバイスは、ライセンスを使用せず、また設定またはアプリケーションベースのポリシーを受け取りません。管理対象外グループにデバイスを追加するには、自動登録または手動デバイス登録の一部として管理対象外グループのデバイス登録キーを使用します。

手順

1. [**グループ&設定**] ページで、[**管理対象外グループ**] を選択します。
2. をクリックします。
   管理対象外グループの編集 ページが表示されます。**グループ名** にグループの名前が表示されます。
3. 次の詳細を編集します。
   - **説明** - グループの簡単な説明です。
   - **グループ トークン** - グループ トークンを有効にするには、このオプションを選択します。
4. **保存** をクリックします。

   メモ: パブリッククラウドの場合、デバイスを登録するには、管理対象外グループのグループトークンを有効にする必要があります。プライベートクラウドの場合、管理対象外グループのグループトークンは自動的に有効にされます。

グループの削除

管理者は、グループ階層からグループを削除できます。

手順

1. [**グループ&設定**] ページで、削除するグループを選択します。
2. をクリックします。
   このアクションにより、グループツリー階層から 1 つまたは複数のグループが削除されることを示す警告メッセージが表示されます。
3. ドロップダウン リストから、現在のグループ内でデバイスの新しいグループを選択します。
4. **グループの追加** をクリックします。

   メモ: グループ階層からグループを削除すると、削除したグループに属するすべてのデバイスは、選択したグループに移動します。

ThinOS 選択グループの削除

管理者は、グループ階層からグループを削除できます。

手順

1. [**グループ&設定**] ページで、削除する ThinOS 選択グループを選択します。
2. をクリックします。
   このアクションにより、グループツリー階層から 1 つまたは複数のグループが削除されることを示す警告メッセージが表示されます。
3. ドロップダウン リストから、現在のグループ内のユーザーおよびデバイスの新しいグループを選択します。
4. **グループの追加** をクリックします。

メモ: グループ階層からグループを削除すると、削除したグループに属するすべてのユーザーとデバイスが、カスタム、デフォルト、または管理対象外のグループに移動します。

メモ: 選択グループを削除すると、削除されたグループのデバイスを別の選択グループに移動することはできません。

グローバルレベルポリシーの設定

手順

1. **グループ & 設定** ページの **ポリシーの編集** ドロップダウンメニューから、デバイスタイプを選択します。
   各デバイスタイプのポリシー設定が表示されます。
2. 設定したいポリシー設定項目を選択し、[**この項目を設定する**] をクリックします。
3. オプションの設定後、**保存して公開** をクリックします。

グループレベルポリシーの設定

グループ レベル ポリシーまたはマルチレベル グループ ポリシーを設定できます。

手順

1. **グループ & 設定** ページで、ポリシーを設定したいグループに移動し、**ポリシーの編集** をクリックします。
2. ドロップダウンメニューから、設定するデバイスタイプを選択します。
   デバイスタイプのポリシー設定が表示されます。
3. ポリシー設定を選択し、**この項目を設定する** をクリックします。
4. **保存して公開** をクリックします。

デバイスレベルのポリシーの設定

手順

1. **デバイス** ページから、設定するデバイスをクリックします。
   デバイスの詳細 ページが表示されます。
2. **デバイス設定** セクションで、**例外の作成 / 編集** をクリックします。

グループ ポリシーのエクスポート

[**ポリシーのエクスポート**] オプションを使用すると、現在のグループからポリシーをエクスポートできます。このオプションは Wyse Management Suite Pro ライセンス ユーザーが使用できます。

手順

1. [**グループ & 設定**] ページで、ポリシーのエクスポート元となるグループを選択します。グループにポリシーが設定されている必要があります。
2. [**ポリシーのエクスポート**] をクリックします。
   [**ポリシーのエクスポート**] 画面が表示されます。
3. エクスポートするデバイス タイプ ポリシーを選択します。
   次のオプションが利用可能です。
   - すべてのデバイス タイプ ポリシー : すべてのデバイス タイプ ポリシーがエクスポートされます。
   - 特定のデバイス タイプ ポリシー : ドロップダウン リストから 1 つまたは複数のデバイス タイプを選択します。選択したデバイス タイプ ポリシーのみがエクスポートされます。
4. **[はい]** ボタンをクリックして、選択したデバイス タイプ ポリシーをエクスポートします。
   親グループ ポリシーはエクスポートされません。選択したグループ レベルまたはターゲット グループ レベルで設定されているポリシーのみがエクスポートされます。
5. ダウンロード リンクをクリックするか、ファイルを右クリックし、[**名前を付けて保存**] をクリックして JSON ファイルを保存します。

メモ: パスワードは、エクスポートしたファイルで暗号化されます。ファイル名は [Group Name]-[ALL]-[Exported Date & Time]UTC.json の形式です。

グループ ポリシーのインポート

[**ポリシーのインポート**] オプションでは、ポリシーをインポートできます。このオプションは Wyse Management Suite Pro ライセンス ユーザーが使用できます。グループ ポリシーは、[**グループ&設定**] ページまたは [**ポリシーの編集**] ページからインポートできます。

[グループと設定] ページからのグループ ポリシーのインポート

手順

1. [**グループ&設定**] ページで、希望のグループを選択します。
   宛先グループに、インポートされたポリシーと同じデバイス タイプのポリシーが含まれている場合、それらは削除され、新しいポリシーが追加されます。
2. [**ポリシーのインポート**] をクリックします。
   [**ポリシーのインポート ウィザード**] 画面が表示されます。
3. 選択したグループからグループ ポリシーをインポートするモードを選択します。
   次のオプションが利用可能です。
   - 既存のグループから: ドロップダウン リストからグループを選択します。そのグループのポリシーが現在のグループにコピーされます。
   - エクスポートされたファイルから: .json ファイルを参照します。そのファイルのポリシーが現在のグループにコピーされます。
4. **次へ** をクリックします。
5. インポートするデバイス タイプの設定を選択します。
   次のオプションが利用可能です。
   - すべてのデバイス タイプ ポリシー: 設定されたすべてのデバイス タイプ ポリシーが現在のグループにインポートされます。
   - 特定のデバイス タイプ ポリシー: ドロップダウン リストから 1 つまたは複数のデバイス タイプを選択します。選択したデバイス タイプ ポリシーのみが現在のグループにインポートされます。
6. **次へ** をクリックします。
   選択したグループ内のポリシーのプレビューが表示されます。
7. **次へ** をクリックします。
   インポート プロセスの概要が表示されます。次のタイプの警告が表示されます。
   - **インポートされた<オペレーティング システム タイプ>ポリシーは、グループ<グループ名>に適用されます**: これは、オペレーティング システムの設定を含まないグループに同設定をインポートしている場合に表示されます。
   - **<オペレーティング システム タイプ>ポリシーは<グループ名>グループに対してすでに存在します。既存の<オペレーティング システム タイプ>ポリシーは削除されます。ポリシーが適用されます**: オペレーティング システム タイプの設定を含むグループに新しいオペレーティング システム タイプの設定をインポートする場合に表示されます。
   - **インベントリー ファイルへの依存関係を含むファイルからポリシーをインポートすると失敗します。このインポートを許可するには、[ポリシーの編集] ウィンドウからインポート オプションを使用します**: インベントリー ファイルへの参照を含むファイルからデバイス タイプの設定をインポートする場合に表示されます。
8. **インポート** をクリックします。

   メモ: **選択しているデバイス タイプの設定のみをインポートできます。選択したデバイス タイプのターゲット グループに定義されているポリシーは、同じデバイス タイプの新しいポリシーが適用される前に削除されます。**

   メモ: **グループ ポリシーのインポート中、パスワードはインポートされません。管理者は、すべてのパスワード フィールドにパスワードを再入力する必要があります。**

[ポリシーの編集] ページからのグループ ポリシーのインポート

手順

1. [**グループ & 設定**] ページで、希望のグループを選択します。
2. [**ポリシーの編集**] をクリックし、希望するオプションを選択します。
3. **インポート** をクリックします。
   [**ポリシーのインポート ウィザード**] 画面が表示されます。
4. 選択したグループからグループ ポリシーをインポートするモードを選択します。次のオプションが利用可能です。
   - 既存のグループから : ドロップダウン リストからグループを選択します。そのグループのポリシーが現在のグループにコピーされます。
   - エクスポートされたファイルから : .JSON ファイルを参照します。そのファイルのポリシーが現在のグループにコピーされます。
5. **次へ** をクリックします。
   選択したグループ内のポリシーのプレビューが表示されます。
6. [**次へ**] をクリックします。インポート プロセスの概要が表示されます。次のタイプの警告が表示されます。
   - **インポートされた<デバイス タイプ>ポリシーは、グループ<グループ名>に適用されます** : デバイス タイプの設定を含まないグループに同設定をインポートしている場合に表示されます。
   - **<デバイス タイプ>ポリシーは、<グループ名>グループに対してすでに存在します。既存の<デバイス タイプ>ポリシーは削除され、インポートされたポリシーが適用されます** : デバイス タイプの設定を含むグループにデバイス タイプの設定をインポートしている場合に表示されます。
   - **インベントリー ファイルへの依存関係を含むファイルからポリシーをインポートすると失敗します。このインポートを許可するには、[ポリシーの編集] ウィンドウからインポート オプションを使用します** : インベントリー ファイルへの参照を含むファイルからデバイス タイプの設定をインポートする場合に表示されます。
7. **インポート** をクリックします。

   メモ: ファイルからポリシーをインポートするときに、参照または無効な依存関係がある場合は、インポートが失敗し、エラー メッセージが表示されます。また、インポートするファイルに参照ファイルまたは依存関係ファイルがある場合は、該当するデバイス タイプの [ポリシーの編集] ページに移動して、グループ ポリシーをインポートします。

タスクの結果

宛先グループに、インポートされたポリシーと同じデバイス タイプのポリシーが含まれている場合、それらは削除され、新しいポリシーが追加されます。

メモ: グループ ポリシーのインポート中、パスワードはインポートされません。管理者は、すべてのパスワード フィールドにパスワードを再入力する必要があります。

ThinOS ポリシー設定の編集

手順

1. **グループ & 設定** をクリックします。
   グループ & 設定 ページが表示されます。
2. **ポリシーの編集** ドロップダウンメニューをクリックします。
3. **ThinOS** をクリックします。
   ThinOS 設定モードの選択 ウィンドウが表示されます。
4. ポリシーを設定するには、希望するモードを選択します。選択できるモードは次のとおりです。
   - ウィザードモード
   - 詳細設定モード

   メモ: ThinOS 詳細設定 をデフォルトモードとして設定するには、チェックボックスを選択します。
5. ポリシーの設定後、**保存して公開** をクリックします。

   メモ: 次の設定を変更すると、シン クライアントが再起動します。

- **BIOS 設定**
- **DP オーディオ**
- **ジャック ポップアップ**
- **端末名**
- **Ethernet 速度**
- **ディスプレイの変更 - 解像度、回転、リフレッシュ、デュアル ディスプレイ、マルチ ディスプレイ**
- **システム モード - VDI、StoreFront、および Classic**
- **LPT ポートのバインド**

ThinOS - ウィザード モード

このページは、ThinOS デバイスで最も使用頻度の高いパラメータを設定するのに使用します。

手順

1. 設定モードとして **ウィザード** を選択します。
2. 必要なオプションを設定します。
3. [**次へ**] をクリックして、次のポリシー設定に移動します。
4. オプションを設定した後、[**保存して公開**] をクリックします。

メモ: ThinOS の詳細設定モードに移動するには、[続行] をクリックします。

ThinOS - 詳細モード

ThinOS デバイスの詳細ポリシーを設定するには、このページを使用します。

手順

1. 設定のモードとして、**詳細設定** を選択します。
2. 必要に応じてオプションを設定します。
3. [**保存して公開**] をクリックし、設定を保存して公開します。

メモ: [ThinOS] ページに戻るには、[ポリシーの削除] をクリックします。

ThinOS 9.x ポリシー設定の編集

前提条件

- アプリケーション パッケージをプッシュするデバイスのグループ トークンを使用してグループを作成します。
- Thin Client を Wyse Management Suite に登録します。

手順

1. [**グループ＆設定**] ページに移動して、グループを選択します。
2. [**ポリシーの編集**] ドロップダウン メニューから、[**ThinOS 9.x**] をクリックします。
   [**設定コントロール** | ThinOS] ウィンドウが表示されます。
3. [**詳細設定**] オプションをクリックします。

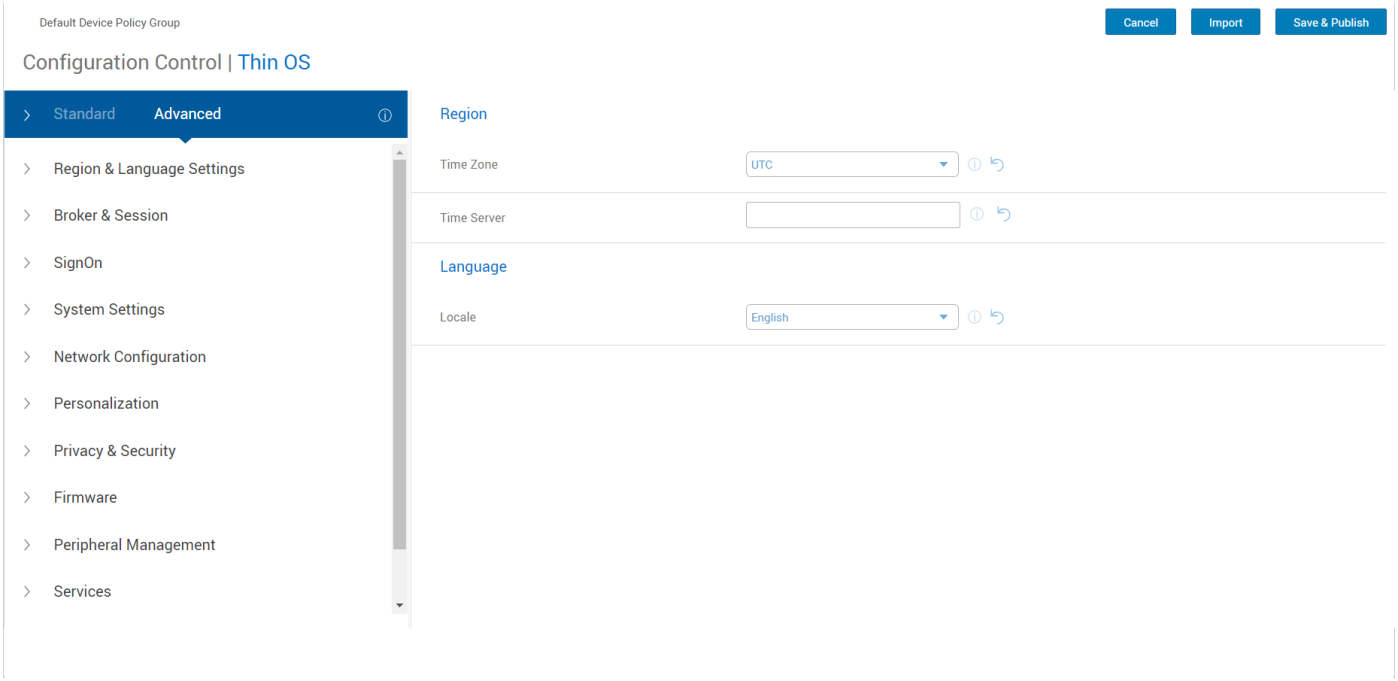


図 3. 詳細設定オプション

4. 設定するオプションを選択します。
5. それぞれのフィールドで、設定するオプションをクリックします。
6. 必要に応じてオプションを設定します。
7. [**保存して公開**] をクリックします。

メモ: [保存して公開] をクリックした後、設定は [標準] タブにも表示されます。

ThinOS 9.0 アプリケーション パッケージのアップロードとプッシュ

前提条件

- グループ トークンで Wyse Management Suite 内にグループを作成します。このグループ トークンを使用して、ThinOS 9.0 デバイスを登録します。
- Thin Client を Wyse Management Suite に登録します。

手順

1. [**グループ&設定**] ページに移動して、グループを選択します。
2. [**ポリシーの編集**] ドロップダウン メニューから、[**ThinOS 9.x**] をクリックします。
   [**設定コントロール** | ThinOS] ウィンドウが表示されます。
3. [**詳細設定**] をクリックします。
4. [**ファームウェア**] フィールドで、[**アプリケーション パッケージのプロパティ**] をクリックします。
5. [**ファイルの選択**] をクリックし、アプリケーション パッケージを参照してアップロードします。
6. [**導入する ThinOS パッケージの選択**] ドロップダウン メニューから、パッケージを選択します。
7. [**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、アプリケーション パッケージがインストールされます。

Windows Embedded Standard ポリシー設定の編集

手順

1. **グループ & 設定** をクリックします。

グループ & 設定 ページが表示されます。

2. **ポリシーの編集** ドロップダウンメニューをクリックします。
3. **WES** をクリックします。
   WES ページが表示されます。
4. ポリシーの設定後、**保存して公開** をクリックします。

Linux ポリシー設定の編集

手順

1. **グループ & 設定** をクリックします。
   グループ & 設定 ページが表示されます。
2. **ポリシーの編集** ドロップダウンメニューをクリックします。
3. **Linux** をクリックします。
4. ポリシーの設定後、**保存して公開** をクリックします。

ThinLinux ポリシー設定の編集

手順

1. **グループ & 設定** をクリックします。
   グループ & 設定 ページが表示されます。
2. **ポリシーの編集** ドロップダウンメニューをクリックします。
3. **ThinLinux** をクリックします。
4. ポリシーの設定後、**保存して公開** をクリックします。

Wyse Software Thin Client ポリシー設定の編集

手順

1. **グループ & 設定** をクリックします。
   グループ & 設定 ページが表示されます。
2. **ポリシーの編集** ドロップダウンメニューをクリックします。
3. **Wyse Software Thin Client** をクリックします。
   Wyse Software Thin Client ページが表示されます。
4. ポリシーの設定後、**保存して公開** をクリックします。

Cloud Connect のポリシー設定の編集

手順

1. **グループ & 設定** をクリックします。
   グループ & 設定 ページが表示されます。
2. **ポリシーの編集** ドロップダウンメニューをクリックします。
3. [**Cloud Connect**] をクリックします。
4. ポリシーの設定後、**保存して公開** をクリックします。

7

デバイスの管理

本項では、管理コンソールを使用して、日常的なデバイス管理タスクを実行する方法について説明します。デバイスのインベントリを特定し、**デバイス** タブをクリックします。グループまたはサブグループ、デバイスタイプ、オペレーティングシステムタイプ、ステータス、サブネット、およびプラットフォーム、タイムゾーンなど、さまざまなフィルタ条件を使用してデバイスのサブセットを表示できます。

デバイス リストは、以下に基づいて並べ替えることができます。

- タイプ
- プラットフォーム
- OS のバージョン
- シリアル番号
- IP アドレス
- 最後のユーザーの詳細
- グループ詳細
- 最終チェックイン時間
- 登録状態
- 書き込みフィルターの状態

特定デバイスの [**デバイスの詳細**] ページを表示するには、ページにリストされているデバイスのエントリーをクリックします。デバイスの詳細設定パラメータと、各パラメータが適用されているグループレベルは、**デバイスの詳細** ページにすべて表示されます。

デバイスに特有の設定パラメータを設定できます。このセクションで設定したパラメーターは、グループまたはグローバル レベル (またはその両方) で設定されたいずれのパラメーターよりも優先されます。

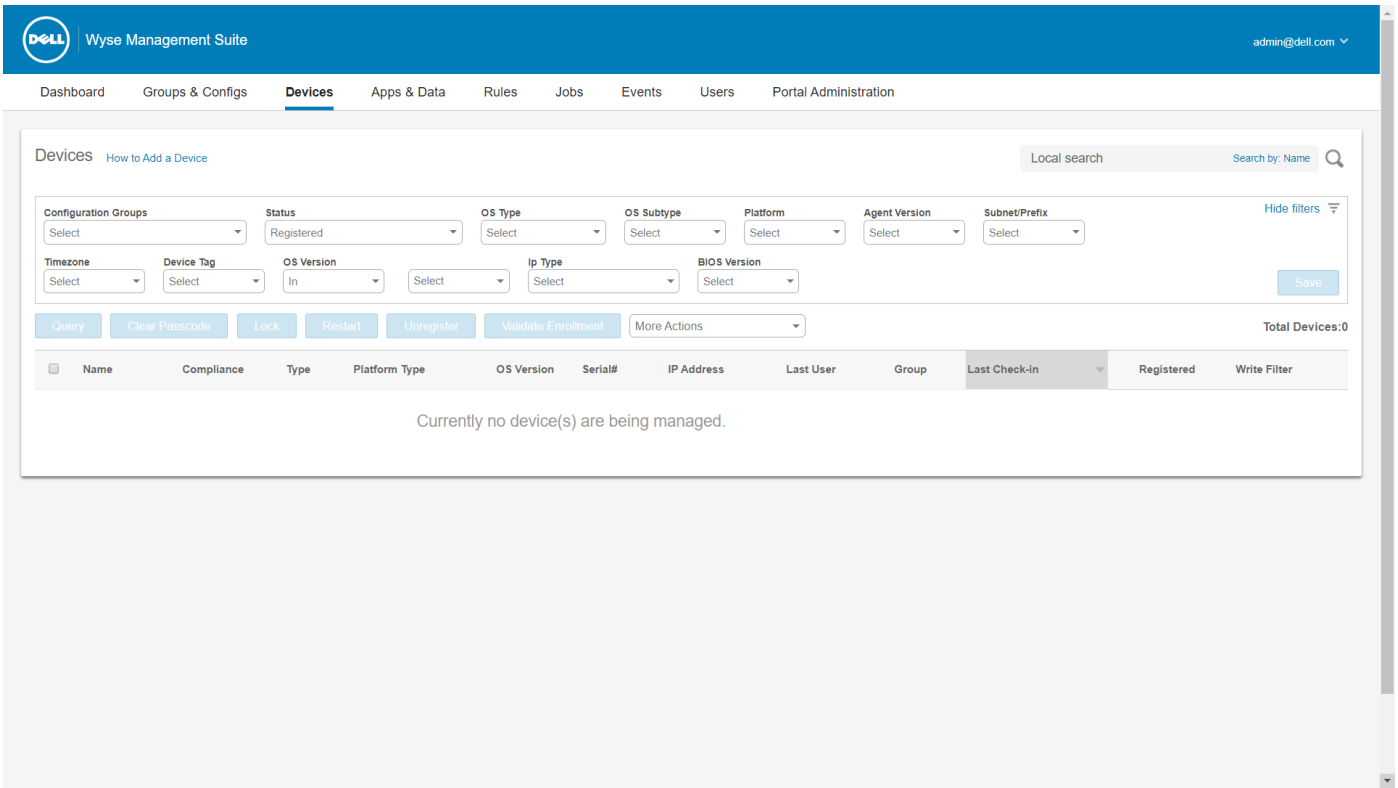


図 4. デバイスページ

トピック：

- デバイスを Wyse Management Suite に登録する方法

- フィルターの使用によるデバイスの検索
- [デバイス] ページでのフィルターの保存
- デバイス ステータスの問い合わせ
- デバイスのロック
- デバイスの再起動
- デバイスの登録解除
- 登録の検証
- ThinOS デバイスを工場出荷時のデフォルト設定にリセットする
- [デバイス] ページでのグループ割り当ての変更
- デバイスへのメッセージの送信
- デバイスのアクティブ化
- デバイスの詳細の表示
- デバイスの概要の管理
- システム情報の表示
- デバイス イベントの表示
- インストール済みアプリケーションの表示
- シンクライアントの名前の変更
- リモート シャドウ接続の設定
- デバイスのシャットダウン
- デバイスにタグを付ける
- デバイスコンプライアンスステータス
- Windows Embedded Standard または ThinLinux イメージの引き出し
- ログ ファイルの要求
- デバイスのトラブルシューティング

デバイスを Wyse Management Suite に登録する方法

Thin Client の Wyse Management Suite への登録は、次のいずれかの方法で行います。

- デバイスで Wyse デバイスエージェント (WDA) によって提供されるユーザーインタフェースを介して手動で登録します。
- DHCP サーバで適切なオプションタグを設定して、自動的に登録します。
- DNS サーバで適切な DNS SRV レコードを設定して、自動的に登録します。

メモ:

- パブリッククラウドの場合、Wyse Management Suite の URL、およびデバイスを登録するグループのグループトークンを指定して、提供することにより Thin Client を登録します。
- プライベート クラウドの場合、Wyse Management Suite の URL、およびこのデバイスを登録するグループのグループ トークン (オプション) を指定して、Thin Client を登録します。グループトークンが指定されていない場合、デバイスは管理対象外グループに登録されます。

Wyse Device Agent を使用した ThinOS デバイスの登録

ThinOS デバイスを手動で登録するには、次の操作を行います。

手順

1. Thin Client のデスクトップのメニューから、**[システム セットアップ]** > **[一元設定]** の順に移動します。
   一元設定 ウィンドウが表示されます。
2. **WDA** タブをクリックします。クライアントのブートアッププロセスの完了後、WDA サービスが自動的に実行されます。
   デフォルトでは、**WMS** が選択されています。
3. **Wyse Management Suite の有効化** チェックボックスを選択して、Wyse Management Suite を有効化します。
4. 管理者が対象グループに対して設定した**グループ登録キー**を入力します。
5. **WMS の詳細設定の有効化** オプションを選択して、WMS サーバまたは MQTT サーバの詳細情報を入力します。

6. ライセンスのタイプに基づき、CA 検証を有効または無効にします。パブリッククラウドの場合、**CA 検証を有効にする** チェックボックスを選択してください。プライベートクラウドの場合、周知の認証局から Wyse Management Suite サーバに証明書をインポート済みであれば、**CA 検証を有効にする** チェックボックスを選択してください。

   プライベートクラウドで CA 検証オプションを有効にするには、同じ自己署名証明書を ThinOS デバイスにもインストールする必要があります。自己署名証明書を ThinOS デバイスにインストールしていない場合は、[**CA 検証を有効にする**] チェック ボックスを選択しないでください。登録後に、Wyse Management Suite を使用して証明書をデバイスにインストールしてから、CA 検証オプションを有効にしてください。

   メモ:

   - **CA 検証を無効にすると、警告メッセージが表示されます。確定するには、[Ok] をクリックしてください。**
   - **米国内のデータセンターでパブリッククラウドバージョンの Wyse Management Suite を使用している場合は、デフォルトの WMS サーバと MQTT サーバの詳細項目を変更しないでください。ヨーロッパのデータセンターでパブリッククラウドバージョンの Wyse Management Suite を使用している場合は、以下を使用してください。**
     - **CCM サーバ：eu1.wysemanagementsuite.com**
     - **MQTT サーバ：eu1-pns.wysemanagementsuite.com:1883**
   - **サーバー アドレスに「http」が含まれていると、警告メッセージが表示されます。確定するには、[Ok] をクリックしてください。**
7. 設定を確認するには、**キーの検証** クリックします。キーの検証後、デバイスは自動的に再起動します。

   メモ: キーが検証されない場合は、入力したグループキーと WMS サーバの URL を確認してください。ネットワークでポート 443 および 1883 がブロックされていないことを確認します。
8. **OK** をクリックします。
   デバイスが、Wyse Management Suite に登録されました。

Wyse Device Agent を使用した Windows Embedded Standard Thin Client の Wyse Management Suite への登録

前提条件

デバイスを登録するには、Wyse Management Suite でグループを作成します。

手順

1. Wyse Device Agent アプリケーションを開きます。
   Wyse Device Agent 画面が表示されます。
2. **管理サーバ** ドロップダウンリストから、**Wyse Management Suite** を選択します。
3. サーバアドレスとポート番号をそれぞれのフィールドに入力します。

   メモ: サーバー アドレスに「http」が含まれている場合、警告メッセージが表示されます。[OK] をクリックして確認します。
4. グループトークンを入力します。シングルテナントについては、グループトークンはオプションの手順です。

   メモ: [グループ トークン] フィールドに入力されたグループ トークンは、クリア テキストでは表示されません。
5. ライセンスのタイプに基づく CA 検証を有効または無効にします。

   メモ: CA 検証を無効にすると、警告メッセージが表示されます。[OK] をクリックして確認します。
6. **登録** をクリックします。

Wyse デバイス エージェントを使用した Wyse Software Thin Client の Wyse Management Suite への登録

前提条件

デバイスを Wyse Management Suite に登録するためのグループを作成します。

手順

1. **Wyse Device Agent** アプリケーションを開きます。
   Wyse Device Agent ウィンドウが表示されます。
2. デバイス登録の詳細を入力します。
3. **管理サーバ** ドロップダウンリストから、**Wyse Management Suite** を選択します。
4. サーバアドレスとポート番号をそれぞれのフィールドに入力します。

   メモ: サーバー アドレスに「http」が含まれている場合、警告メッセージが表示されます。[OK] をクリックして確認します。
5. グループトークンを入力します。シングルテナントについては、グループトークンはオプションの手順です。
6. ライセンスのタイプに基づく CA 検証を有効または無効にします。

   メモ: CA 検証を無効にすると、警告メッセージが表示されます。[OK] をクリックして確認します。
7. **登録** をクリックします。
   登録が完了した後、「Wyse Management Suite に登録されました」というメッセージが表示されます。

Wyse デバイス エージェントを使用した ThinLinux Thin Client の登録

前提条件

デバイスを登録するには、Wyse Management Suite でグループを作成します。

手順

1. Wyse Device Agent アプリケーションを開きます。
   Wyse Device Agent 画面が表示されます。
2. デバイス登録の詳細を入力します。
3. Wyse Management Suite で、Wyse Management Suite サーバの詳細を入力します。
4. グループトークンを入力します。
   シングルテナントについては、グループトークンはオプションの手順です。
5. **登録** をクリックします。
   登録が完了すると、確認メッセージが表示されます。

FTP INI メソッドを使用した ThinOS デバイスの登録

前提条件

Wyse Management Suite に登録するグループを作成します。

手順

1. `wnos.ini` ファイルを作成します。次のパラメータを入力します。

   CCMEnable=`yes/no` **CCMServer**=`FQDN of WMS Server` **GroupPrefix**=`The prefix of the Group Token` **GroupKey**=`The Group Key` **CAValidation**=`yes/no` **Discover**=`yes/no`

   たとえば、ThinOS デバイスを Wyse Management Suite (サーバの FQDN は ServerFQDN.domain.com) に登録するには、グループトークン defa-defadefa を使用し、CA 検証オプションを有効にして、次の INI パラメータを入力します。

   CCMEnable=`yes` **CCMServer**=` is ServerFQDN.domain.com` **GroupPrefix**=`defa` **GroupKey**=`defadefa` **CAValidation**=`yes` **Discover**=`yes`
2. `wnos.ini` ファイルを任意の FTP パスの wnos フォルダー内に配置します。
3. ThinOS デバイスの **一元設定** に移動します。
4. [**一般**] タブで、ファイル サーバーの FTP パスまたは親フォルダーへのパスを指定します。
5. 必要に応じて、FTP 資格情報を入力します。FTP が資格情報を必要としない場合は、ユーザー名とパスワードを匿名にできます。

6. **OK** をクリックして、Thin Client を再起動します。
7. ThinOS デバイスの **一元設定** に移動します。
Wyse デバイスエージェント タブで、Wyse 管理サーバの詳細がそれぞれのフィールドで使用可能で、クライアントのエントリーが Wyse 管理サーバ の デバイス ページに表示されていることを確認します。

FTP INI メソッドを使用した ThinLinux バージョン 2.0 デバイスの登録

前提条件

Wyse Management Suite に登録するグループを作成します。

手順

1. `wlx.ini` ファイルを作成します。次のパラメータを入力します。

   WMSEnable=yes\no

   WMSServer=https://FQDN of the WMS Server:Port <By default 443 is used>

   GroupRegistrationKey=GroupToken present in WMS Server

   CAValidation=True/False

   たとえば、ThinLinux バージョン 2.0 デバイスを Wyse Management Suite (サーバの FQDN は ServerFQDN.domain.com) に登録するには、グループトークン defa-defadefa を使用し、CA 検証オプションを有効にして、次の INI パラメータを入力します。

   WMSEnable=yes

   WMSServer=https://ServerFQDN.domain.com:443

   GroupRegistrationKey=defa-defadefa

   CAValidation=True
2. wlx ini ファイルを wyse\wlx2 フォルダに配置します。
3. **設定** に移動し、ThinLinux Thin Client で admin に切り替えます。
4. **[管理]** > **[INI]** の順に移動します。
5. FTP サーバの URL を入力します。
6. [**保存**] をクリックして、Thin Client を再起動します。
7. **[管理]** > **[Wyse デバイス エージェント]** の順に移動します。
Wyse デバイスエージェント タブで、Wyse 管理サーバの詳細がそれぞれのフィールドで使用可能で、クライアントのエントリーが Wyse 管理サーバ の デバイス ページに表示されていることを確認します。

FTP INI メソッドを使用した ThinLinux バージョン 1.0 デバイスの登録

前提条件

Wyse Management Suite に登録するグループを作成します。

手順

1. `wlx.ini` ファイルを作成し、次のパラメーターを入力します。

   WMSEnable=yes\no

   WMSServer=https://FQDN of the WMS Server:Port <By default 443 is used>

   GroupRegistrationKey=GroupToken present in WMS Server

   CAValidation=True/False

   たとえば、ThinLinux バージョン 1.0 デバイスを Wyse Management Suite (サーバの FQDN は ServerFQDN.domain.com) に登録するには、グループトークン defa-defadefa を使用し、CA 検証オプションを有効にして、次の INI パラメータを入力します。

WMSEnable=yes

WMSServer=https://ServerFQDN.domain.com:443

GroupRegistrationKey=defa-defadefa

CAValidation=True

2. wlx.ini ファイルを wyse\wlx フォルダーに配置します。
3. **設定** に移動し、ThinLinux Thin Client で admin に切り替えます。
4. **[管理]** > **[INI]** の順に移動します。
5. FTP サーバの URL を入力します。
6. [**保存**] をクリックして、Thin Client を再起動します。
7. **[管理]** > **[Wyse デバイス エージェント]** の順に移動します。
   Wyse デバイスエージェント タブで、Wyse 管理サーバの詳細がそれぞれのフィールドで使用可能で、クライアントのエントリーが Wyse 管理サーバ の デバイス ページに表示されていることを確認します。

DHCP オプションタグの使用によるデバイスの登録

DHCP オプション タグを使用して、デバイスを登録できます。

表 3. DHCP オプションタグの使用によるデバイスの登録

オプションタグ	説明
名前 - WMS **データタイプ** - 文字列 **コード** - 165 **説明** - WMS サーバ FQDN	このタグは、Wyse Management Suite サーバ URL をポイントします。たとえば、wmsserver.acme.com:443 であれば、wmsserver.acme.com は、Wyse Management Suite がインストールされているサーバの完全修飾ドメイン名です。
名前 - MQTT **データタイプ** - 文字列 **コード** - 166 **説明** - MQTT サーバ	このタグは、デバイスを Wyse Management Suite のプッシュ通知サーバ (PNS) にポイントします。プライベートクラウドのインストールについては、デバイスは Wyse Management Suite サーバ上の MQTT サービスに向けられます。例 : wmsservername.domain.com:1883。 デバイスを Wyse Management Suite のパブリッククラウドで登録するには、デバイスがパブリッククラウドで PNS (MQTT) サーバをポイントする必要があります。たとえば、次のとおりです。 US1 : us1-pns.wysemanagementsuite.com EU1 : eu1-pns.wysemanagementsuite.com
名前 - CA 検証 **データタイプ** - 文字列 **コード** - 167 **説明** - 認証局の検証	プライベートクラウドの Wyse Management Suite にデバイスを登録する場合、CA 検証オプションを有効または無効にできます。デフォルトでは、CA 検証はパブリッククラウドで有効になっています。パブリッククラウドでも、CA 検証を無効にできます。 クライアントと Wyse Management Suite サーバ間の https 通信のために既知の認証局から SSL 証明書をインポートしている場合は、**True** を入力します。 クライアントと Wyse Management Suite サーバ間の https 通信のために既知の認証局から SSL 証明書をインポートしていない場合は、**False** を入力します。
名前 - GroupToken **データタイプ** - 文字列 **コード** - 199 **説明** - グループトークン	パブリックまたはプライベートクラウドで ThinOS デバイスを Wyse Management Suite に登録する場合、このタグは必須です。 プライベートクラウドで Windows Embedded Standard または ThinLinux デバイスを Wyse Management Suite に登録する場合、このタグは任意です。タグが使用できない場合、デバイスは、オンプレミスのインストール中に自動的に管理対象外グループに登録されます。

メモ: Windows サーバーで DHCP オプション タグを追加する詳細な手順は、「DHCP オプション タグの作成方法と設定方法」を参照してください。

DNS SRV レコードの使用によるデバイスの登録

DNS ベースのデバイスの登録は、次のバージョンの Wyse デバイス エージェントでサポートされています。

- Windows Embedded Systems - 13.0 以降のバージョン
- Thin Linux - 2.0.24 以降のバージョン
- ThinOS - 8.4 ファームウェア以降のバージョン

DNS SRV レコードのフィールドに有効な値が設定されている場合は、Wyse Management Suite サーバにデバイスを登録することができます。

メモ: Windows サーバーで DNS SRV レコードを追加する詳細な手順は、「DNS SRV レコードを作成して設定する方法」を参照してください。

次の表に、DNS SRV レコードの有効な値を示します。

表 4. DNS SRV レコードの使用によるデバイスの設定

URL/ タグ	説明
レコード名 - _WMS_MGMT **レコード FQDN** - _WMS_MGMT._tcp.<ドメイン名> **レコードタイプ** - SRV	このレコードは、Wyse Management Suite サーバ URL をポイントします。たとえば、`wmsserver.acme.com:443` であれば、wmsserver.acme.com は、Wyse Management Suite がインストールされているサーバの完全修飾ドメイン名です。 **メモ: サーバの URL で https:// を使用しないでください。使用すると、Thin Client が Wyse Management Suite の下に登録されません。**
レコード名 - _WMS_MQTT **レコード FQDN** - _WMS_MQTT._tcp.<ドメイン名> **レコードタイプ** - SRV	このレコードは、デバイスを Wyse Management Suite のプッシュ通知サーバ (PNS) にポイントします。プライベートクラウドのインストールについては、デバイスは Wyse Management Suite サーバ上の MQTT サービスに向けられます。例：`wmsservername.domain.com:1883`。 **メモ: MQTT は、最新バージョンの Wyse Management Suite では任意です。** デバイスを Wyse Management Suite のパブリッククラウドで登録するには、デバイスがパブリッククラウドで PNS (MQTT) サーバをポイントする必要があります。たとえば、次のとおりです。 US1 - us1-pns.wysemanagementsuite.com EU1 - eu1-pns.wysemanagementsuite.com
レコード名 - _WMS_GROUPTOKEN **レコード FQDN** - _WMS_GROUPTOKEN._tcp.<ドメイン名> **レコードタイプ** - テキスト	パブリックまたはプライベートクラウドで ThinOS デバイスを Wyse Management Suite に登録する場合、このレコードは必須です。 プライベートクラウドで Windows Embedded Standard または ThinLinux デバイスを Wyse Management Suite に登録する場合、このレコードは任意です。レコードが使用できない場合、デバイスは、オンプレミスのインストール中に自動的に管理対象外グループに登録されます。 **メモ: プライベートクラウド上の最新バージョンの Wyse Management Suite ではグループトークンはオプションです。**
レコード名 - _WMS_CAVALIDATION **レコード FQDN** - _WMS_CAVALIDATION._tcp.<ドメイン名> **レコードタイプ** - テキスト	プライベートクラウドの Wyse Management Suite にデバイスを登録する場合、CA 検証オプションを有効または無効にできます。デフォルトでは、CA 検証はパブリッククラウドで有効になっています。パブリッククラウドでも、CA 検証を無効にできます。

URL/ タグ	説明
	クライアントと Wyse Management Suite サーバ間の https 通信のために既知の認証局から SSL 証明書をインポートしている場合は、**True** を入力します。 クライアントと Wyse Management Suite サーバ間の https 通信のために既知の認証局から SSL 証明書をインポートしていない場合は、**False** を入力します。 メモ: **CA 検証は、最新バージョンの Wyse Management Suite では任意です。**

フィルターの使用によるデバイスの検索

手順

1. **設定グループ** ドロップダウンリストから、デフォルトポリシーグループまたは、管理者によって追加されたグループのどちらかを選択します。
2. [**ステータス**] ドロップダウン リストから、次のオプションのいずれかを選択します。
   - **登録**
     - 登録済み
     - 事前登録済み
     - 未登録
     - 準拠
     - 登録の検証保留中
     - 保留中
     - 非準拠
   - **オンライン状態**
     - オンライン
     - オフライン
     - 不明
   - **その他**
     - 最近追加
3. [**OS タイプ**] ドロップダウン リストから、次のいずれかのオペレーティング システムを選択します。
   - **Thin Client**
     - Linux
     - ThinLinux
     - ThinOS
     - WES
     - Teradici (プライベートクラウド)
     - Wyse Software Thin Client
4. **OS サブタイプ** ドロップダウンリストから、お使いのオペレーティングシステムのサブタイプを選択します。
5. **プラットフォーム** ドロップダウンリストから、プラットフォームを選択します。
6. **OS バージョン** ドロップダウンリストから、OS のバージョンを選択します。
7. **エージェントバージョン** ドロップダウンリストから、エージェントのバージョンを選択します。
8. **サブネット** ドロップダウンリストから、サブネットを選択します。
9. **タイムゾーン** ドロップダウンリストから、タイムゾーンを選択します。
10. **デバイスタグ** ドロップダウンリストから、デバイスタグを選択します。

[デバイス] ページでのフィルターの保存

必要なフィルター オプションを設定することで、現在のフィルターをグループとして保存できます。

手順

1. フィルタの **名前** を入力します。
2. **説明** ボックスに、フィルタの説明を入力します。
3. 現在のフィルタをデフォルトオプションとして設定するには、このチェックボックスを選択します。
4. **ファイルの保存** をクリックします。

デバイス ステータスの問い合わせ

システムのデバイス情報とステータスを更新するコマンドを送信できます。

手順

1. **デバイス** をクリックします。
   デバイス ページが表示されます。
2. フィルタで使用するデバイスを検索します。
3. デバイスのチェックボックスを選択します。
4. **クエリ** をクリックします。
   アラート ウィンドウが表示されます。
5. **コマンドの送信** をクリックして、クエリコマンドを送信します。

デバイスのロック

コマンドを送信して、登録済みデバイスをロックできます。

手順

1. **デバイス** をクリックします。
   デバイス ページが表示されます。
2. フィルタで使用するデバイスを検索します。
3. デバイスのチェックボックスを選択します。
4. **ロック** をクリックします。
   アラート ウィンドウが表示されます。
5. **コマンドの送信** をクリックして、ロックコマンドを送信します。

デバイスの再起動

コマンドを送信して、登録済みデバイスを再起動できます。

手順

1. **デバイス** をクリックします。
   デバイス ページが表示されます。
2. フィルタで使用するデバイスを検索します。
3. デバイスのチェックボックスを選択します。
4. **再起動** をクリックします。
   アラート ウィンドウが表示されます。
5. **コマンドの送信** をクリックして、再起動コマンドを送信します。

デバイスの登録解除

Wyse Management Suite からデバイスを登録解除するコマンドを送信できます。

手順

1. **デバイス** をクリックします。
   デバイス ページが表示されます。

2. フィルタで使用するデバイスを検索します。
3. デバイスのチェックボックスを選択します。
4. **登録解除** をクリックします。
   アラート ウィンドウが表示されます。
5. **強制登録解除** チェックボックスを選択します。
6. **コマンドの送信** をクリックして、登録解除コマンドを送信します。

   メモ: サーバとクライアントの間に通信がない場合に、強制登録解除 オプションを使用すると、デバイスを削除することができます。デバイスは管理対象外状態になり、サーバー エントリーから削除できます。登録解除と強制登録解除の処理は、WES WDA UI でも実行できます。

登録の検証

デバイスを手動または DHCP/DNS 自動検出メソッドを使用して登録する場合、グループ トークンが定義されていると、デバイスが特定のグループに登録されます。グループ トークンが定義されていない場合、デバイスは管理対象外グループに登録されます。

Wyse Management Suite では、デバイスをグループに登録する前にテナントが手動で承認する必要がある [**登録の検証**] オプションが導入されています。

[**登録の検証**] オプションを有効にすると、自動検出されたデバイスは、[**デバイス**] ページで [**検証保留中**] 状態になります。テナントは、[**デバイス**] ページで 1 台または複数のデバイスを選択して、登録を検証することができます。デバイスは検証された後、目的のグループに移動されます。デバイスの検証方法の詳細については、「登録の検証」を参照してください。

メモ: パブリック クラウド内の既存のテナントに対して、またはオンプレミス テナントをアップグレードする場合、[登録の検証] オプションは無効になります。

デバイスの検証ステータスも、[**ダッシュボード**] ページの [**デバイス**] セクションに表示されます。

デバイスの登録の検証

[**登録の検証**] を有効にすると、グループへのシン クライアントの手動/自動登録を管理者が制御できるようになります。[**ダッシュボード**] ページで [**保留**] の件数をクリックするか、[**デバイス**] ページの [**ステータス**] ドロップダウン リストで [**登録の検証保留中**] を選択することで、[**検証保留中**] 状態のデバイスをフィルターで絞り込むことができます。

前提条件

- Wyse Management Suite のインストール時に、または [**ポータル管理**] ページでの操作時に、[**登録の検証**] オプションを有効にする必要があります。
- デバイスは [登録保留中] 状態になっている必要があります。

手順

1. 検証するデバイスのチェック ボックスを選択します。
2. [**登録の検証**] オプションをクリックします。
   アラート ウィンドウが表示されます。
3. **コマンドの送信** をクリックします。
   デバイスが目的のグループに移動され、デバイスが登録されます。

ThinOS デバイスを工場出荷時のデフォルト設定にリセットする

ThinOS ベースのデバイスを工場出荷時のデフォルト設定にリセットするコマンドを送信できます。

手順

1. **デバイス** をクリックします。
   デバイス ページが表示されます。
2. フィルタで使用するデバイスを検索します。
3. デバイスのチェックボックスを選択します。

4. **その他のアクション** ドロップダウンメニューから、**工場出荷時設定へのリセット** をクリックします。
   アラート ウィンドウが表示されます。
5. クライアントをリセットする理由を入力します。
6. **コマンドの送信** をクリックします。

[デバイス] ページでのグループ割り当ての変更

[**デバイス**] ページを使用して、デバイスのグループ割り当てを変更することができます。

手順

1. **デバイス** をクリックします。
   デバイス ページが表示されます。
2. フィルタで使用するデバイスを検索します。
3. デバイスのチェックボックスを選択します。
4. **追加アクション** ドロップダウンメニューから、**グループの変更** をクリックします。
   グループ割り当ての変更 ウィンドウが表示されます。
5. ドロップダウンメニューから、デバイスの新しいグループを選択します。
6. **保存** をクリックします。

デバイスへのメッセージの送信

[**デバイス**] ページを使用して、登録済みデバイスにメッセージを送信できます。

手順

1. **デバイス** をクリックします。
   デバイス ページが表示されます。
2. フィルタで使用するデバイスを検索します。
3. デバイスのチェックボックスを選択します。
4. **その他のアクション** ドロップダウンメニューで、**メッセージの送信** をクリックします。
   メッセージの送信 ウィンドウが表示されます。
5. メッセージを入力します。
6. **送信** をクリックします。

デバイスのアクティブ化

デバイスの電源がオフ、またはスリープ モードの場合は、コマンドを送信してデバイスをアクティブ化できます。

手順

1. **デバイス** をクリックします。
   デバイス ページが表示されます。
2. フィルタで使用するデバイスを検索します。
3. デバイスのチェックボックスを選択します。
4. **追加アクション** ドロップダウンメニューから、**Wake On LAN** をクリックします。
   アラート ウィンドウが表示されます。
5. **コマンドの送信** をクリックします。

デバイスの詳細の表示

手順

1. **デバイス** をクリックします。
   デバイス ページが表示されます。
2. フィルタで使用するデバイスを検索します。

使用するデバイスのリストが表示されます。

3. 表示されているデバイスのいずれかをクリックします。
デバイスの詳細 ページが表示されます。

デバイスの概要の管理

[**デバイス**] ページを使用して、メモ、グループ割り当て、アラート、デバイス設定に関する情報を表示/管理できます。

手順

1. **デバイス** をクリックします。
2. **デバイスの詳細** ページで、**概要** タブをクリックします。
デバイスの概要が表示されます。
3. 右ペインで、**メモの追加** をクリックします。
メモの追加 ウィンドウが表示されます。
4. 表示されたフィールドにメッセージを入力し、**保存** をクリックします。
5. 右側のウィンドウで、**グループ割り当ての変更** をクリックします。
グループ割り当ての変更 ウィンドウが表示されます。
6. ドロップダウンメニューから、デバイスの新しいグループを選択します。
7. **保存** をクリックします。
8. **例外の作成/編集** をクリックしてデバイスレベルの例外を作成または編集し、**デバイス** ページで特定のデバイスポリシーを設定します。

システム情報の表示

手順

1. **デバイス** をクリックします。
デバイス ページが表示されます。
2. フィルタで使用するデバイスを検索します。
使用するデバイスのリストが表示されます。
3. 表示されているデバイスのいずれかをクリックします。
デバイスの詳細 ページが表示されます。
4. **システム情報** をクリックします。
システム情報が表示されます。

デバイス イベントの表示

デバイスに関するシステム イベントについて、情報を表示および管理できます。

手順

1. **デバイス** をクリックします。
デバイス ページが表示されます。
2. フィルタで使用するデバイスを検索します。
使用するデバイスのリストが表示されます。
3. 表示されているデバイスのいずれかをクリックします。
デバイスの詳細 ページが表示されます。
4. **デバイスの詳細** ページで、**イベント** タブをクリックします。
デバイス上のイベントが表示されます。

インストール済みアプリケーションの表示

手順

1. **デバイス** をクリックします。

デバイス ページが表示されます。

2. フィルタで使用するデバイスを検索します。
   使用するデバイスのリストが表示されます。
3. 表示されているデバイスのいずれかをクリックします。
   デバイスの詳細 ページが表示されます。
4. **インストールされているアプリ** タブをクリックします。
   デバイス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表示されます。

   このオプションは、Windows Embedded Standard、Linux、および ThinLinux デバイスで利用できます。以下は、ページに表示される属性です。

   - 名前
   - 公開元
   - バージョン
   - インストール先

   メモ:

   インストール済みアプリケーションの数は、アプリケーションのインストールまたはアンインストールに基づいて増減します。リストはデバイスがチェックインしたとき、または次にクエリされるときに更新されます。

シンクライアントの名前の変更

このページでは、Windows Embedded Standard、ThinLinux、ThinOS オペレーティング システムで実行しているシン クライアントのホスト名を変更できます。

手順

1. **デバイス** ページで、該当デバイスをクリックします。
2. **その他のオプション** ドロップダウンリストから、**ホスト名の変更** オプションを選択します。
3. プロンプトが表示されたら、新しいホスト名を入力します。

   メモ: ホスト名には、英数字およびハイフンのみを含めることができます。

4. Windows Embedded Standard デバイスでは、[**アラート**] ウィンドウに [**再起動**] ドロップダウン リストがあります。システムを再起動するには、**再起動** オプションを選択します。[**後で再起動**] オプションを選択すると、設定した時間にデバイスが再起動してからホスト名がアップデートされます。

   メモ: ホスト名のアップデートのために、ThinLinux デバイスを再起動する必要はありません。

5. **コマンドの送信** をクリックします。
   確認メッセージが表示されます。

リモート シャドウ接続の設定

グローバルおよびグループ管理者が Windows Embedded Standard、ThinLinux、および ThinOS Thin Client セッションにリモートでアクセスできるようにするには、このページを使用します。この機能は、プライベートクラウドにのみ適用可能で、Standard と Pro 両方のライセンスで利用できます。

手順

1. **デバイス** ページで、該当デバイスをクリックします。
2. **その他のオプション** ドロップダウンリストから、**リモートシャドー (VNC)** オプションを選択します。
   ターゲット Thin Client の IP アドレスとポート番号が、**リモートシャドー (VNC)** ダイアログボックスに表示されます。

   メモ: デフォルトのポート番号は 5900 です。

3. ターゲット Thin Client のポート番号を変更します (オプション)。
4. **接続** をクリックし、ターゲット Thin Client へのリモートセッションを開始します。

   メモ: Wyse Management Suite ポータルは、テナントごとに最大 5 つのリモートシャドーセッションをサポートします。

デバイスのシャットダウン

Wyse Management Suite を使用して、Windows Embedded Standard、ThinLinux、ThinOS Thin Client などのデバイスをシャットダウンできます。

手順

1. **デバイス** をクリックします。
   デバイス ページが表示されます。
2. フィルタで使用するデバイスを検索します。
   使用するデバイスのリストが表示されます。
3. [**その他のオプション**] ドロップダウン リストから、[**今すぐシャットダウン**] をクリックします。
   デバイスをシャットダウンするリモート コマンドが、選択したデバイスに送信されます。デバイスがサーバーに応答し、コマンドが正常に適用されます。

   メモ: Linux オペレーティング システムで実行されているシン クライアントでは、[今すぐシャットダウン] オプションは有効になっていません。

デバイスにタグを付ける

Wyse Management Suite の **タグデバイス** オプションで、デバイスまたはデバイスのグループを識別することができます。

手順

1. **デバイス** をクリックします。
   デバイス ページが表示されます。
2. フィルタで使用するデバイスを検索します。
   使用するデバイスのリストが表示されます。
3. 1 つまたは複数のデバイスを選択します。**その他のオプション** ドロップダウンリストから、**タグデバイス** をクリックします。
   デバイスのタグの設定 ウィンドウが表示されます。
4. タグ名を入力します。
5. **タグの設定** をクリックします。

デバイスコンプライアンスステータス

デフォルトでは、次の色がデバイスステータスとして表示されます。

- 赤 - 登録済みデバイスが 7 日以上チェックインされていない場合。
- 灰色 - デバイスに設定ポリシーを適用した場合。
- 緑 - すべての設定ポリシーをデバイスに適用した場合。

デフォルト値は 1 日から 99 日に変更することができます。

オンラインステータス オプションは、デバイス名の横にあります。オンラインステータスには、次の色が表示されます。

- 赤 — デバイスがハートビートを 4 回以上送信していない場合。
- 灰色 - デバイスがハートビートを 3 回以上送信しておらず、送信が 2 回以下である場合。
- 緑 - デバイスがハートビートを定期的に送信している場合。

Windows Embedded Standard または ThinLinux イメージの引き出し

前提条件

- Wyse Management Suite 1.3 リモート リポジトリーを使用している場合、リカバリー/リカバリー + OS プル テンプレートはリポジトリーで使用できません。テンプレートにアクセスするには、Wyse Management Suite を 1.4 以降のバージョンにアップグレードする必要があります。
- ThinLinux イメージのプル操作を実行するには、ThinLinux デバイスの [**設定**] ウィンドウを閉じる必要があります。ThinLinux デバイスから OS/OS+ リカバリー イメージをプルする前に、この操作を実行する必要があります。

- ThinLinux 1.x から 2.x にアップグレードするには、管理者はデバイスを最新の WDA および Merlin でアップデートしてからイメージをプルする必要があります。ThinLinux 1.x から 2.x へのアップグレードには、このプルされたイメージを使用する必要があります。

手順

1. Windows Embedded Standard または ThinLinux デバイスのページに移動します。
2. **追加アクション** ドロップダウンリストから **OS イメージの引き出し** オプションを選択します。
3. 次の詳細を入力または選択します。
   - **イメージの名前** - イメージの名前を入力します。類似した名前のイメージ、および正常に完了していないイメージファイルの置き換えには、**上書き名** をクリックします。
   - **ファイルリポジトリ** - ドロップダウンリストから、イメージのアップロード先になるファイルリポジトリを選択します。ファイル リポジトリーには、次の 2 つのタイプがあります。
     - ローカルリポジトリ
     - リモート Wyse Management Suite リポジトリ
   - **プルタイプ** - プルタイプの要件に基づき、**デフォルト** または **詳細設定** のいずれかを選択します。
     - **デフォルト** プルタイプを選択した場合、次のオプションが表示されます。
       - 圧縮
       - OS (オペレーティングシステム)
       - BIOS
       - リカバリー : ThinLinux 2.x 用
     - **詳細設定** プルタイプを選択すると、テンプレートを選択するためのドロップダウンリストが表示されます。デフォルトで使用可能な任意のテンプレートを選択します。

       メモ: 既存またはデフォルト テンプレートを編集して手動で作成したカスタム テンプレートを使用できます。
4. **イメージのプルの準備** をクリックします。

タスクの結果

OS イメージの引き出し コマンドが送信されると、クライアントデバイスはサーバからイメージ引き出し要求を受信します。イメージ引き出し要求メッセージは、クライアント側に表示されます。次のいずれかのオプションをクリックします。

- **Sysprep 後に引き出し** - デバイスは再起動し、無効状態でオペレーティング システムにログインします。カスタム Sysprep を実行します。カスタム sysprep が完了した後、デバイスで Merlin オペレーティング システムが起動し、イメージの引き出し操作が実行されます。

  メモ: このオプションは、Windows Embedded Standard デバイスに適用されます。
- **今すぐ引き出し** - デバイスで Merlin オペレーティング システムが起動し、イメージの引き出し操作が実行されます。

ログ ファイルの要求

Windows Embedded Standard、ThinOS、ThinLinux のデバイス ログを要求できます。ThinOS デバイスはシステムログをアップロードします。Windows Embedded Standard は、Wyse デバイスエージェントのログと Windows イベント ビューアのログをアップロードします。Linux または ThinLinux は、Wyse デバイスエージェントのログとシステムログをアップロードします。

前提条件

ログファイルを取得するにはデバイスを有効にする必要があります。

手順

1. **デバイス** ページに進み、特定のデバイスをクリックします。

   デバイスの詳細が表示されます。
2. **デバイスのログ** タブをクリックします。
3. **ログファイルの要求** をクリックします。
4. Wyse Management Suite サーバにログファイルをアップロードした後で、**ここをクリック** リンクをクリックし、ログをダウンロードします。

   メモ: Linux または ThinLinux は、ログ ファイルを .tar 形式でアップロードします。Windows または ThinOS 9.x システム上のファイルを抽出する場合は、7zip またはその他の同等のファイルが必要です。

デバイスのトラブルシューティング

[**デバイス**] ページを使用して、トラブルシューティング情報を表示および管理できます。

手順

1. **デバイスの詳細** ページで、**トラブルシューティング** タブをクリックします。
2. **スクリーンショットの要求** をクリックします。
   クライアントのアクセス許可の有無にかかわらず、Thin Client のスクリーンショットをキャプチャすることができます。[**ユーザーの受け入れが必要です**] チェック ボックスを選択した場合、クライアントにメッセージが表示されます。このオプションは、Windows Embedded Standard、Linux、および ThinLinux デバイスにのみ適用されます。
3. Thin Client 上で稼動するプロセスのリストを表示するには、**プロセスリストの要求** をクリックします。
4. Thin Client 上で稼動するサービスのリストを表示するには、**サービスリストの要求** をクリックします。
5. パフォーマンスメトリック コンソールにアクセスするには、**監視の開始** をクリックします。
   パフォーマンスメトリック コンソールには、次の詳細が表示されます。
   - 過去 1 分間の平均 CPU
   - 過去 1 分間の平均メモリー使用量

8

アプリとデータ

本項では、Wyse 管理コンソールを使用して、日常的なデバイスアプリケーションタスク、オペレーティングシステムのイメージング、インベントリ管理、およびポリシーの設定を行う方法について説明します。リポジトリー名は、ステータスを示すために色分けされています。

次のタイプのポリシーを、[**アプリとデータ**] ページを使用して設定できます。

- 標準アプリケーション ポリシー - このポリシーを使用すると、単一アプリケーション パッケージをインストールできます。
- 高度なアプリケーション ポリシー - このポリシーを使用すると、複数のアプリケーション パッケージをインストールできます。
- イメージ ポリシー - このポリシーを使用すると、オペレーティング システムをインストールできます。

Thin Client へのアプリケーションポリシーおよびオペレーティングシステムイメージの導入は、特定のタイムゾーンやお使いのデバイスで設定されているタイムゾーンに基づいて、すぐにまたは後で実行するかのスケジュールを設定できます。

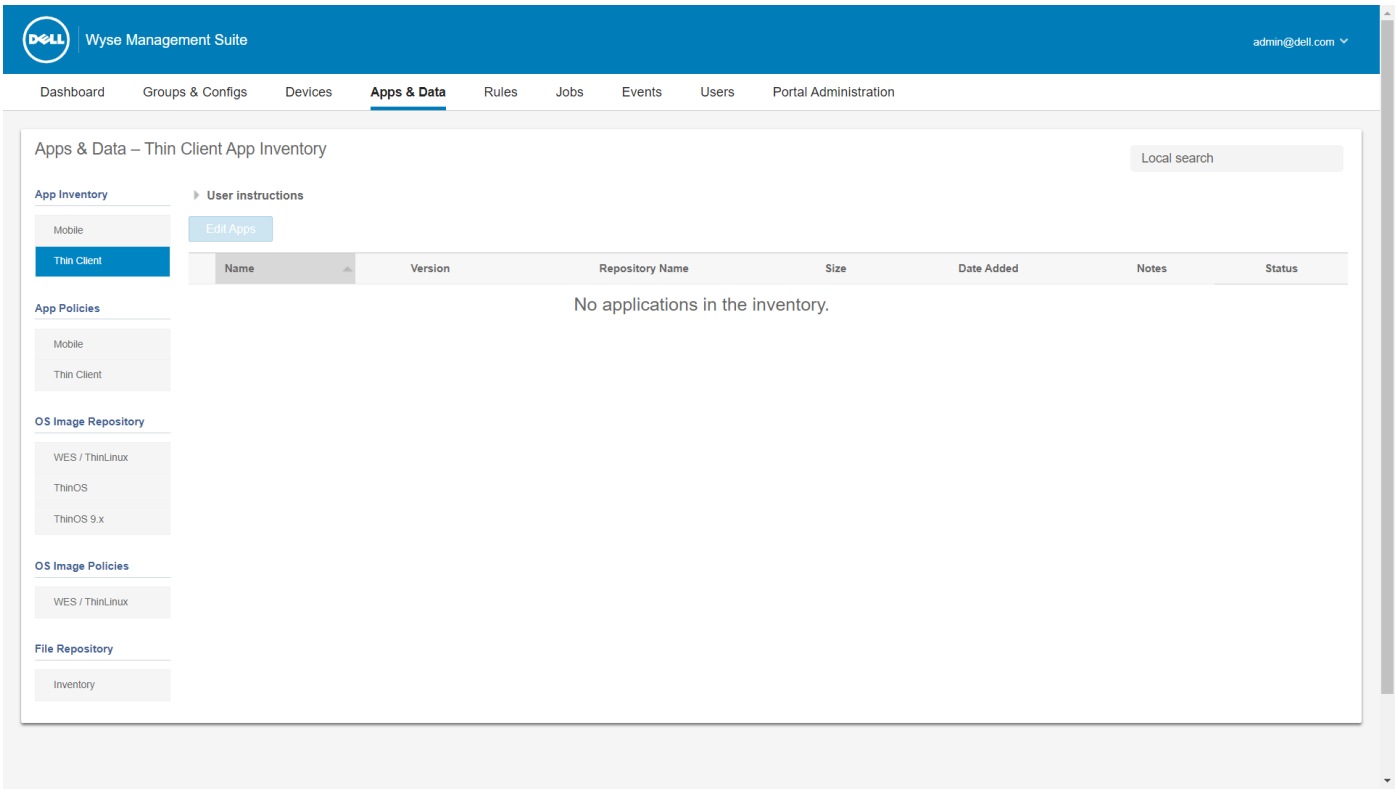


図 5. [アプリとデータ] ページ

トピック：

- アプリケーションポリシー
- イメージポリシー
- ファイル リポジトリーの管理

アプリケーションポリシー

Wyse Management Suite は、次のタイプのアプリケーションインベントリポリシーおよびアプリケーション導入ポリシーをサポートします。

- Thin Client アプリケーション インベントリーの設定
- Wyse Software Thin Client のアプリケーション インベントリーの設定

- Thin Client に対する標準アプリケーション ポリシーの作成および導入
- Thin Client に対する高度なアプリケーション ポリシーの作成および導入
- Wyse Software Thin Client に対する標準アプリケーション ポリシーの作成および導入
- Wyse Software Thin Client に対する高度なアプリケーション ポリシーの作成および導入

Windows ベースのデバイスに関する重要な注意事項：

- Windows ベースのアプリケーション（拡張子が.msi、.exe、.msu、.msp）のインストールをサポートします。

  他の拡張子を持つアプリケーションは、`%sytemdrive%\wyse\WDA" Ex: "C:\wyse\WDA` にダウンロードされます。
- Wyse Management Suite を使用して .exe アプリケーションを展開するには、サイレントインストールの方法に従います。必要に応じて、適切なサイレントパラメータを入力する必要があります。たとえば、「**VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**」と入力します。
- ファイル拡張子が .bat、.cmd、.ps1、.bds のスクリプト導入をサポートします。

  他の拡張子を持つスクリプトは、`%sytemdrive%\wyse\WDA" 例:"C:\wyse\WDA` にダウンロードされます。
- Wyse Management Suite を使用してプッシュされたスクリプトは、非インタラクティブである必要があります。これは、インストール時にユーザーの操作が必要ないことを意味します。
- 高度なアプリケーションポリシーでは、0 以外の値を返すスクリプト / exe がある場合は、失敗と見なされます。
- 高度なアプリケーションポリシーでは、事前インストールが失敗すると、アプリケーションのインストールは継続されません。
- 標準アプリケーションを使用してプッシュされたすべての exe / スクリプトは、正常終了と報告され、エラーコードはジョブのステータスで更新されます。
- 拡張子が msi / msu / msp のアプリケーションの場合、標準エラーコードが報告されます。アプリケーションが REBOOT_REQUIRED を返す場合は、デバイスはさらにもう 1 回再起動します。

Linux デバイスに関する重要な注意事項

- Linux ベースのアプリケーション（ThinLinux 2.0 の場合は拡張子.bin と.deb、Thin Linux 1.0 の場合は拡張子.RPM）のインストールをサポートします。
- 拡張子が .sh の ThinLinux デバイスのスクリプト導入をサポートします。
- 標準または高度なアプリケーションポリシーでは、0 以外の値を返すスクリプト / deb / rpm がある場合は、失敗と見なされます。
- 高度なアプリケーションポリシーでは、事前インストールが失敗した場合、アプリのインストールは継続されません。

Thin Client アプリケーション インベントリーの設定

手順

1. **アプリとデータ** タブをクリックします。
2. 左側のペインで、**アプリインベントリ** > **Thin Client** に移動します。
   Thin Client インベントリ ウィンドウにアプリケーションの詳細が表示されます。
3. インベントリにアプリケーションを追加するには、`<repo-dir>\repository\thinClientApps` フォルダに Thin Client アプリケーションファイルを配置します。
   Wyse Management Suite のリポジトリは、Wyse Management Suite のサーバにすべてのファイルのメタデータを定期的に送信します。
4. アプリケーションを編集するには、次の手順を実行します。
   a) リストからアップロードされたアプリケーションを選択します。
   b) **アプリの編集** をクリックします。
   アプリケーションの編集 ウィンドウが表示されます。
   c) メモを入力します。
   d) **保存** をクリックします。

   メモ: オペレーターがアップロードしたアプリケーションにグローバル サフィックスが追加されます。

   異なるリポジトリーに存在するアプリケーションが一度リストされます。[**リポジトリー名**] 列には、アプリケーションが存在するリポジトリーの数が表示されます。列の上にカーソルを置くと、リポジトリーの名前を表示できます。また、リポジトリーの名前は可用性を指定するために色分けされています。

Wyse Software Thin Client のアプリケーション インベントリーの設定

手順

1. **アプリとデータ** タブをクリックします。
2. 左側のペインで、**アプリインベントリ** > **Wyse Software Thin Client** に移動します。
3. インベントリにアプリケーションを追加するには、`<repo-dir>\repository\softwareTcApps` フォルダに Thin Client アプリケーションファイルを配置します。
   Wyse Management Suite のリポジトリは、Wyse Management Suite のサーバにすべてのファイルのメタデータを定期的に送信します。

Thin Client に対する標準アプリケーション ポリシーの作成および導入

手順

1. ローカルリポジトリで **thinClientApps** に移動して、アプリケーションをフォルダにコピーします。
2. **[アプリとデータ]** > **[アプリ インベントリー]** > **[Thin Client]** の順に移動して、アプリケーションが Wyse Management Suite に登録されていることを確認します。

   メモ: 最近追加したプログラムがアプリインベントリのインタフェースに表示されるまで約 2 分かかります。
3. **[アプリとデータ]** > **[アプリ ポリシー]** > **[Thin Client]** の順に移動します。
4. **ポリシーの追加** をクリックします。
   標準アプリポリシーの追加 ウィンドウが表示されます。
5. **ポリシー名** を入力します。
6. [**グループ**] ドロップダウン リストから、グループを選択します。
7. [**タスク**] ドロップダウン リストから、タスクを選択します。
8. [**OS タイプ**] ドロップダウン リストから、オペレーティング システムを選択します。
9. アプリケーションをフィルターするには、[**拡張子に基づいてファイルをフィルター**] チェックボックスを選択します。
10. [**アプリケーション**] ドロップダウン リストから、アプリケーションを選択します。
    アプリケーション ファイルが複数のリポジトリーで使用可能な場合、リポジトリーの数がファイル名の横に表示されます。
11. 特定のオペレーティングシステムまたはプラットフォームにこのポリシーを導入する場合は、**OS サブタイプフィルタ** または **プラットフォームフィルタ** を選択します。
12. [**ポリシーを自動的に適用**] ドロップダウン リストから、次のいずれかのオプションを選択します。
    - **自動的に適用しない** - このオプションは、ポリシーをデバイスに自動的に適用しません。
    - **ポリシーを新しいデバイスに適用** - このオプションは、選択したグループに属するデバイス、または選択したグループに移動されたデバイスが登録されると、自動的にポリシーを適用します。
    - **チェックイン時にポリシーをデバイスに適用** - このオプションは、チェックイン時に自動的にデバイスに適用されます。

    メモ: Windows ベースのデバイスの場合、サイレント モードでアプリケーションを実行するために、.exe ファイルのサイレント インストールのパラメーターを指定します。たとえば、「VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart」と入力します。
13. 定義した値の時間が経過した後にインストール プロセスを停止するには、[**アプリケーションのインストール タイムアウト**] フィールドに時間 (分) を指定します。デフォルト値は 60 分です。

    メモ: [アプリケーションのインストール タイムアウト] オプションは、Windows Embedded Standard、Wyse Software Thin Client、Linux、Thin Linux デバイスにのみ適用されます。
14. **保存** クリックしてポリシーを作成します。
    メッセージが表示され、管理者はグループに基づいてデバイスでこのポリシーをスケジュールできるようになります。
15. 同じページ上のジョブをスケジュールするには、**はい** を選択します。
16. 次のオプションを任意に選択します。
    - **即時** - サーバは即時ジョブを実行します。

- **デバイスのタイムゾーン** - サーバーは各デバイスのタイムゾーンに 1 つのジョブを作成し、デバイスのタイムゾーンの選択した日付や時刻にジョブをスケジュールします。
- **選択したタイムゾーン** - サーバーは、指定されたタイムゾーンの日付や時刻に実行するジョブを 1 つ作成します。

17. ジョブを作成するには、**プレビュー** をクリックすると、次のページにスケジュールが表示されます。
18. [**ジョブ**] ページに移動して、ジョブのステータスを確認できます。

Thin Client に対する標準アプリケーション ポリシーの作成および導入

手順

1. ローカルリポジトリで **softwareTcApps** に移動して、アプリケーションをフォルダにコピーします。
2. **[アプリとデータ]** > **[アプリ インベントリー]** > **[Wyse Software Thin Client]** の順に移動して、アプリケーションが Wyse Management Suite に登録されていることを確認します。

   メモ: 最近追加したプログラムがアプリインベントリのインタフェースに表示されるまで約 2 分かかります。
3. **ポリシーの追加** をクリックします。
   標準アプリポリシーの追加 ウィンドウが表示されます。
4. **ポリシー名** を入力します。
5. [**グループ**] ドロップダウン リストから、グループを選択します。
6. [**タスク**] ドロップダウン リストから、タスクを選択します。
7. [**OS タイプ**] ドロップダウン リストから、オペレーティング システムを選択します。
8. アプリケーションをフィルターするには、[**拡張子に基づいてファイルをフィルター**] チェックボックスを選択します。
9. [**アプリケーション**] ドロップダウン リストから、アプリケーションを選択します。
   アプリケーション ファイルが複数のリポジトリーで使用可能な場合、リポジトリーの数がファイル名の横に表示されます。
10. 特定のオペレーティングシステムまたはプラットフォームにこのポリシーを導入する場合は、**OS サブタイプフィルタ** または **プラットフォームフィルタ** を選択します。
11. [**ポリシーを自動的に適用**] ドロップダウン リストから、次のいずれかのオプションを選択します。
    - **自動的に適用しない** - このオプションは、ポリシーをデバイスに自動的に適用しません。
    - **ポリシーを新しいデバイスに適用** - このオプションは、選択したグループに属するデバイス、または選択したグループに移動されたデバイスが登録されると、自動的にポリシーを適用します。
    - **チェックイン時にポリシーをデバイスに適用** - このオプションは、チェックイン時に自動的にデバイスに適用されます。

    メモ: Windows ベースのデバイスの場合、サイレント モードでアプリケーションを実行するために、.exe ファイルのサイレント インストールのパラメーターを指定します。たとえば、「VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart」と入力します。
12. 定義した値の時間が経過した後にインストール プロセスを停止するには、[**アプリケーションのインストール タイムアウト**] フィールドに時間 (分) を指定します。デフォルト値は 60 分です。

    メモ: [アプリケーションのインストール タイムアウト] オプションは、Windows Embedded Standard デバイスと Wyse Software Thin Client にのみ適用されます。
13. **保存** クリックしてポリシーを作成します。
    メッセージが表示され、管理者はグループに基づいてデバイスでこのポリシーをスケジュールできるようになります。
14. 同じページ上のジョブをスケジュールするには、**はい** を選択します。
15. 次のオプションを任意に選択します。
    - **即時** - サーバは即時ジョブを実行します。
    - **デバイスのタイムゾーン** - サーバーは各デバイスのタイムゾーンに 1 つのジョブを作成し、デバイスのタイムゾーンの選択した日付や時刻にジョブをスケジュールします。
    - **選択したタイムゾーン** - サーバーは、指定されたタイムゾーンの日付や時刻に実行するジョブを 1 つ作成します。
16. ジョブを作成するには、**プレビュー** をクリックすると、次のページにスケジュールが表示されます。
17. [**ジョブ**] ページに移動して、ジョブのステータスを確認できます。

標準アプリケーション ポリシーを使用して Citrix StoreFront のシングル サインオンを有効にする

Citrix StoreFront のシングル サインオンを有効にするには、次の手順を実行します。

- **シナリオ 1** - Citrix Receiver の現在のバージョンで StoreFront のシングル サインオンを有効にする場合は、次の手順を実行します。
  1. 標準アプリケーション ポリシーを作成して展開し、パラメーター/silent を使用して Citrix Receiver をアンインストールします。
  2. 標準アプリケーション ポリシーを作成して展開し、パラメーター/silent /includeSSON /AutoUpdateCheck = Disabled を使用して Citrix Receiver を再度インストールします。
- **シナリオ 2** - Citrix Receiver をアップグレードし、StoreFront のシングル サインオンを有効にする場合は、次の手順を実行します。
  1. 標準アプリケーション ポリシーを作成して展開し、パラメーター/silent /includeSSON /AutoUpdateCheck = Disabled を使用して Citrix Receiver をアップグレードします。
- **シナリオ 3** - Citrix Receiver をダウングレードし、StoreFront のシングル サインオンを有効にする場合は、次の手順を実行します。
  1. 標準アプリケーション ポリシーを作成して展開し、パラメーター/silent /includeSSON /AutoUpdateCheck = Disabled を使用して Citrix Receiver をダウングレードします。

Thin Client に対する高度なアプリケーション ポリシーの作成および導入

手順

1. 導入するアプリケーションおよびプレ / ポストインストールスクリプト (必要な場合) を、Thin Client にコピーします。
2. アプリケーションおよびプリ / ポストインストールスクリプトを、ローカルリポジトリまたは Wyse Management Suite リポジトリの thinClientApps フォルダに保存します。
3. **[アプリとデータ]** > **[アプリ インベントリー]** > **[Thin Client]** の順に移動して、アプリケーションが登録されていることを確認します。
4. **[アプリとデータ]** > **[アプリ ポリシー]** > **[Thin Client]** の順に移動します。
5. **詳細なポリシーの追加** をクリックします。
   [**詳細なアプリ ポリシーの追加**] ページが表示されます。
6. **ポリシー名** を入力します。
7. [**グループ**] ドロップダウン リストから、グループを選択します。
8. [**サブ グループ**] チェック ボックスを選択して、ポリシーをサブ グループに適用します。
9. [**タスク**] ドロップダウン リストから、タスクを選択します。
10. [**OS タイプ**] ドロップダウン リストから、オペレーティング システムを選択します。
11. アプリケーションをフィルターするには、[**拡張子に基づいてファイルをフィルター**] チェックボックスを選択します。
12. **アプリの追加** をクリックし、**アプリ** の下で 1 つ、または複数のアプリケーションを選択します。各アプリケーションについて、[**プリインストール**]、[**ポストインストール**]、[**パラメーターのインストール**] の下で、プレ/ポストインストール スクリプトを選択できます。
13. アプリケーションが正常にインストールされた後にシステムを再起動したい場合は、**再起動** を選択します。
14. **アプリの追加** をクリックし、ステップを繰り返して複数のアプリケーションを追加します。

    メモ: 最初に失敗したときにアプリケーションポリシーを停止するには、アプリの依存関係を有効にする を選択します。このオプションが選択されていない場合、アプリケーションの失敗がポリシーの実装に影響します。

    アプリケーション ファイルが複数のリポジトリーで使用可能な場合、リポジトリーの数がファイル名の横に表示されます。
15. 特定のオペレーティングシステムまたはプラットフォームにこのポリシーを導入する場合は、**OS サブタイプフィルタ** または **プラットフォームフィルタ** を選択します。
16. メッセージダイアログボックスをクライアントに表示する時間 (分) を指定します。
    クライアントにメッセージが表示され、インストールを開始する前に作業内容を保存する時間が提供されます。
17. ポリシー実施の遅延を有効にするには、[**ポリシー実行の遅延を許可**] チェック ボックスを選択します。このオプションが選択されている場合、以下のドロップダウンメニューが有効になります。

- **遅延あたりの最大時間** ドロップダウンリストから、ポリシーの実行を遅らせることができる最大時間 (1 ~ 24 時間) を選択します。
- **最大遅延** ドロップダウンリストから、ポリシーの実行を遅らせることができる回数 (1 ~ 3 回) を選択します。

18. [**ポリシーを自動的に適用**] ドロップダウン リストから、次のいずれかのオプションを選択します。
    - **自動的に適用しない** - このオプションは、ポリシーをデバイスに自動的に適用しません。
    - **ポリシーを新しいデバイスに適用** - このオプションは、選択したグループに属するデバイス、または選択したグループに移動されたデバイスが登録されると、自動的にポリシーを適用します。
    - **チェックイン時にポリシーをデバイスに適用** - このオプションは、チェックイン時に自動的にデバイスに適用されます。

    メモ: Windows ベースのデバイスの場合、サイレント モードでアプリケーションを実行するために、.exe ファイルのサイレント インストールのパラメーターを指定します。たとえば、「VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart」と入力します。
19. **書き込みフィルタチェックをスキップ** チェックボックスを選択して、書き込みフィルタのサイクルをスキップします。このオプションは、Windows Embedded Standard オペレーティングシステムデバイスおよび Wyse Software Thin Client デバイスに適用されます。
20. 定義した値の時間が経過した後にインストール プロセスを停止するには、[**アプリケーションのインストール タイムアウト**] フィールドに時間 (分) を指定します。デフォルト値は 60 分です。

    メモ: [アプリケーションのインストール タイムアウト] オプションは、Windows Embedded Standard デバイスと Wyse Software Thin Client にのみ適用されます。
21. **保存** クリックしてポリシーを作成します。
    メッセージが表示され、管理者はグループに基づいてデバイスでこのポリシーをスケジュールできるようになります。
22. 同じページ上のジョブをスケジュールするには、**はい** を選択します。
23. 次のオプションを任意に選択します。
    - **即時** - サーバは即時ジョブを実行します。
    - **デバイスのタイムゾーン** - サーバーは各デバイスのタイムゾーンに 1 つのジョブを作成し、デバイスのタイムゾーンの選択した日付や時刻にジョブをスケジュールします。
    - **選択したタイムゾーン** - サーバーは、指定されたタイムゾーンの日付や時刻に実行するジョブを 1 つ作成します。
24. ジョブを作成するには、**プレビュー** をクリックすると、次のページにスケジュールが表示されます。
25. [**ジョブ**] ページに移動して、ジョブのステータスを確認できます。

Wyse Software Thin Client に対する高度なアプリケーション ポリシーの作成および導入

手順

1. 導入するアプリケーションおよびプレ / ポストインストールスクリプト (必要な場合) を、Thin Client にコピーします。
2. アプリケーションおよびプリ/ポスト インストール スクリプトを、ローカル リポジトリーまたは Wyse Management Suite リポジトリーの `softwareTcApps` フォルダーに保存します。
3. **[アプリとデータ]** > **[アプリ インベントリー]** > **[Wyse Software Thin Client]** の順に移動して、アプリケーションが登録されていることを確認します。
4. **[アプリとデータ]** > **[アプリ ポリシー]** > **[Wyse Software Thin Client]** の順に移動します。
5. **詳細なポリシーの追加** をクリックします。
   [**詳細なアプリ ポリシーの追加**] ページが表示されます。
6. **ポリシー名** を入力します。
7. [**グループ**] ドロップダウン リストから、グループを選択します。
8. [**サブ グループ**] チェック ボックスを選択して、ポリシーをサブ グループに適用します。
9. [**タスク**] ドロップダウン リストから、タスクを選択します。
10. [**OS タイプ**] ドロップダウン リストから、オペレーティング システムを選択します。
11. アプリケーションをフィルターするには、[**拡張子に基づいてファイルをフィルター**] チェックボックスを選択します。
12. **アプリの追加** をクリックし、**アプリ** の下で 1 つ、または複数のアプリケーションを選択します。各アプリケーションについて、[**プリインストール**]、[**ポストインストール**]、[**パラメーターのインストール**] の下で、プレ/ポストインストール スクリプトを選択できます。
13. アプリケーションが正常にインストールされた後にシステムを再起動したい場合は、**再起動** を選択します。
14. **アプリの追加** をクリックし、ステップを繰り返して複数のアプリケーションを追加します。

メモ: **最初に失敗したときにアプリケーションポリシーを停止するには、アプリの依存関係を有効にする を選択します。このオプションが選択されていない場合、アプリケーションの失敗がポリシーの実装に影響します。**

アプリケーション ファイルが複数のリポジトリーで使用可能な場合、リポジトリーの数がファイル名の横に表示されます。

15. 特定のオペレーティングシステムまたはプラットフォームにこのポリシーを導入する場合は、**OS サブタイプフィルタ** または **プラットフォームフィルタ** を選択します。
16. メッセージダイアログボックスをクライアントに表示する時間 (分) を指定します。
クライアントにメッセージが表示され、インストールを開始する前に作業内容を保存する時間が提供されます。
17. ポリシー実施の遅延を有効にするには、[**ポリシー実行の遅延を許可**] チェック ボックスを選択します。このオプションが選択されている場合、以下のドロップダウンメニューが有効になります。
    - **遅延あたりの最大時間** ドロップダウンリストから、ポリシーの実行を遅らせることができる最大時間 (1 ~ 24 時間) を選択します。
    - **最大遅延** ドロップダウンリストから、ポリシーの実行を遅らせることができる回数 (1 ~ 3 回) を選択します。
18. [**ポリシーを自動的に適用**] ドロップダウン リストから、次のいずれかのオプションを選択します。
    - **自動的に適用しない** - このオプションは、ポリシーをデバイスに自動的に適用しません。
    - **ポリシーを新しいデバイスに適用** - このオプションは、選択したグループに属するデバイス、または選択したグループに移動されたデバイスが登録されると、自動的にポリシーを適用します。
    - **チェックイン時にポリシーをデバイスに適用** - このオプションは、チェックイン時に自動的にデバイスに適用されます。

    メモ: **Windows ベースのデバイスの場合、サイレント モードでアプリケーションを実行するために、.exe ファイルのサイレント インストールのパラメーターを指定します。たとえば、「VMware-Horizon-Client-4.6.1-6748947.exe /silent / install /norestart」と入力します。**
19. **書き込みフィルタチェックをスキップ** チェックボックスを選択して、書き込みフィルタのサイクルをスキップします。このオプションは、Windows Embedded Standard オペレーティングシステムデバイスおよび Wyse Software Thin Client デバイスに適用されます。
20. 定義した値の時間が経過した後にインストール プロセスを停止するには、[**アプリケーションのインストール タイムアウト**] フィールドに時間 (分) を指定します。デフォルト値は 60 分です。

    メモ: **[アプリケーションのインストール タイムアウト] オプションは、Windows Embedded Standard デバイスと Wyse Software Thin Client にのみ適用されます。**
21. **保存** クリックしてポリシーを作成します。
メッセージが表示され、管理者はグループに基づいてデバイスでこのポリシーをスケジュールできるようになります。
22. 同じページ上のジョブをスケジュールするには、**はい** を選択します。
23. 次のオプションを任意に選択します。
    - **即時** - サーバは即時ジョブを実行します。
    - **デバイスのタイムゾーン** - サーバーは各デバイスのタイムゾーンに 1 つのジョブを作成し、デバイスのタイムゾーンの選択した日付や時刻にジョブをスケジュールします。
    - **選択したタイムゾーン** - サーバーは、指定されたタイムゾーンの日付や時刻に実行するジョブを 1 つ作成します。
24. ジョブを作成するには、**プレビュー** をクリックすると、次のページにスケジュールが表示されます。
25. [**ジョブ**] ページに移動して、ジョブのステータスを確認できます。

イメージポリシー

Wyse Management Suite は、次のタイプのオペレーティングシステムイメージ導入ポリシーをサポートします。

- Windows Embedded Standard オペレーティング システムおよび ThinLinux のイメージのリポジトリーへの追加
- リポジトリーへの ThinOS ファームウェアの追加
- リポジトリーへの ThinOS パッケージ ファイルの追加
- リポジトリーへの ThinOS BIOS ファイルの追加
- リポジトリーへの Teradici ファームウェアの追加
- Windows Embedded Standard および ThinLinux のイメージ ポリシーの作成。

Windows Embedded Standard オペレーティング システムおよび ThinLinux イメージのリポジトリーへの追加

前提条件

- クラウド環境で Wyse Management Suite を使用している場合は、**ポータル管理** > **コンソールの設定** > **ファイルリポジトリ** の順に移動します。[**バージョン 2.0 のダウンロード**] または [**バージョン 1.4 のダウンロード**] をクリックして、`WMS_Repo.exe` ファイルをダウンロードし、Wyse Management Suite リポジトリー インストーラーをインストールします。
- オンプレミス環境で Wyse Management Suite を使用している場合、ローカルリポジトリは Wyse Management Suite のインストールプロセス中にインストールされます。

手順

1. Windows Embedded Standard オペレーティングシステムイメージまたは ThinLinux イメージを、<**リポジトリの場所**>`\repository\osImages\zipped` フォルダにコピーします。

   圧縮フォルダからファイルが解凍され、<**リポジトリの場所**>`\repository\osImages\valid` にファイルがアップロードされます。イメージのサイズに応じて、解凍に数分かかる場合があります。

   メモ: ThinLinux オペレーティングシステムの場合、merlin イメージ (例 : `1.0.7_3030LT_merlin.exe`) をダウンロードして、<リポジトリの場所>`\Repository\osImages\zipped` フォルダにコピーします。

   イメージがリポジトリに追加されます。
2. 登録済みのイメージを表示するには、**[アプリとデータ]** > **[OS イメージ リポジトリー]** > **[WES/ThinLinux]** の順に進みます。

リポジトリーへの ThinOS ファームウェアの追加

手順

1. **アプリ & データ** タブで、**OS イメージリポジトリ** の **ThinOS** をクリックします。
2. [**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 画面が表示されます。
3. ファイルを選択するには、[**参照**] をクリックしてファイルがある場所に移動します。
4. お使いのファイルの説明を入力します。
5. 既存のファイルを上書きする場合は、チェックボックスを選択します。
6. **アップロード** をクリックします。

   メモ: チェックボックスを選択すると、ファイルはリポジトリに追加されますが、グループまたはデバイスのいずれにも割り当てられません。デバイスまたはデバイスのグループにファームウェアを導入するには、それぞれのデバイスまたはグループの設定ページに移動します。

リポジトリーへの ThinOS BIOS ファイルの追加

手順

1. **アプリ & データ** タブで、**OS イメージリポジトリ** の **ThinOS** をクリックします。
2. [**BIOS ファイルの追加**] をクリックします。
   ファイルの追加 画面が表示されます。
3. ファイルを選択するには、[**参照**] をクリックしてファイルがある場所に移動します。
4. お使いのファイルの説明を入力します。
5. 既存のファイルを上書きする場合は、チェックボックスを選択します。
6. BIOS プラットフォーム タイプのドロップダウン リストからプラットフォームを選択します。
7. **アップロード** をクリックします。

   メモ: チェックボックスを選択すると、ファイルはリポジトリに追加されますが、グループまたはデバイスのいずれにも割り当てられません。デバイスまたはデバイスのグループに BIOS ファイルを導入するには、それぞれのデバイスまたはグループの設定ページに移動します。

リポジトリーへの ThinOS パッケージ ファイルの追加

手順

1. **アプリ & データ** タブで、OS イメージリポジトリ の **ThinOS** をクリックします。
2. [**パッケージ ファイルの追加**] をクリックします。
   ファイルの追加 画面が表示されます。
3. ファイルを選択するには、[**参照**] をクリックしてファイルがある場所に移動します。
4. お使いのファイルの説明を入力します。
5. **アップロード** をクリックします。

   メモ: アプリケーションがパブリック リポジトリーに存在している場合は、アプリケーション リファレンスがインベントリーに追加されます。そうでない場合、アプリケーションはパブリック リポジトリーにアップロードされ、リファレンスがインベントリーに追加されます。また、オペレーターがアップロードした ThinOS ファームウェアおよび BIOS パッケージは、テナント管理者が削除することはできません。

リポジトリーへの ThinOS 9.x ファームウェアの追加

手順

1. [**アプリとデータ**] タブで、[OS イメージ リポジトリー] の [**ThinOS 9.x**] をクリックします。
2. [**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 画面が表示されます。
3. ファイルを選択するには、[**参照**] をクリックしてファイルがある場所に移動します。
4. お使いのファイルの説明を入力します。
5. 既存のファイルを上書きする場合は、チェックボックスを選択します。
6. **アップロード** をクリックします。

   メモ: チェックボックスを選択すると、ファイルはリポジトリに追加されますが、グループまたはデバイスのいずれにも割り当てられません。デバイスまたはデバイスのグループにファームウェアを導入するには、それぞれのデバイスまたはグループの設定ページに移動します。

リポジトリーへの ThinOS 9.x パッケージ ファイルの追加

手順

1. [**アプリとデータ**] タブで、[OS イメージ リポジトリー] の [**ThinOS 9.x**] をクリックします。
2. [**パッケージ ファイルの追加**] をクリックします。
   ファイルの追加 画面が表示されます。
3. ファイルを選択するには、[**参照**] をクリックしてファイルがある場所に移動します。
4. お使いのファイルの説明を入力します。
5. **アップロード** をクリックします。

   メモ: アプリケーションがパブリック リポジトリーに存在している場合は、アプリケーション リファレンスがインベントリーに追加されます。そうでない場合、アプリケーションはパブリック リポジトリーにアップロードされ、リファレンスがインベントリーに追加されます。また、オペレーターがアップロードした ThinOS ファームウェアおよび BIOS パッケージは、テナント管理者が削除することはできません。

Windows Embedded Standard および ThinLinux のイメージ ポリシーの作成

手順

1. **アプリとデータ** タブの OS イメージポリシー の下で、**WES/ThinLinux** をクリックします。

2. **ポリシーの追加** をクリックします。
   WES/ThinLinux **ポリシーの追加** ページが表示されます。
3. WES/ThinLinux **ポリシーの追加** ページで、次の手順を実行します。
   a. **ポリシー名** を入力します。
   b. **グループ** ドロップダウンメニューから、グループを選択します。
   c. **OS タイプ** ドロップダウンメニューから、OS タイプを選択します。
   d. **OS サブタイプフィルタ** ドロップダウンメニューから、OS サブタイプフィルタを選択します。
   e. 特定のオペレーティングシステムまたはプラットフォームにイメージを展開する場合は、**OS サブタイプフィルタ** または **プラットフォームフィルタ** を選択します。
   f. **OS イメージ** ドロップダウンメニューから、OS イメージファイルを選択します。
   g. **ルール** ドロップダウンメニューから、イメージポリシーに設定する次のいずれかのルールを選択します。
      - アップグレードのみ
      - ダウングレードを許可
      - このバージョンを強制
   h. [**ポリシーを自動的に適用**] ドロップダウン メニューから、次のオプションのいずれかを選択します。
      - 自動的に適用しない - イメージポリシーは Wyse Management Suite に登録されたデバイスに自動的に適用されません。
      - 新規デバイスにポリシーを適用 - イメージポリシーは Wyse Management Suite に登録された新しいデバイスに適用されます。
      - チェックイン時にポリシーをデバイスに適用 - イメージポリシーは、Wyse Management Suite に登録された新しいデバイスのチェックイン時に適用されます。
4. **保存** をクリックします。

ファイル リポジトリーの管理

このセクションでは、壁紙、ロゴ、EULA テキスト ファイル、Windows ワイヤレス プロファイル、証明書ファイルなどのファイル リポジトリーのインベントリーを表示および管理できます。

手順

1. **ファイルリポジトリ** の下の **アプリとデータ** タブで、**インベントリ** をクリックします。
2. **ファイルの追加** をクリックします。
   ファイルの追加 画面が表示されます。
3. ファイルを選択するには、[**参照**] をクリックしてファイルがある場所に移動します。
4. **タイプ** ドロップダウンメニューからファイルのタイプに合った次のオプションのいずれかを選択します。
   - 証明書
   - 壁紙
   - ロゴ
   - EULA テキストファイル
   - Windows ワイヤレスプロファイル
   - INI ファイル
   - ロケール
   - プリンタマッピング
   - フォント
   - ホスト
   - ルール

   メモ: アップロードが可能なファイルの最大サイズおよびサポートされるフォーマットを表示するには、情報 (i) アイコンをクリックします。
5. 既存のファイルを上書きする場合は、チェックボックスを選択します。
   メモ: チェックボックスを選択すると、ファイルはリポジトリに追加されますが、グループまたはデバイスのいずれにも割り当てられません。ファイルを割り当てるには、それぞれのデバイス設定ページに移動します。
6. **アップロード** をクリックします。

マーケティンググループに属するすべてのデバイスの壁紙を変更する方法

手順

1. [**アプリとデータ**] タブに移動します。
2. 左側ペインのナビゲーションバーで、**インベントリ** を選択します。
3. **ファイルの追加** ボタンをクリックします。
4. 壁紙として使用するイメージを参照して選択します。
5. タイプには、**壁紙** を選択します。
6. 説明を入力して [**アップロード**] をクリックします。

新しい壁紙を割り当てて、グループの設定ポリシーを変更するには、次の操作を行います。

1. [**グループ&設定**] ページに移動します。
2. ポリシーグループを選択します。
3. **ポリシーの編集** をクリックして、**WES** を選択します。
4. **デスクトップエクスペリエンス** をクリックし、**この項目を設定する** をクリックします。
5. **デスクトップの壁紙** を選択します。
6. ドロップダウンリストから、壁紙ファイルを選択します。
7. **保存して公開** をクリックします。

ジョブ をクリックし、設定ポリシーのステータスを確認します。**詳細** 列内のステータスフラグの横の番号をクリックして、デバイスのステータスを確認します。

9

ルールの管理

この項では、Wyse Management Suite コンソールでルールを追加および管理する方法について説明します。次のフィルタオプションが利用可能です。

- **登録**
- **管理対象外のデバイスの自動割り当て**
- **アラート通知**

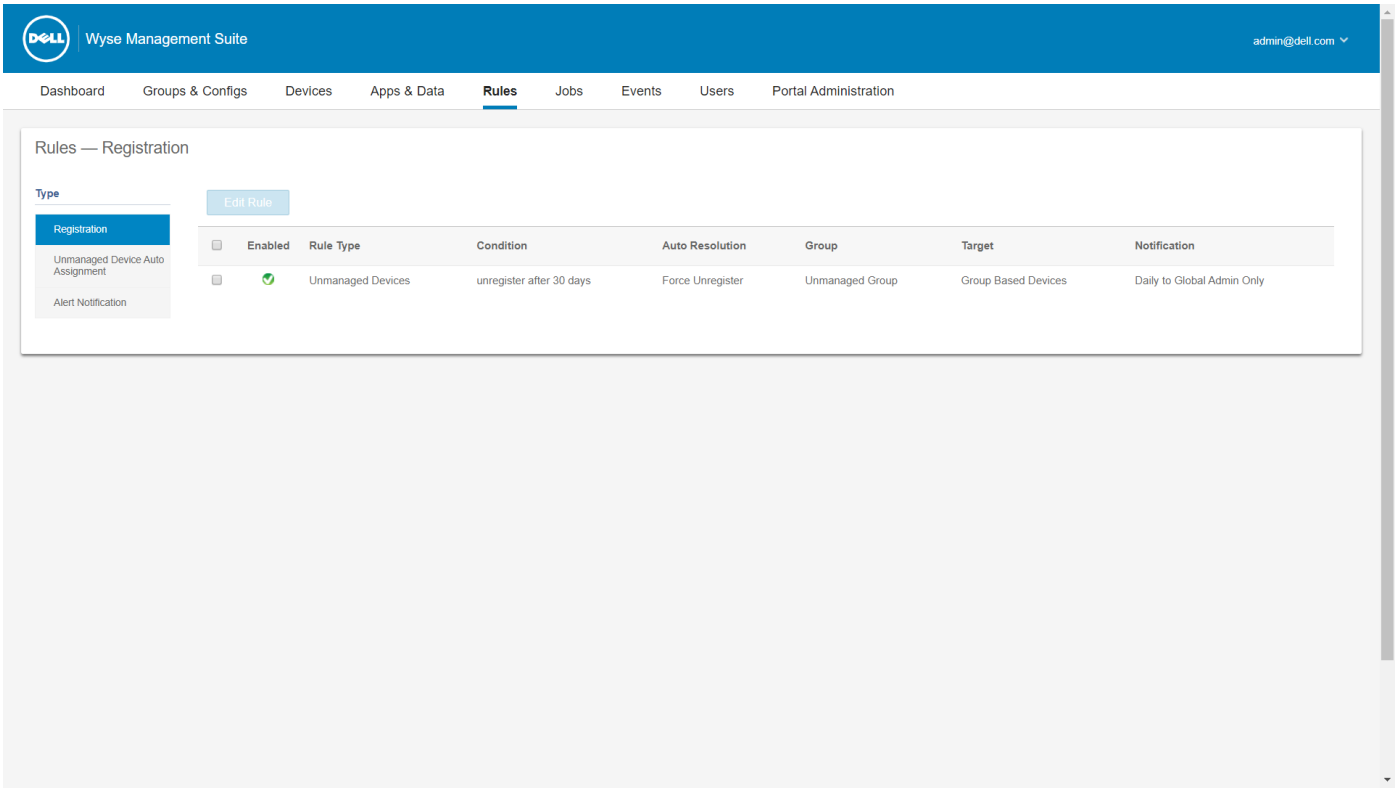


図 6. ルール ページ

トピック：

- 登録ルールの編集
- 管理対象外デバイスの自動割り当てルールの作成
- 管理対象外のデバイスの自動割り当てルールの編集
- 管理対象外のデバイスの自動割り当てルールの無効化と削除
- ルールの順序の保存
- アラート通知のルールの追加
- アラート通知ルールの編集

登録ルールの編集

登録 オプションを使用して、管理対象外のデバイスのルールを設定します。

手順

1. **ルール** をクリックします。
   ルール ページが表示されます。

2. [**登録**] をクリックし、管理対象外デバイスのオプションを選択します。
3. **ルールの編集** をクリックします。
   ルールの編集 ウィンドウが表示されます。

   次の詳細を表示できます。

   - ルール
   - 説明
   - デバイスターゲット
   - グループ
4. ドロップダウンメニューから、**通知ターゲット** オプションを適用するターゲットクライアントと、**通知頻度** オプションを適用する期間を選択します。

   メモ: 通知の頻度は、ターゲットデバイスに対して、4 時間毎、12 時間ごと、毎日、または毎週に設定することができます。
5. ルールを適用するまでの日数を、**ルール適用までの期間 (1 ~ 30 日)** ボックスに入力します。

   メモ: デフォルトでは、管理対象外デバイスの登録は 30 日後に登録解除されます。
6. **保存** をクリックします。

管理対象外デバイスの自動割り当てルールの作成

手順

1. **ルール** タブをクリックします。
2. **管理対象外のデバイスの自動割り当て** オプションを選択します。
3. **ルールの追加** タブをクリックします。
4. **名前**を入力し、**宛先グループ**を選択します。
5. [**条件を追加**] オプションをクリックして、割り当てられたルールの条件を選択します。
6. **保存** をクリックします。

   ルールは、管理対象外グループリストに表示されます。このルールは自動的に適用され、デバイスは宛先グループに一覧表示されます。

   メモ: ルールは、[登録保留中] 状態のデバイスには適用されません。

管理対象外のデバイスの自動割り当てルールの編集

手順

1. **ルール** タブをクリックします。
2. **管理対象外のデバイスの自動割り当て** オプションを選択します。
3. ルールを選択して、[**編集**] オプションをクリックします。
4. **名前**を入力し、**宛先グループ**を選択します。
5. [**条件を追加**] オプションをクリックして、割り当てられたルールの条件を選択します。
6. **保存** をクリックします。

管理対象外のデバイスの自動割り当てルールの無効化と削除

手順

1. **ルール** タブをクリックします。
2. **管理対象外のデバイスの自動割り当て** オプションを選択します。
3. ルールを選択し、[**ルールの無効化**] オプションをクリックします。
   選択したルールが無効になります。

4. 無効になったルールを選択し、[**無効化したルールを削除する**] オプションをクリックします。
   ルールが削除されます。

ルールの順序の保存

前提条件

複数のルールがある場合、デバイスで適用されるルールの順序を変更することができます。

手順

1. **ルール** タブをクリックします。
2. **管理対象外のデバイスの自動割り当て** オプションを選択します。
3. 移動したいルールを選択し、一番上の順序に移動します。
4. **ルールの順序を保存** をクリックします。

   メモ: IPV6 プレフィックス ルールの順序を変更することはできません。

アラート通知のルールの追加

手順

1. **ルール** タブをクリックします。
2. **アラート通知** オプションを選択します。
3. **ルールの追加** をクリックします。
   ルールの追加 ウィンドウが表示されます。
4. **ルール** ドロップダウンリストで、ルールを選択します。
5. **説明** を押します。
6. **グループ** ドロップダウンリストから、希望するオプションを選択します。
7. ドロップダウンメニューから、**通知ターゲット** を適用するターゲットデバイスと、**通知頻度** を適用する期間を選択します。
8. **保存** をクリックします。

アラート通知ルールの編集

手順

1. **ルール** タブをクリックします。
2. **アラート通知** オプションを選択します。
3. **ルールの編集** をクリックします。
   ルールの編集 ウィンドウが表示されます。
4. **ルール** ドロップダウンリストで、ルールを選択します。
5. **説明** を押します。
6. **グループ** ドロップダウンリストで、グループを選択します。
7. ドロップダウンリストで、**通知ターゲット** を適用するターゲットデバイスと、**通知頻度** を適用する期間を選択します。
8. **保存** をクリックします。

10

ジョブの管理

この項では、管理コンソールでジョブをスケジュールおよび管理する方法について説明します。

このページでは、次のフィルタリングオプションに基づいてジョブを参照できます。

- **設定グループ** - ドロップダウンメニューから、設定グループタイプを選択します。
- **スケジュール元** - ドロップダウンメニューから、スケジュールアクティビティを実行するスケジューラを選択します。利用できるオプションは次のとおりです。
  - システム管理者
    - アプリポリシー
    - イメージポリシー
    - デバイスコマンド
  - システム
    - グループ設定の公開
    - その他
- **OS タイプ** - ドロップダウンメニューから、オペレーティングシステムを選択します。利用できるオプションは次のとおりです。
  - ThinOS
  - WES
  - Linux
  - Thin Linux
  - Wyse Software Thin Client
- **ステータス** - ドロップダウンメニューから、ジョブのステータスを選択します。利用できるオプションは次のとおりです。
  - スケジュール済み
  - 実行中 / 進行中
  - 完了
  - キャンセル済み
  - 失敗
- **詳細なステータス** - ドロップダウンメニューから、詳細のステータスを選択します。利用できるオプションは次のとおりです。
  - 失敗
  - 保留
  - 進行中
  - キャンセル
  - 完了
- **追加アクション** - ドロップダウンメニューから、**BIOS 管理者パスワードを同期する** オプションを選択します。BIOS 管理者パスワードジョブを同期する ウィンドウが表示されます。

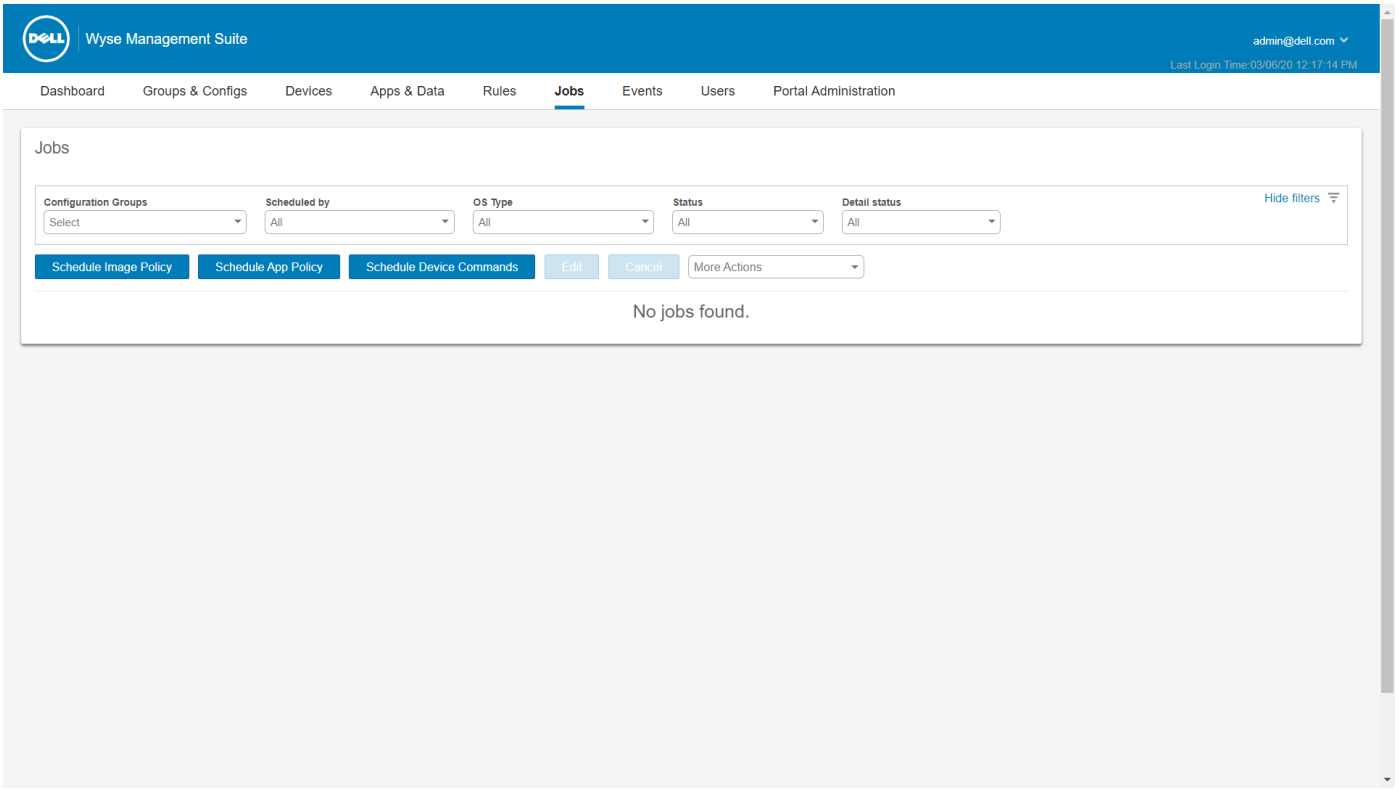


図 7. [ジョブ] ページ

トピック：

- BIOS 管理者パスワードを同期する
- フィルターを使用してスケジュールされたジョブの検索
- デバイス コマンド ジョブのスケジュール
- イメージ ポリシーのスケジュール
- アプリケーション ポリシーのスケジュール

BIOS 管理者パスワードを同期する

手順

1. **ジョブ** をクリックします。
   ジョブ ページが表示されます。
2. **追加アクション** ドロップダウンメニューから、**BIOS 管理者パスワードを同期する** オプションを選択します。
   BIOS 管理者パスワードジョブを同期する ウィンドウが表示されます。
3. パスワードを入力します。パスワードには、最低 4 文字、最大 32 文字を指定する必要があります。
4. **パスワードの表示** チェックボックスを選択して、パスワードを表示します。
5. **OS タイプ** ドロップダウンメニューから、希望するオプションを選択します。
6. **プラットフォーム** ドロップダウンメニューから、希望するオプションを選択します。
7. ジョブの名前を表示します。
8. **グループ** ドロップダウンメニューから、希望するオプションを選択します。
9. [**すべてのサブグループを含める**] チェック ボックスを選択し、サブグループを含めます。
10. **説明** ボックスに説明を入力します。
11. **プレビュー** をクリックします。

フィルターを使用してスケジュールされたジョブの検索

この項では、スケジュールされたジョブの検索方法と、管理コンソールでジョブを管理する方法について説明します。

手順

1. **ジョブ** をクリックします。
   ジョブ ページが表示されます。
2. **設定グループ** ドロップダウンメニューから、デフォルトポリシーグループまたは、管理者によって追加されたグループのどちらかを選択します。
3. **スケジュール元** ドロップダウンメニューから、スケジュールアクティビティを実行するスケジューラを選択します。
   利用できるオプションは次のとおりです。
   - システム管理者
     - アプリポリシー
     - イメージポリシー
     - デバイスコマンド
   - システム
     - グループ設定の公開
     - その他
4. **OS タイプ** ドロップダウンメニューから、オペレーティングシステムを選択します。
   利用できるオプションは次のとおりです。
   - ThinOS
   - WES
   - Linux
   - Thin Linux
   - Wyse Software Thin Client
   - Teradici - プライベート クラウド
5. **ステータス** ドロップダウンメニューから、ジョブのステータスを選択します。
   利用できるオプションは次のとおりです。
   - スケジュール済み
   - 実行中 / 進行中
   - 完了
   - キャンセル済み
   - 失敗
6. **詳細なステータス** ドロップダウンメニューから、詳細のステータスを選択します。
   利用できるオプションは次のとおりです。
   - 失敗
   - 保留
   - 進行中
   - キャンセル
   - 完了
7. **追加アクション** ドロップダウンメニューから、**BIOS 管理者パスワードを同期する** オプションを選択します。
   BIOS 管理者パスワードジョブを同期する ウィンドウが表示されます。詳細については、「BIOS 管理者パスワードを同期する」を参照してください。

デバイス コマンド ジョブのスケジュール

手順

1. **ジョブ** ページで、**デバイスコマンドジョブのスケジュール** をクリックします。
   デバイスのコマンドジョブ 画面が表示されます。

2. [**コマンド**] ドロップダウン リストから、コマンドを選択します。利用できるオプションは次のとおりです。
   - 再起動
   - Wake on LAN
   - シャットダウン
   - クエリ

   デバイス コマンドは定期ジョブです。選択した曜日と特定の時間に、選択したデバイスにコマンドが送信されます。
3. ドロップダウンリストから、オペレーティングシステムのタイプを選択します。
4. ジョブの名前を表示します。
5. ドロップダウンリストから、グループ名を選択します。
6. ジョブの説明を入力します。
7. ドロップダウンリストから、日付または時刻を選択します。
8. 次の詳細を入力または選択します。
   - **有効** - 開始および終了の日付を入力します。
   - **開始時間** - 開始および終了時刻を入力します。
   - **指定日（複数可）** - 曜日を選択します。
9. **プレビュー** オプションをクリックし、スケジュールされたジョブの詳細を表示します。
10. 次のページで、**スケジュール** オプションをクリックします。

イメージ ポリシーのスケジュール

イメージポリシーに定期ジョブはありません。各コマンドは、デバイスによって異なります。

手順

1. **ジョブ** ページをクリックして、**イメージポリシーのスケジュール** オプションをクリックします。
   イメージアップデートジョブ 画面が表示されます。
2. ドロップダウンリストから、ポリシーを選択します。
3. ジョブの説明を入力します。
4. ドロップダウンリストから、日付または時刻を選択します。
5. 次の詳細を入力または選択します。
   - **有効** - 開始および終了の日付を入力します。
   - **開始時間** - 開始および終了時刻を入力します。
   - **指定日（複数可）** - 曜日を選択します。
6. **プレビュー** オプションをクリックし、スケジュールされたジョブの詳細を表示します。
7. **スケジュール** オプションをクリックし、ジョブを開始します。

アプリケーション ポリシーのスケジュール

アプリケーションポリシーは定期ジョブではありません。各コマンドは、デバイスによって異なります。

手順

1. **ジョブ** ページで、**アプリケーションポリシーのスケジュール** オプションをクリックします。
   アプリポリシージョブ 画面が表示されます。
2. ドロップダウンリストから、ポリシーを選択します。
3. ジョブの説明を入力します。
4. ドロップダウンリストから、日付または時刻を選択します。
5. 次の詳細を入力または選択します。
   - **有効** - 開始および終了の日付を入力します。
   - **開始時間** - 開始および終了時刻を入力します。
   - **指定日（複数可）** - 曜日を選択します。
6. **プレビュー** オプションをクリックし、スケジュールされたジョブの詳細を表示します。
7. 次のページで、**スケジュール** オプションをクリックします。

11

イベントの管理

[**イベント**] ページでは、管理コンソールを使用して、管理システムですべてのイベントとアラートを表示できます。また、システム監査の目的のためにイベントとアラートの監査を表示する手順についても説明します。

イベントとアラートの概要は、システムでのできごとの読みやすい日次概要を取得するためにも使用します。**監査** ウィンドウでは、情報を標準的な監査ログ表示に整列します。タイムスタンプ、イベントタイプ、ソース、および各イベントの説明を時間順に表示できます。

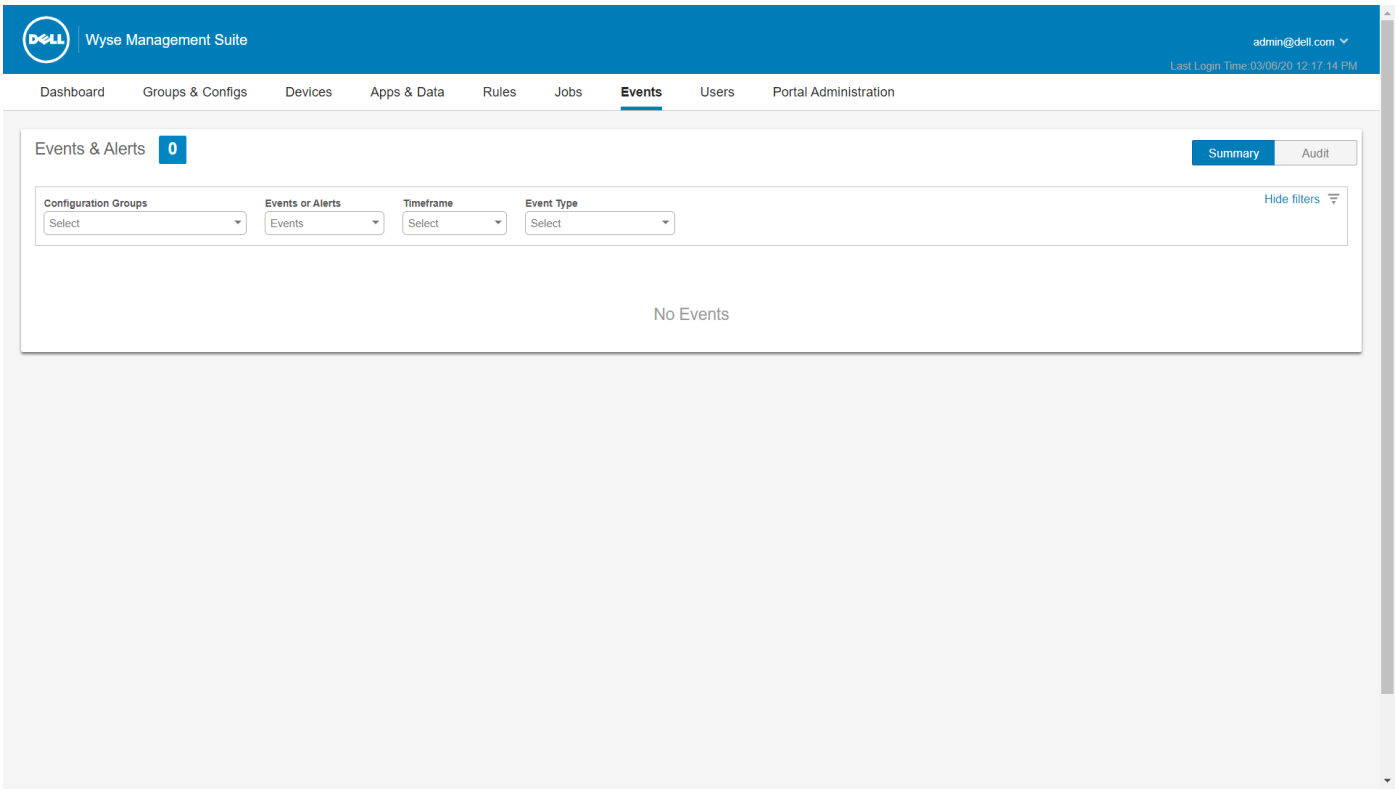


図 8. [イベント] ページ

トピック：

- フィルターを使用したイベントまたはアラートの検索
- イベントの概要の表示
- 監査ログの表示

フィルターを使用したイベントまたはアラートの検索

手順

1. **イベント** をクリックします。
   イベント ページが表示されます。
2. **設定グループ** ドロップダウンメニューから、デフォルトポリシーグループまたは、管理者によって追加されたグループのどちらかを選択します。
3. **イベントまたはアラート** ドロップダウンメニューから、次のオプションのいずれかを選択します。

- イベント
- 現在のアラート
- アラート履歴

4. **時間枠** ドロップダウンメニューから、次のいずれかのオペレーティングシステムを選択します。

   このオプションを使用すると、特定の時間枠で発生するイベントを表示できるようになります。利用できるドロップダウンメニューのオプションは次のとおりです。

   - 今日
   - 昨日
   - 今週
   - カスタム

5. [**イベント タイプ**] ドロップダウン メニューから、オペレーティング システムを選択します。

   すべてのイベントは、いずれかのグループに分類されます。利用できるドロップダウンメニューのオプションは次のとおりです。

   - アクセス
   - 登録
   - 設定
   - リモートコマンド
   - 管理
   - コンプライアンス

イベントの概要の表示

イベント & アラート ウィンドウには、システムで実行されたすべてのイベントおよびアラートが表示されます。**イベント** > **概要** の順に移動します。

監査ログの表示

監査 ウィンドウでは、情報を標準的な監査ログ表示に整列します。タイムスタンプ、イベントタイプ、ソース、および各イベントの説明を時間順に表示できます。

手順

1. **イベント** > **監査** の順に移動します。
2. **設定グループ** ドロップダウンリストから、監査ログを表示するグループを選択します。
3. **時間枠** ドロップダウンリストから、該当する期間中に発生したイベントを表示する期間を選択します。

   メモ: 監査ファイルは翻訳されておらず、英語のみで提供されています。

12

ユーザーの管理

このセクションでは、管理コンソールで日常的なユーザー管理タスクを実行する方法について説明します。ユーザーには、次の 2 つのタイプがあります。

- **管理者** - Wyse Management Suite 管理者は、グローバル管理者、グループ管理者、またはビューアの役割に割り当てることができます。
  - グローバル管理者は Wyse Management Suite のすべての機能に対するアクセス権があります。
  - グループ管理者は、自分に割り当てられている特定のグループのすべての資産および機能に対するアクセス権があります。
  - ビューアにはすべてのデータに読み取り専用のアクセス権があり、シャットダウンや再起動など、特定のリアルタイムコマンドをトリガーする許可を割り当てることができます。

  管理者を選択する場合は、次のいずれの操作も実行できます。

  - 管理者の追加
  - 管理者の編集
  - 管理者のアクティブ化
  - 管理者の非アクティブ化
  - 管理者の削除
  - 管理者のロック解除
- **割り当て解除された管理者**：AD サーバーからインポートされたユーザーは、[**割り当て解除された管理者**] ページに表示されます。これらのユーザーには後でポータルから役割を割り当てることができます。

  ユーザーの管理を適切かつ迅速に行うには、使用可能なフィルタオプションに基づいて、希望するユーザーを選択します。**管理対象外のユーザー**を選択する場合は、次のいずれの操作も実行できます。

  - ユーザーの編集
  - ユーザーのアクティブ化
  - ユーザーの非アクティブ化
  - ユーザーの削除

メモ: .CSV ファイルからユーザーをインポートするには、[一括インポート] をクリックします。

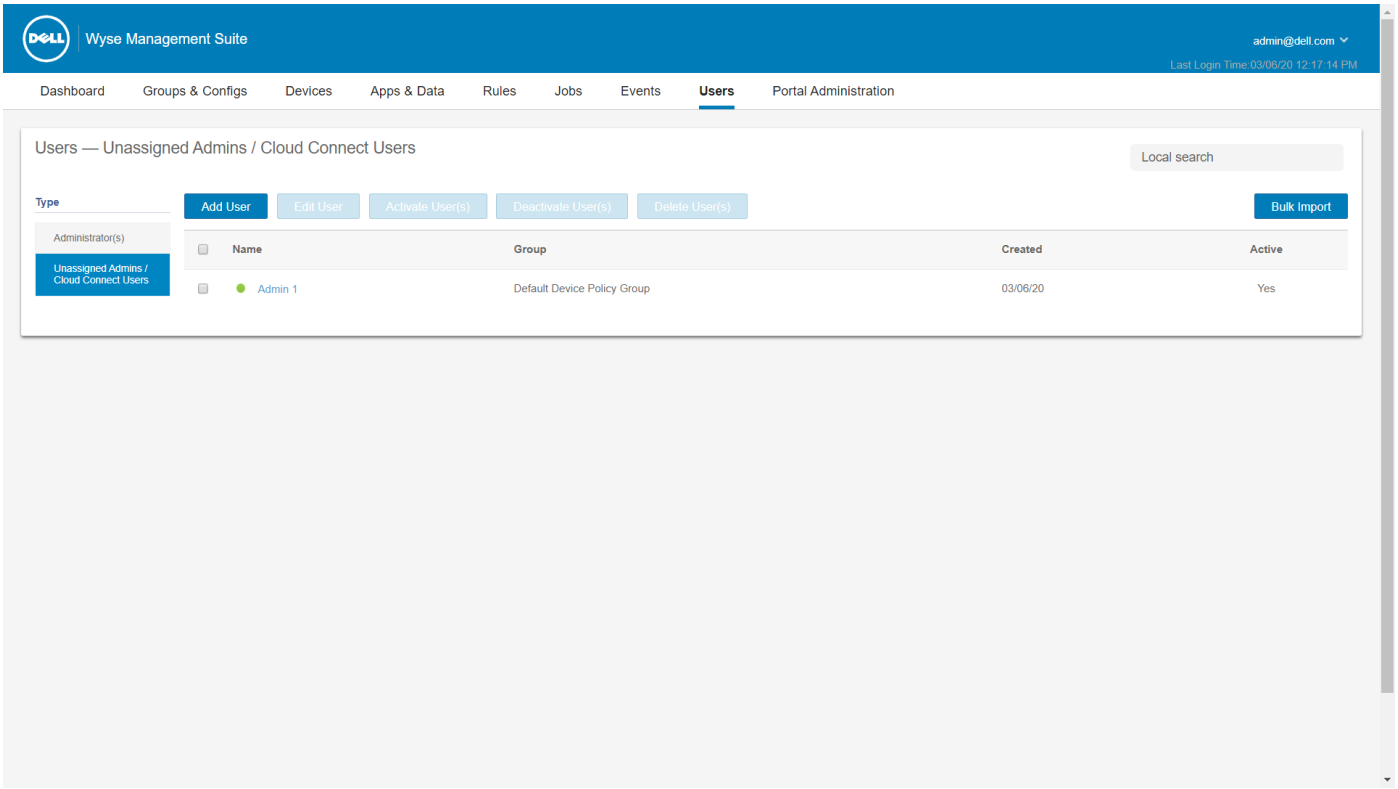


図 9. [ユーザー] ページ

トピック：

- 管理者プロファイルの新規追加
- 管理対象外デバイスの自動割り当てルールの作成
- 管理者プロファイルの編集
- 管理者プロファイルの非アクティブ化
- 管理者プロファイルの削除
- ユーザー プロファイルの編集
- CSV ファイルのインポート

管理者プロファイルの新規追加

手順

1. **ユーザー** をクリックします。
2. **管理者** をクリックします。
3. **管理者の追加** をクリックします。
   新規管理ユーザー ウィンドウが表示されます。
4. 電子メール ID とユーザー名をそれぞれのフィールドに入力します。
5. 電子メールに記載されているのと同じユーザー名を使用するには、チェックボックスを選択します。
6. 次の手順のいずれか 1 つを実行します。
   - **個人情報** タブをクリックした場合は、次の詳細情報を入力します。
     - 名
     - 姓
     - 役職
     - 携帯電話番号
   - **役割** タブをクリックした場合は、次の詳細情報を入力します。
     a. **役割** セクションの **役割** ドロップダウンリストから、**管理者役割** を選択します。

- グローバル管理者
- グループ管理者
- ビューア

  メモ: 管理者役割 をビューア として選択した場合は、次の管理タスクが表示されます。

  - **デバイスのクエリ**
  - **デバイスの登録解除**
  - **デバイスの再起動 / シャットダウン**
  - **グループ割り当ての変更**
  - **リモートシャドー**
  - **デバイスのロック**
  - **デバイスの消去**
  - **メッセージの送信**
  - **WOL デバイス**

b. **パスワード** セクションで、次の手順を実行します。

1. カスタムパスワードを入力します。
2. ランダムなパスワードを生成するには、**ランダムパスワードの生成** ラジオボタンを選択します。

7. **保存** をクリックします。

管理対象外デバイスの自動割り当てルールの作成

手順

1. **ルール** タブをクリックします。
2. **管理対象外のデバイスの自動割り当て** オプションを選択します。
3. **ルールの追加** タブをクリックします。
4. **名前** を入力し、**宛先グループ** を選択します。
5. **条件を追加** オプションをクリックして、割り当てられたルールの条件を選択します。
6. **保存** をクリックします。

   ルールは、管理対象外グループリストに表示されます。このルールは自動的に適用され、デバイスは宛先グループに一覧表示されます。

管理者プロファイルの編集

手順

1. **ユーザー** をクリックします。
2. **管理者** をクリックします。
3. **管理者の編集** をクリックします。
   管理ユーザーの編集 ウィンドウが表示されます。
4. 電子メール ID とユーザー名をそれぞれのフィールドに入力します。

   メモ: ログイン名をアップデートすると、コンソールから強制的にログアウトされます。アップデートしたアカウントログイン名を使用して、コンソールにログインします。
5. 次の手順のいずれか 1 つを実行します。
   - **個人情報** タブをクリックした場合は、次の詳細情報を入力します。
     - 名
     - 姓
     - 役職
     - 携帯電話番号
   - **役割** タブをクリックした場合は、次の詳細情報を入力します。

     a. **役割** セクションの **役割** ドロップダウンリストから、**管理者役割** を選択します。
     b. **パスワード** セクションで、次の手順を実行します。

1. カスタムパスワードを入力します。
2. ランダムなパスワードを生成するには、**ランダムパスワードの生成** ラジオボタンを選択します。

6. **保存** をクリックします。

管理者プロファイルの非アクティブ化

管理者プロファイルを非アクティブ化すると、コンソールにログインできなくなり、登録済みのデバイスのリストから、アカウントが削除されます。

手順

1. **ユーザー** をクリックします。
2. **管理者** をクリックします。
3. リストから、ユーザーを選択して **管理者の非アクティブ化** をクリックします。
   アラートウィンドウが表示されます。
4. **OK** をクリックします。

管理者プロファイルの削除

このタスクについて

プロファイルを削除するには、先に管理者を非アクティブ化しておく必要があります。管理者プロファイルを削除するには、次の操作を行います。

手順

1. **ユーザー** をクリックします。
2. **管理者** をクリックします。
3. 削除したい単独または複数の管理者のチェックボックスを選択します。
4. **管理者の削除** をクリックします。
   アラート ウィンドウが表示されます。
5. 削除の理由を入力して **削除** リンクを有効にします。
6. **削除** をクリックします。

ユーザー プロファイルの編集

手順

1. **ユーザー** をクリックします。
2. **割り当て解除された管理者** をクリックします。
3. **ユーザーの編集** をクリックします。
   管理ユーザーの編集 ウィンドウが表示されます。
4. 電子メール ID とユーザー名をそれぞれのフィールドに入力します。

   メモ: ログイン名をアップデートすると、コンソールから強制的にログアウトされます。アップデートしたアカウントログイン名を使用して、コンソールにログインします。
5. 次の手順のいずれか 1 つを実行します。
   - **個人情報** タブをクリックした場合は、次の詳細情報を入力します。
     - 名
     - 姓
     - 役職
     - 携帯電話番号
   - **役割** タブをクリックした場合は、次の詳細情報を入力します。
     a. **役割** セクションの **役割** ドロップダウンリストから、**管理者役割** を選択します。
     b. **パスワード** セクションで、次の手順を実行します。

1. カスタムパスワードを入力します。
2. ランダムなパスワードを生成するには、**ランダムパスワードの生成** ラジオボタンを選択します。

6. **保存** をクリックします。

CSV ファイルのインポート

手順

1. **ユーザー** をクリックします。
   ユーザー ページが表示されます。
2. **割り当て解除された管理者** オプションを選択します。
3. **一括インポート** をクリックします。
   一括インポート ウィンドウが表示されます。
4. **参照** をクリックして CSV ファイルを選択します。
5. **インポート** をクリックします。

13

ポータル管理

本項には、システムのセットアップと管理に必要なシステム管理タスクの概要が含まれます。

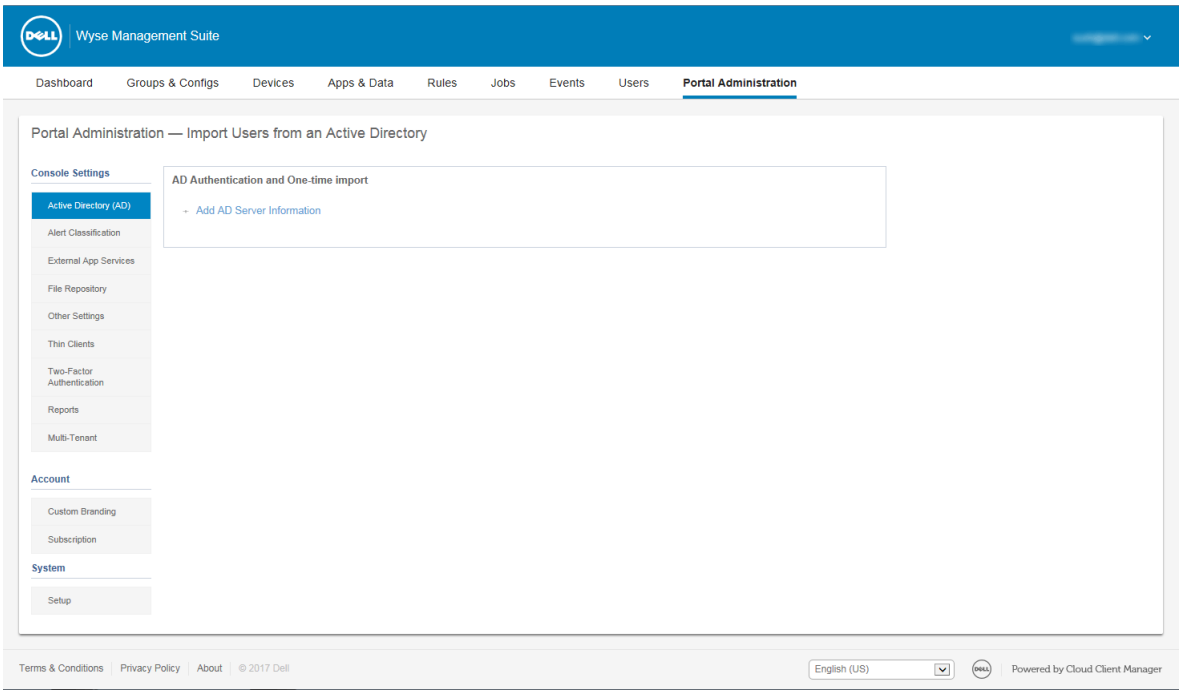


図 10. ポータル管理

トピック：

- Wyse Management Suite プライベート クラウドへの Active Directory サーバー情報の追加
- Active Directory によるパブリック クラウドへのユーザーのインポート
- アラート分類
- アプリケーション プログラミング インターフェイス（API）アカウントの作成
- Wyse Management Suite ファイル リポジトリーへのアクセス
- その他の設定
- Teradici 設定の管理
- 二要素認証の有効化
- マルチテナントアカウントの有効化
- レポートの生成
- カスタムブランド化の有効化
- システム セットアップの管理

Wyse Management Suite プライベート クラウドへの Active Directory サーバー情報の追加

Active Directory ユーザーを Wyse Management Suite プライベート クラウドにインポートできます。

手順

1. Wyse Management Suite プライベートクラウドにログインします。
2. **[ポータル管理]** > **[コンソール設定]** > **[Active Directory（AD）]** の順に移動します。

3. **AD サーバ情報の追加** リンクをクリックします。
4. **AD サーバ名**、**ドメイン名**、**サーバ URL**、**ポート** などのサーバの詳細を入力します。
5. **保存** をクリックします。
6. **インポート** をクリックします。
7. ユーザー名とパスワードを入力します

   メモ: グループおよびユーザーを検索するには、検索ベース および グループ名に含む オプションに基づいてフィルタを適用します。次のように値を入力します。

   - **OU=<OU Name>、たとえば、次のとおりです。OU=TestOU**
   - **DC=<Child Domain>, DC=<Parent Domain>, DC=com,、たとえば、次のとおりです。DC=Skynet, DC=Alpha, DC=Com**

   カンマの後にスペースを入力できますが、一重または二重引用符は使用できません。
8. **ログイン** をクリックします。
9. **ユーザーグループ** ページで、**グループ名** をクリックし、グループ名を入力します。
10. [**検索**] フィールドに選択するグループ名を入力します。
11. グループを選択します。
    選択されたグループがページの右側のペインに移動します。
12. **次へ** をクリックします。
13. **ユーザーのインポート** をクリックします。

    メモ: 無効な名前を指定した場合、または姓を指定しない場合、または名前として電子メールアドレスを指定した場合、エントリを Wyse Management Suite にインポートできません。これらのエントリは、ユーザーのインポートプロセスでスキップされます。

    Wyse Management Suite ポータルには、インポートされた Active Directory ユーザーの数を含む確認メッセージが表示されます。インポートされた Active Directory ユーザーは、**ユーザー タブ割り当て解除された管理者** にリストされます。
14. 異なる役割やパーミッションを割り当てるには、ユーザーを選択して、**ユーザーの編集** をクリックします。

    Active Directory ユーザーに役割を割り当てた後は、それらのユーザーは **ユーザー** ページの **管理者** タブに移動されます。

次の手順

Active Directory ユーザーは、ドメイン資格情報を使用して Wyse Management Suite 管理ポータルにログインすることができます。Wyse Management Suite ポータルにログインするには、次の手順を実行します。

1. Wyse Management Suite 管理ポータルを開始します。
2. ログイン画面で、**ドメイン資格情報でサインインする** リンクをクリックします。
3. ドメインユーザー資格情報を入力し、**サインイン** をクリックします。

子ドメインの資格情報を使用して Wyse Management Suite ポータルにログインするには、次の手順を実行します。

1. Wyse Management Suite 管理ポータルを開始します。
2. ログイン画面で、**ドメイン資格情報でサインインする** リンクをクリックします。
3. [**ユーザー ドメインの変更**] をクリックします。
4. ユーザー資格情報と完全なドメイン名を入力します。
5. **サインイン** をクリックします。

インポートした Active Directory ユーザーは、グローバル管理者ログインを使用して、**ユーザー** ページでアクティブ化または非アクティブ化できます。お使いのアカウントが無効にされている場合、Wyse Management Suite 管理ポータルにログインすることはできません。

メモ: LDAPS プロトコルを使用してユーザーをインポートするには、次の手順を実行します。

1. **キーツールを使用して、AD ドメインサーバのルート証明書を Java キーストアに手動でインポートします。例：**
   <C:\Program Files\DELL\WMS\jdk1.8.0_152\jre\bin>keytool.exe> -importcert -alias "WIN-O358EA52H8H" -keystore "<C:\Program Files\DELL\WMS\jdk1.8.0_152\jre\lib\security\cacerts>" -storepass changeit -file "Root Certificate Path"
2. **Tomcat サービスを再起動します。**

パブリッククラウドでの Active Directory フェデレーション サービス機能の設定

パブリック クラウドで、Active Directory フェデレーション サービス (ADFS) を設定できます。

手順

1. **ポータル管理** ページの **コンソール設定** で **Active Directory (AD)** をクリックします。
2. Wyse Management Suite の詳細を ADFS に入力します。Wyse Management Suite の xml ファイルをアップロードする必要がある ADFS サーバーの場所の詳細を知るには、[**情報 (i)**] アイコンにマウス ポインターを重ねます。

   メモ: Wyse Management Suite の.xml ファイルをダウンロードするには、ダウンロード リンクをクリックします。
3. ADFS で Wyse Management Suite のルールを設定します。カスタム クレーム ルールの詳細を知るには、[**情報 (i)**] アイコンにマウス ポインターを重ねます。

   メモ: Wyse Management のルールを表示するには、WMS ルールの表示 リンクをクリックします。Wyse Management Suite のルールは、[Wyse Management Suite のルール] ウィンドウにあるリンクをクリックしてダウンロードすることもできます。
4. ADFS の詳細を設定するには、**設定の追加** をクリックし、次の手順を実行します。

   メモ: テナントが ADFS 設定に従うことを許可するには、ADFS のメタデータファイルをアップロードします。

   a) Thin Client に保存されている.XML ファイルをアップロードするには、[**XML ファイルのロード**] をクリックします。
   ファイルは、`https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml` で利用できます。
   b) エンティティ ID と X.509 署名証明書の詳細をそれぞれのボックスに入力します。
   c) ADFS ログイン URL アドレスと ADFS ログアウト URL アドレスをそれぞれのボックスに入力します。
   d) ADFS を使用してテナントがシングルサインオンを設定できるようにするには、**ADFS を使用して SSO ログインを有効にする** チェックボックスを選択します。この機能は、セキュリティアサーションマークアップランゲージ (SAML) 標準仕様に従います。
   e) 設定情報を検証するには、**ADFS ログインのテスト** をクリックします。これにより、保存する前にテナントはセットアップをテストできます。

   メモ: テナントは、ADFS を使用して SSO ログインをアクティブ化 / 非アクティブ化できます。
5. **保存** をクリックします。
6. メタデータファイルを保存した後、**設定のアップデート** をクリックします。

   メモ: テナントは、ADFS から設定した AD 資格情報を使用してログインおよびログアウトできます。AD ユーザーが Wyse Management Suite サーバにインポートされていることを確認する必要があります。ログインページで、サインイン をクリックし、ドメイン資格情報を入力します。AD ユーザーの電子メールアドレスを指定してサインインする必要があります。ユーザーをパブリック クラウドにインポートするには、リモート リポジトリーをインストールする必要があります。ADFS のマニュアルについての詳細は、Technet.microsoft.com を参照してください。

タスクの結果

ADFS テスト接続に成功したら、リモート リポジトリーにある AD コネクターを使用してユーザーをインポートします。

Active Directory によるパブリック クラウドへのユーザーのインポート

手順

1. ファイルリポジトリをダウンロードしてインストールするには、「ファイルリポジトリへのアクセス」を参照してください。リポジトリは、会社のネットワークを使用してインストールされている必要があり、ユーザーをプルするために AD サーバにアクセスできる必要があります。
2. リポジトリをパブリッククラウドに登録します。一度登録したら、UI に記載されている手順に従って、ユーザーを Wyse Management Suite パブリッククラウドにインポートします。Wyse Management Suite パブリッククラウドにインポートした後で、AD ユーザーのロールを編集できます。

3. パブリック クラウドで ADFS を設定するには、「パブリック クラウドでの Active Directory フェデレーション サービスの機能の設定」を参照してください。

アラート分類

アラート ページは、アラートを **重要**、**警告**、**情報** に分類します。

メモ: アラートを電子メールで受け取るには、右上に表示されるユーザー名メニューから、アラート プリファランス オプションを選択します。

以下のアラートについて、**重要**、**警告**、または **情報** などの希望する通知タイプを選択します。

- デバイス正常性アラート
- デバイスはチェックインしていません

アプリケーション プログラミング インターフェイス (API) アカウントの作成

このタスクについて

このセクションでは、アプリケーションプログラミングインタフェース (API) アカウントを作成できます。このサービスは、特別なアカウントを作成する機能を提供します。外部アプリケーションサービスを設定するには、次の操作を行います。

手順

1. Wyse Management Suite ポータルにログインして、[**ポータル管理**] タブをクリックします。
2. **コンソール設定** の下の **外部アプリサービス** を選択します。
3. **追加** タブを選択して API サービスを追加します。
   [**外部アプリ サービスの追加**] ダイアログ ボックスが表示されます。
4. 次の詳細を入力して外部アプリケーションサービスを追加します。
   - 名前
   - 説明
5. **自動承認** チェックボックスを選択します。
   チェックボックスを選択すると、グローバル管理者からの承認は必要ありません。
6. **保存** をクリックします。

Wyse Management Suite ファイル リポジトリーへのアクセス

ファイルリポジトリは、**ファイル**が保存されて整理されている場所です。Wyse Management Suite には次の 2 つのリポジトリタイプがあります。

- **ローカルリポジトリ** - Wyse Management Suite のプライベートクラウドのインストール中、Wyse Management Suite インストーラにローカルリポジトリのパスを指定します。インストール後、**ポータル管理** > **ファイルリポジトリ** の順に移動して、ローカルリポジトリを選択します。リポジトリの設定を表示および編集するには、**編集** オプションをクリックします。
- **Wyse Management Suite リポジトリー** - Wyse Management Suite のパブリック クラウドにログインし、**[ポータル管理]** > **[ファイル リポジトリー]** の順に移動して、Wyse Management Suite リポジトリーのインストーラーをダウンロードします。インストール後、必要な情報を指定して、Wyse Management Suite リポジトリを Wyse Management Suite 管理サーバに登録します。

[**自動レプリケーション**] オプションを有効にして、任意のファイル リポジトリーに追加されたファイルを他のリポジトリーにレプリケートできます。このオプションを有効にすると、警告メッセージが表示されます。[**既存ファイルのレプリケーション**] チェックボックスを選択して、既存のファイルをファイル リポジトリーにレプリケートできます。

リポジトリーがすでに登録されている場合に、[**既存ファイルのレプリケーション**] オプションが適用されます。新しいリポジトリーが登録されると、すべてのファイルが新しいリポジトリーにコピーされます。[**イベント**] ページでファイルのレプリケーション ステータスを表示できます。

メモ:

- **イメージ プル** テンプレートは、他のリポジトリーに自動的にレプリケートされません。これらのファイルは手動でコピーする必要があります。
- ファイルのレプリケーション機能は、**Wyse Management Suite 2.0** 以降のバージョンのリポジトリーでのみサポートされています。
- リモート リポジトリーの自己署名証明書を **Wyse Management Suite** サーバーにインポートすることはできません。リモート リポジトリーに対して **CA** 検証が有効になっている場合、リモート リポジトリーからローカル リポジトリーへのファイルのレプリケーションは失敗します。

Wyse Management Suite リポジトリを使用するには、次の手順を実行します。

1. パブリッククラウドのコンソールから Wyse Management Suite リポジトリをダウンロードします。
2. インストールプロセスの後、アプリケーションを起動します。
3. Wyse Management Suite リポジトリ ページで、資格情報を入力して、Wyse Management Suite リポジトリを Wyse Management Suite サーバに登録します。
4. **パブリック WMS 管理ポータルへの登録** オプションを有効にする場合は、リポジトリを Wyse Management Suite のパブリッククラウドに登録することができます。
5. **ファイルの同期** オプションをクリックして、ファイルの同期コマンドを送信します。
6. **チェックイン** をクリックしてから、**コマンドの送信** をクリックして、デバイスにデバイス情報コマンドを送信します。
7. **登録解除** オプションをクリックして、オンプレミスサービスを登録解除します。
8. **編集** をクリックしてファイルを編集します。
9. **ファイルの同時ダウンロード** オプションのドロップダウンリストから、ファイルの数を選択します。
10. **Wake on LAN** オプションを有効または無効にします。
11. **ファイルの高速アップロードおよびダウンロード（HTTP）** オプションを有効または無効にします。
    - HTTP が有効な場合、ファイルのアップロードおよびダウンロードは HTTP 経由で実行されます。
    - HTTP が有効ではない場合、ファイルのアップロードおよびダウンロードは HTTPS 経由で実行されます。
12. **証明書の検証** チェックボックスを選択して、パブリッククラウドの CA 検証を有効にします。

    メモ: Wyse Management Suite サーバからの CA 検証が有効になっている場合、クライアントに証明書が存在する必要があります。アプリおよびデータ、イメージのプル / プッシュなど、すべての操作が成功します。クライアントに証明書が存在しない場合、Wyse Management Suite サーバの イベント ページに、「認証局の検証に失敗しました」という汎用監査イベントメッセージが表示されます。アプリおよびデータ、イメージのプル / プッシュなど、すべての操作が失敗します。また、Wyse Management Suite サーバーからの CA 検証が無効になっている場合、サーバーおよびクライアントからの通信はセキュアなチャネルで、証明書署名の検証を行わずに実行されます。
13. 所定のボックスにメモを追加します。
14. **設定の保存** をクリックします。

サブネット マッピング

Wyse Management Suite 2.0 から、ファイル リポジトリーにサブネットを割り当てることができます。ファイル リポジトリーを最大 25 のサブネットまたは範囲に関連づけることができます。またリポジトリーに関連づけられたサブネットに対して優先順位を設定できます。

サブネット マッピングの設定

手順

1. **[ポータル管理]** > **[ファイル リポジトリー]** の順に移動します。

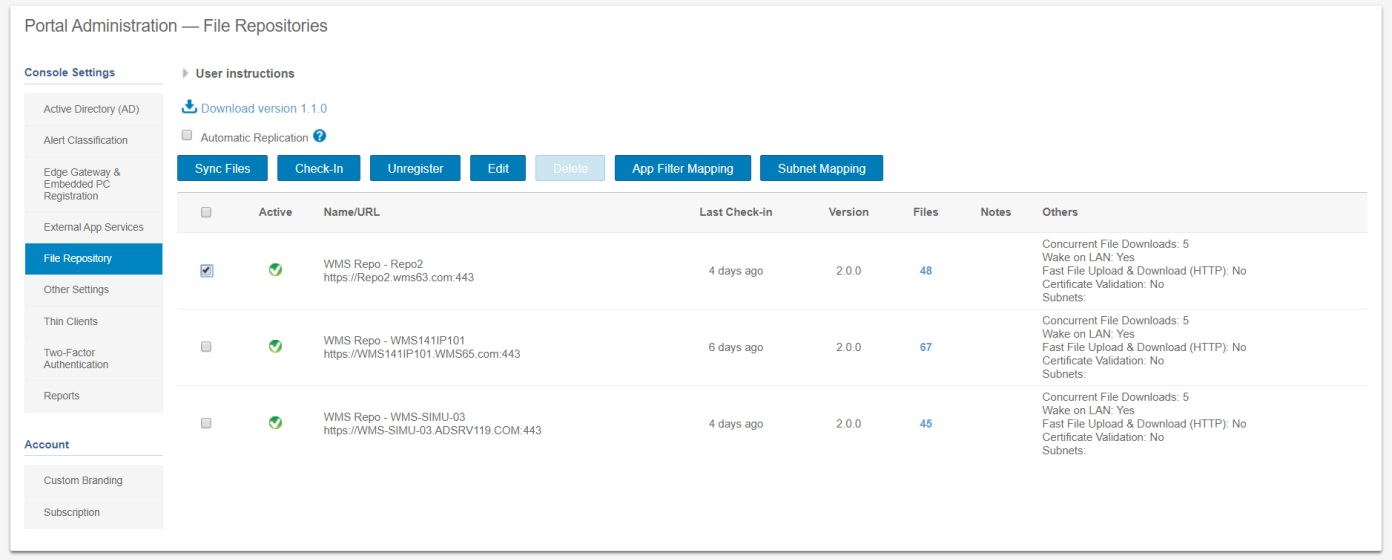


図 11. ファイルリポジトリ

2. ファイル リポジトリーを選択します。
3. [**サブネット マッピング**] オプションをクリックします。
4. サブネットまたは範囲の値を、1行につき1つ入力します。範囲を区切るにはハイフンを使用する必要があります。
5. オプションとして、設定したサブネットまたは範囲からのみファイル リポジトリーにアクセスする場合は、[**サブネットの近接性を使用したフォールバック方法として、このファイル リポジトリーにマップされていないサブネットのデバイスが、このリポジトリーからファイルをダウンロードできるようにする**] チェック ボックスをオフにします。

メモ: [サブネットの近接性を使用したフォールバック方法として、このファイル リポジトリーにマップされていないサブネットのデバイスが、このリポジトリーからファイルをダウンロードできるようにする] オプションは、デフォルトで選択されています。

その他の設定

以下の設定を使用して、**APNS 警告**、**ライセンスの有効期限切れ警告**、および他の **セルフサービス法的合意**を強制できます。

- **ダッシュボード ページでライセンス期限切れ警告を無視** - **ダッシュボード** ページでライセンス期限切れ警告の表示を無効にするには、このチェックボックスを選択します。
- **Android 設定ポリシー構成 ページで高度な Dell Wyse Cloud Connect オプションを有効化 (メモ：プロフェッショナルティアのみ)** - Android 設定ポリシー構成 ページで高度な Dell Wyse Cloud Connect オプションを有効にするには、このオプションを選択します。
- **ハートビート間隔** - 時間を入力します。デバイスは 60 ~ 360 分ごとにハートビート信号を送信します。
- **チェックイン間隔** - 時間を入力します。デバイスは 8 ~ 24 時間ごとに完全なチェック信号を送信します。
- **未チェックインコンプライアンスアラート** - デバイスが **未チェックインコンプライアンスアラート** をトリガーするまでの日数を入力します。範囲は 1 ~ 99 です。
- **WMS コンソール タイムアウト** – ユーザーがコンソールからログアウトするまでのアイドル時間を分単位で入力します。この設定は、任意のグローバル管理者が構成できます。デフォルト値は 30 分です。
- **登録の検証** - [**登録の検証**] オプションが有効になっている場合、自動検出されたデバイスは、[**デバイス**] ページで [**検証保留中**] 状態になります。テナントは、[**デバイス**] ページで1台または複数のデバイスを選択して、登録を検証することができます。デバイスは検証された後、目的のグループに移動されます。

Teradici 設定の管理

Teradici サーバを追加するには、次の手順を実行します。

手順

1. **ポータル管理** タブの **コンソール設定** で、**Teradici** をクリックします。
2. **サーバの追加** をクリックします。
   サーバの追加 画面が表示されます。

3. **サーバ名** を入力します。ポート番号が自動的に入力されます。
4. CA 検証を有効にするには、**CA 検証** チェックボックスを選択します。
5. **テスト** をクリックします。

二要素認証の有効化

システムに、少なくとも 2 人のアクティブなグローバル管理者のユーザーが存在する必要があります。

前提条件

タスクに進む前に、2 人以上のグローバル管理者を作成します。

このタスクについて

1. Wyse Management Suite ポータルにログインして、**ポータル管理** タブをクリックします。
2. **コンソール設定** の下にある **二要素認証** をクリックします。
3. 2 要素認証を有効にするには、チェックボックスを選択する必要があります。

   メモ: 管理者は、ワンタイムパスコードを使用して管理ポータルにログインし、2 番目の認証要素を検証する必要があります。
4. 自分の電子メールアドレスにワンタイムパスコードが送信されます。ワンタイム パスコードを入力します。

デフォルトでは、ワンタイムパスコードを検証するために 8 回まで試行できます。パスコードの検証に失敗した場合、アカウントはロックされます。グローバル管理者だけがロックされたアカウントをロック解除できます。

マルチテナントアカウントの有効化

このセクションでは、テナント アカウントを作成し、それぞれ独立して管理することができます。組織を個別に管理することができます。各アカウントには独自のライセンスキーがあり、独自の管理者アカウント、ポリシー、オペレーティングシステムのイメージ、アプリケーション、ルール、アラートなどを設定できます。高レベルオペレータが、これらの組織を作成します。

マルチテナントアカウントを有効にするには、次の操作を行います。

1. Wyse Management Suite ポータルにログインして、**ポータル管理** タブをクリックします。
2. **コンソール設定** の下の **マルチテナント** を選択します。
3. マルチテナントオプションを有効にするには、このチェックボックスを選択します。
4. 次の詳細を入力します。
   - ユーザー名
   - パスワード
   - パスワードの確認
   - 電子メール
5. **設定の保存** をクリックします。

レポートの生成

ジョブ、デバイス、グループ、イベント、アラート、ポリシーのレポートをダウンロードすることができます。エンドポイントのトラブルシューティングを行う場合、レポートを管理者と共有することができます。

手順

1. **ポータル管理** > **レポート** の順に移動します。
2. **レポートの生成** オプションをクリックします。
   レポートの生成 ウィンドウが表示されます。
3. **タイプ** ドロップダウンリストからレポートのタイプを選択します。
4. **グループ** ドロップダウンリストで、グループを選択します。
5. 区切り文字を選択します。
6. **保存** をクリックします。

カスタムブランド化の有効化

このタスクについて

このオプションでは、会社の名前とロゴまたはブランドを追加できます。独自のヘッダーロゴ、お気に入りアイコンをアップロードし、ヘッダーのタイトルを追加し、ヘッダーの色を変更して、Wyse Management Suite ポータルをカスタマイズすることができます。カスタムブランド化にアクセスし、指定するには、次の手順を実行します。

手順

1. **[ポータル管理者]** > **[アカウント]** > **[カスタム ブランド化]** の順に移動します。
2. [**カスタム ブランド化を有効にする**] をクリックします。
3. [**ヘッダー ロゴ**] で [**参照**] をクリックし、フォルダーの場所からヘッダー ロゴのイメージを選択します。
   ヘッダーロゴの最大サイズは、500*50 ピクセルにする必要があります。
4. **タイトル** オプションの下にタイトルを入力します。
5. ブラウザでタイトルを表示するには、**ブラウザウィンドウ / タブにタイトルを表示** チェックボックスを選択します。
6. **ヘッダーの背景色** および **ヘッダーテキストの色** にカラーコードを入力します。
7. **参照する** をクリックし、**お気に入りアイコン** を選択します。
   お気に入りアイコンが、ウェブサイト URL の横にあるブラウザのアドレスバーに表示されます。
   メモ: イメージは、.ico ファイルでのみ保存する必要があります。
8. **設定の保存** をクリックします。

システム セットアップの管理

インストール時に設定された SMTP の詳細、証明書、MQTT の詳細、外部 Wyse Management Suite の URL 詳細を変更することができます。Wyse Management Suite 2.0 からは、サーバー側で変更を加えることなく最新の設定を更新できる**動的スキーマ設定**が、ThinOS 9.x デバイスでサポートされています。パブリック クラウドでは、Wyse Management Suite のオペレーターが、9.x 設定のユーザー インタフェースをアップグレードできます。プライベート クラウドの場合 (pro 機能のみ)、グローバル ユーザーが、9.x 設定のユーザー インタフェースをアップグレードできます。**マルチテナント**機能が有効化されている場合、Wyse Management Suite のオペレーターは、最新のスキーマを [**管理**] セクションからアップロードできます。

手順

1. Wyse Management Suite ポータルにログインして、**ポータル管理** タブをクリックします。
2. **システム** の下で **セットアップ** をクリックします。
3. チェックボックスを選択すると、デバイスとサーバ間のすべての通信についてサーバ証明書の検証を実行します。
4. **電子メールアラート用に SMTP をアップデート** エリアに、次の詳細情報を入力します。
   - SMTP サーバー
   - 送信元アドレス
   - ユーザー名
   - パスワード
   - テストアドレス

   現在の証明書 : [**証明書の検証**] チェック ボックスを選択して、プライベート クラウドの CA 検証を有効にします。サーバーとクライアントからのすべての通信 (Local Repo からのファイルのダウンロード、オペレーティング システム イメージのダウンロードを含む) は、その証明書を使用します。
   メモ: Wyse Management Suite サーバからの CA 検証が有効になっている場合、クライアントに証明書が存在する必要があります。アプリおよびデータ、イメージのプル / プッシュなど、すべての操作が成功します。クライアントに証明書が存在しない場合、Wyse Management Suite サーバの イベント ページに、「認証局の検証に失敗しました」という汎用監査イベントメッセージが表示されます。アプリおよびデータ、イメージのプル / プッシュなど、すべての操作が失敗します。また、Wyse Management Suite サーバーからの CA 検証が無効になっている場合、サーバーおよびクライアントからの通信はセキュアなチャネルで、証明書署名の検証を行わずに実行されます。
5. 次のオプションを選択し、詳細を入力します。
   - **キー/証明書** - HTTPS キー/証明書ファイル ペアをアップロードします (PEM フォーマットのみがサポートされます)。
   - **PKCS-12** - HTTPS PKCS-12 をアップロードします (.pfx、.p12)。Apache の中間証明書は IIS pfx に必要です。
6. 外部 MQTT の詳細をアップデートするには、[**外部 MQTT の変更**] オプションをクリックして詳細を設定します。

7. 外部の Wyse Management Suite URL をアップデートするには、[**外部 WMS URL の変更**] オプションをクリックして詳細を設定します。

   メモ: 以前の設定に戻すには、[前回の URL に戻す] オプションをクリックし、[保存] をクリックします。

8. 9.x 設定のユーザー インタフェースをアップグレードする場合は、[**設定 UI パッケージ**] フィールドの [**ファイルの選択**] をクリックして、.zip ファイルを参照します。

   メモ: マルチテナント機能が有効になっている場合、このオプションは使用できません。

9. **保存** をクリックします。

14

Teradici デバイス管理

Teradici デバイス管理 セクションでは、Teradici デバイスの管理と検出について説明します。Teradici 管理コンソール は SDK を使用して、tera デバイスの管理と構成をサポートします。 これは、Wyse Management Suite のプライベートクラウドに Pro ライセンスタイプが適用される場合にのみ適用されます。

トピック：

Teradici デバイスの検出

前提条件

- 最新バージョンの Wyse Management Suite を Microsoft Windows 2012 Server またはそれ以降のバージョンにインストールしてあること。Threadx 5.x および 6.x デバイスは、最新バージョンのオペレーティングシステムで動作します。
- **EMSDK** コンポーネントをインストールして有効にしてあること。
- Wyse Management Suite サーバの FQDN が、**DHCP** または **DNS** の設定で使用できる必要がある。
- `Cert.pem` がデフォルトのパス `C:\Program Files\Dell\WMS\Teradici\EMSDK` に配置されている必要がある。これは Threadx デバイスの検出に使用されます。

セキュリティ レベル

エンドポイントの設定済みセキュリティ レベルによっては、EBM/EM 証明書を使用してエンドポイントをプロビジョニングする必要がある場合もあります。

中レベルまたは高レベルのセキュリティ向けに設定されたエンドポイントでは、EBM または EM に接続する前に、証明書ストアに信頼された証明書が含まれている必要があります。一部のエンドポイントでは、証明書が出荷時のデフォルトとしてベンダーによって事前にロードされている場合があります。それ以外の場合は、エンドポイントの AWI を使用して証明書を手動でアップロードできます。

次のいずれかに該当する場合、低セキュリティ用に設定されたエンドポイントでは、信頼される証明書ストアに MC 証明書は必要ありません。

- DHCP 検出または DNS 検出を使用しており、DHCP または DNS サーバーは EBM 証明書のフィンガープリントでプロビジョニングしている。
- 手動検出方法によってエンドポイントを検出している。

表 5. エンドポイントの証明書要件

検出方法	低セキュリティ	中セキュリティ	高セキュリティ
EBM フィンガープリントがプロビジョニングされていない DHCP/DNS 検出	証明書が必要です	証明書が必要です	適用なし
EBM フィンガープリントをプロビジョニングした DHCP/DNS 検出	証明書は必要ありません	証明書が必要です	適用なし
高度なセキュリティ環境向けに設定されたエンドポイントによって開始される検出	適用なし	適用なし	証明書が必要です
MC によって開始される手動検出	証明書は必要ありません	適用なし	適用なし

クライアントによる手動検出

1. `https://<clientIP>` に移動します。
2. 証明書についての警告メッセージを受け入れます。
3. 管理者パスワード (デフォルトのパスワードは「Administrator」) を入力し、ログインします。
4. **アップロード** > **証明書** に移動します。デフォルトのパスから `Cert.pem` ファイルを選択し、**アップロード** をクリックします。
5. **構成** > **管理** に移動します。**管理状態をクリア** ボタンをクリックして、デバイスを新しい管理サーバに登録します。
6. **マネージャ検出モード** を手動に設定します。
7. **Endpoint Bootstrap Manager の URL** を次の形式で入力します。**wss://<IP Address of the WMS server>**

   メモ: EMSDK がカスタムポートでインストールされている場合は、Endpoint Bootstrap Manager の URL は次の形式で指定します。wss://<IP Address:Custom port>
8. **適用**、**続行** の順にクリックします。
9. **管理ステータス** が、エンドポイントサーバに接続されていると表示されます。

DHCP サーバへの PCoIP エンドポイントベンダークラスの追加

1. DHCP サーバにログインします。
2. **サーバ** ペインの DHCP サーバを右クリックして、**DHCP マネージャ** を選択します。
3. **IPv4** オプションを右クリックして、**ベンダークラスの定義** を選択します。
4. **追加** をクリックして新しい DHCP ベンダークラスを追加します。
5. **表示名** フィールドに **PCoIP エンドポイント** を入力します。
6. ベンダー ID として **ASCII** 列に **PCoIP エンドポイント** を入力します。
7. **OK** をクリックして設定を保存します。

DHCP オプションの設定

1. **IPv4** オプションを右クリックして、**定義済みオプションの設定** を選択します。
2. **オプション** クラスとして **PCoIP エンドポイント** を選択し、**追加** をクリックします。
3. **オプションのタイプ** ダイアログで、名前に **EBM URI**、データタイプに **文字列**、コードに **10**、説明に **Endpoint Bootstrap Manager の URI** を入力し、**OK** をクリックします。
4. **OK** をクリックして設定を保存します。
5. オプションを適用する DHCP スコープを展開します。
6. **スコープオプション** を右クリックして、**オプションの設定** を選択します。
7. **詳細**タブをクリックし、**PCoIP エンドポイント**ベンダークラスを選択します。
8. **010 EBM URI** チェックボックスをオンにして、有効な管理コンソールの URI を **文字列** フィールドに入力します。**適用** をクリックします。この URL には、セキュアな WebSocket プレフィックス (たとえば、`wss://<MC IP address>:[port number]`) が必要です。MC のリスニングポートは、5172 です。このポート番号の入力は、オプションのステップです。
9. **OK** をクリックして設定を保存します。
10. **PCoIP エンドポイント**を**オプション**クラスとして選択し、**追加**をクリックします。
11. **オプションのタイプ** ダイアログで、名前に **EBM X.509 SHA-256 フィンガープリント**、データタイプに **文字列**、コードに **11**、説明に **EBM X.509 SHA-256 フィンガープリント** を入力し、**OK** をクリックします。
12. オプションを適用する DHCP スコープを展開します。
13. **スコープオプション** を右クリックして、**オプションの設定** を選択します。
14. **詳細**タブをクリックし、**PCoIP エンドポイント**ベンダークラスを選択します。
15. **011 EBM X.509 SHA-256 フィンガープリント** チェックボックスを選択し、SHA-256 フィンガープリントを貼り付けます。
16. **OK** をクリックして設定を保存します。
17. クライアントの Web ブラウザに移動します。
18. **構成** > **管理**に移動し、**マネージャ検出モード** を **自動** に設定します。
19. クライアントは、DHCP サーバに記載されているサーバに接続されます。

DNS SRV レコードの作成

1. **DNS サーバ**にログインします。

2. **サーバ** ペインの DNS サーバを右クリックして、コンテキストメニューから **DNS マネージャ** を選択します。
3. **前方参照ゾーン** でドメインを右クリックし、コンテキストメニューから **その他の新しいレコード** を選択します。
4. **リソースレコードの種類** ダイアログボックスでリストから **サービスロケーション (SRV)** を選択し、**レコードの作成** をクリックします。
5. **サービス** を **_pcoip-bootstrap** に、プロトコルを **_tcp** に、**ポート番号** を **5172** (MC のデフォルトのリスニングポート) に設定します。**このサービスを提供するホスト** には、MC の FQDN を入力します。

   メモ: DNS の仕様では SRV レコードで IP アドレスを使用できないため、MC の FQDN を入力する必要があります。
6. **OK** をクリックします。

DNS TXT レコードの追加

1. **前方参照ゾーン** でドメインを右クリックし、コンテキストメニューから **その他の新しいレコード** を選択します。
2. **リソースレコードの種類** ダイアログボックスでリストから **テキスト (TXT)** を選択し、**レコードの作成** をクリックします。
3. 次の詳細を入力します。
   a. **レコード名** フィールドに、サービスを提供する Wyse Management Suite サーバのホスト名を入力します。FQDN フィールドは自動的に入力されます。これは、Wyse Management Suite サーバの FQDN と一致するはずです。
   b. **テキスト** フィールドに **pcoip-bootstrap-cert=** と入力し、Wyse Management Suite サーバ証明書 SHA-256 指紋認証を貼り付けます。
4. **OK** をクリックします。
5. クライアントの Web ブラウザに移動します。
6. クライアントは、DNS サーバに記載されている Wyse Management Suite サーバに接続されます。

SHA-256 指紋認証の作成

1. Mozilla Firefox を起動します。
2. **オプション、詳細** タブに移動します
3. **証明書** をクリックして証明書を表示します。
4. **証明書マネージャ** の下の **認証局証明書** をクリックして、**インポート** をクリックします。
5. 証明書を表示し、**表示** をクリックします。
6. **SHA-256** フィンガープリントをコピーします。

CIFS のユースケースのシナリオ

Wyse Management Suite では、次のユースケースがサポートされます。

- Wyse Management Suite のプライベートクラウドのインストール中に、**Wyse Management Suite** を **セットアップタイプ** として選択した場合。
  - CIFS の設定 ページが表示されます。このページが必要になるのは、共有フォルダを設定する必要があるためです。

    メモ: CIFS ユーザー資格情報の設定 オプションは、デフォルトでは無効になっています。
- Wyse Management Suite のプライベートクラウドのインストール中に、**Teradici EMSDK** を **セットアップタイプ** として選択した場合。
  - CIFS 資格情報のためには、既存のアカウントを使用するか、新しいアカウントを作成することができます。
- Wyse Management Suite のプライベートクラウドのインストール中に、**Wyse Management Suite** と **Teradici EMSDK** の両方を **セットアップタイプ** として選択した場合。
  - CIFS の設定 ページが表示されます。このページが必要になるのは、共有フォルダを設定する必要があるためです。

    メモ: CIFS ユーザー資格情報の設定 オプションは、デフォルトでは無効になっています。
  - CIFS 資格情報のためには、既存のアカウントを使用するか、新しいアカウントを作成することができます。
- EMSDK サービスがすでにインストールされているシステムに EMSDK のみをインストールする場合。
  - Teradici EMSDK が選択されている場合、**セットアップタイプ** のページで **次へ** をクリックすると、警告メッセージが表示されます。メッセージは次のとおりです。**Teradici EMSDK がすでにインストールされていることをインストーラが検出しました。EMSDK は、必要に応じて更新されます。** ポート番号は必要ありません。
    - **CIFS ユーザー資格情報の設定** オプションが選択されている場合 (デフォルト)。
      1. サービスを停止します。

2. EMSDK サービスをアップデートします。
3. サービスを再起動します。これは、同じ事前設定されたユーザーの下で動作します。

- **CIFS ユーザー資格情報の設定** オプションが、**既存のユーザーを使用** オプションとともに選択されている場合。

1. サービスを停止します。
2. EMSDK サービスをアップデートします。
3. ユーザーのサービスログを、選択したユーザーにアップデートします。
4. サービスを再起動します。これは、同じ事前設定されたユーザーの下で動作します。

- **CIFS ユーザー資格情報の設定** オプションが、**新規ユーザーの作成** オプションとともに選択されている場合。

1. サービスを停止します。
2. EMSDK サービスをアップデートします。
3. ユーザーのサービスログを、新規作成されたユーザーにアップデートします。
4. サービスを再起動します。これは、同じ事前設定されたユーザーの下で動作します。

- すでに EMSDK サービスがインストールされているシステムに **Wyse Management Suite** と **Teradici EMSDK** の両方をインストールする場合。
  - 「**EMSDK サービスがすでにインストールされているシステムに EMSDK のみをインストールする場合**」と同じですが、**CIFS ユーザー資格情報の設定** オプションがデフォルトで選択され、グレー表示されます。CIFS 資格情報を入力する必要があります。

15

ライセンスサブスクリプションの管理

このセクションでは、管理コンソールのライセンス サブスクリプションとその使用状況を表示し管理できます。

ポータル管理 ページで、**サブスクリプション** オプションを表示できます。このページは次の情報を提供します。

- ライセンス サブスクリプション
- ライセンスの注文
- ライセンスの使用状況 - 登録済みの Thin Client デバイス
- サーバー情報
- ライセンスのインポート - プライベート クラウド
- プライベート クラウドのライセンスのエクスポート - パブリック クラウド

トピック：

Wyse Management Suite パブリック クラウドからのライセンスのインポート

Wyse Management Suite パブリック クラウドから Wyse Management Suite プライベート クラウドにライセンスをインポートできます。

手順

1. Wyse Management Suite プライベートクラウドコンソールにログインします。
2. **[ポータル管理]** > **[アカウント]** > **[サブスクリプション]** の順に移動します。
3. Wyse Management Suite パブリック クラウドの詳細を入力します。
   - ユーザー名
   - パスワード
   - データセンター
   - TC シート数
   - Edge Gateway および Embedded PC シートの数
   - Wyse Software Thin Client シートの数
4. **インポート** をクリックします。

   メモ: Wyse Management Suite プライベート クラウドは、Wyse Management Suite パブリック クラウドに接続されている必要があります。

Wyse Management Suite プライベート クラウドへのライセンスのエクスポート

Wyse Management Suite パブリック クラウドから Wyse Management Suite プライベート クラウドにライセンスをエクスポートできます。

手順

1. Wyse Management Suite のパブリッククラウドコンソールにログインします。
2. **[ポータル管理]** > **[アカウント]** > **[サブスクリプション]** の順に移動します。

3. Wyse Management Suite のプライベートクラウドにエクスポートする必要があるシンクライアントのシート数を入力します。
4. **エクスポート** をクリックします。
5. 生成されたライセンスキーをコピーします。
6. Wyse Management Suite プライベートクラウドコンソールにログインします。
7. **[ポータル管理]** > **[アカウント]** > **[サブスクリプション]** の順に移動します。
8. 生成されたライセンスキーをボックスに入力します。
9. **インポート** をクリックします。

Thin Client のライセンス割り当て

Wyse Management Suite プライベート クラウドと Wyse Management Suite パブリック クラウド アカウント間で Thin Client ライセンスを割り当てることができます。

手順

1. Wyse Management Suite パブリッククラウドコンソールにログインします。
2. **[ポータル管理]** > **[アカウント]** > **[サブスクリプション]** の順に移動します。
3. Thin Client のシート数を入力します。

   メモ: Thin Client シートは、パブリッククラウドで管理可能である必要があります。入力する Thin Client シート数は、管理可能 オプションに表示される数を超えてはいけません。
4. **エクスポート** をクリックします。

   メモ: パブリッククラウドのライセンス数は、プライベートクラウドにエクスポートされた Thin Client シート数に基づいて調整されます。
5. 生成されたライセンスキーをコピーします。
6. Wyse Management Suite プライベートクラウドコンソールにログインします。
7. **[ポータル管理]** > **[アカウント]** > **[サブスクリプション]** の順に移動します。
8. エクスポートされたライセンスキーをプライベートクラウドにインポートします。

   メモ: プライベートクラウドで現在管理されているデバイスの管理に十分な数の Thin Client シートがない場合は、ライセンスをインポートできません。その場合は、手順 3 ~ 8 を繰り返して、Thin Client シートを割り当てます。

ライセンスの注文

パブリック クラウドの [**ライセンスの注文**] セクションには、期限切れのライセンスを含む確定済みの注文のリストが表示されます。デフォルトでは、期限切れの注文は表示されません。期限切れの注文を表示するには、**期限切れの注文を含める** チェックボックスを選択します。すでに期限切れの注文は赤色で表示され、期限が 30 日以内に近づいている注文はオレンジ色で表示されます。

メモ: オンプレミス導入環境では注文履歴が表示されないため、この機能は利用できません。ただし、パブリック クラウド ポータルにテナント管理者としてログインしている場合は、オンプレミスのライセンス注文履歴を利用できます。

16

ファームウェアアップグレード

Wyse Management Suite を使用して、ファームウェアをアップグレードできます。

トピック：

- ThinLinux 1.x から 2.1 以降のバージョンへのアップグレード
- ThinOS 8.x から 9.0 へのアップグレード

ThinLinux 1.x から 2.1 以降のバージョンへのアップグレード

アップグレード前に TL 2.x からカスタム イメージを取得する場合は、ThinLinux 2.x を準備してから ThinLinux 1.x イメージをアップグレードする必要があります。

ThinLinux 2.x イメージの準備

前提条件

ThinLinux ビルド バージョン 2.0.19 または 2.1 から 2.2 へアップグレードするには、Wyse Management Suite バージョン 1.4 以降を使用します。

手順

1. www.dell.com/support にアクセスします。
2. [**製品サポート**] をクリックし、お使いのシン クライアントの**サービス タグ**を入力して、**Enter** をクリックします。

   メモ: サービス タグがない場合は、お使いのシン クライアントのモデルを手動で参照します。
3. [**ドライバーおよびダウンロード**] をクリックします。
4. [**オペレーティング システム**] ドロップダウン リストから、[**ThinLinux**] を選択します。
5. `merlin_nonpxe-4.0.1-0 0.04.amd64.deb` および `wda_3.4.6-05_amd64.tar` アドオンをダウンロードします。
6. ダウンロードしたアドオンを`<drive C>/wms/localrepo/repository/thinClientsApps/`にコピーします。
7. ThinLinux 2.x を実行しているシン クライアントで、**[設定]** > **[管理]** > **[Wyse Device Agent]** に移動します。
8. デバイスを Wyse Management Suite サーバーに登録します。
9. [**設定**] ウィンドウを閉じます。

   メモ: [設定] ウィンドウが閉じていない場合は、イメージを導入した後に「プロファイルがロックされている」というエラーが表示されます。
10. Wyse Management Suite コンソールにログインします。
11. `merlin_nonpxe-4.0.1-0 0.04.amd64.deb` および `wda_3.4.6-05_amd64.tar` アドオンのアプリケーション ポリシーを作成して導入します。
12. シン クライアントを再起動します。
13. Wyse Management Suite サーバーにログインします。
14. [デバイス] ページに移動して、Merlin および WDA のバージョンがアップデートされていることを確認します。
15. 登録済みデバイスをクリックし、**[追加アクション]** > **[OS イメージの吸出し]** の順に移動します。
    [**OS イメージの吸出し**] ウィンドウが表示されます。
16. イメージの名前を入力します。
17. [ファイル リポジトリー] ドロップダウン リストから、ファイル リポジトリーを選択します。
18. 実行する引き出し操作のタイプを選択します。
    - **デフォルト** - [**OS+リカバリー**] チェック ボックスを選択して、イメージを引き出します (圧縮/圧縮解除)。

- **詳細** - テンプレート Compress_OS_Recovery_Commandsxml/uncompress_OS_Recovery_CommandsXml を選択して画像を引き出します。

タスクの結果

メモ:

- **Wyse Management Suite 1.3 リモート リポジトリーを使用している場合、XML ファイルはリポジトリーで使用できません。ファイルにアクセスするには、Wyse Management Suite を 1.4 以降にアップグレードする必要があります。**
- **リカバリーの引き出し操作では、ユーザー設定は保持されません。**

ThinLinux 1.x から 2.x へのアップグレード

手順

1. www.dell.com/support にアクセスします。
2. [**製品サポート**] をクリックし、お使いのシン クライアントの**サービス タグ**を入力して、**Enter** をクリックします。

   メモ: サービス タグがない場合は、お使いのシン クライアントのモデルを手動で参照します。
3. [**ドライバーおよびダウンロード**] をクリックします。
4. [**オペレーティング システム**] ドロップダウン リストから、[**ThinLinux**] を選択します。
5. ページを下にスクロールして、次の手順を実行します。
   - Platform_util-1.0.26-0.3.x86_64.rpm、wda-2.1.23-00.01.x86_64.rpm、および merlin-nonpxe_3.7.7-00.05_amd64.deb アドオンをダウンロードします。
   - 最新の ThinLinux バージョン 2.x のイメージ ファイル (2.1.0.01_3040_16GB_merlin.exe または 2.2.0.00_3040_merlin_16GB.exe) をダウンロードします。
6. Thin Client で、**[設定]** > **[管理]** > **[Wyse Device Agent]** の順に移動します。
7. デバイスを Wyse Management Suite サーバーに登録します。
8. Wyse Management Suite コンソールにログインします。
9. Platform_util-1.0.26-0.3.x86_64.rpm、wda-2.1.23-00.01.x86_64.rpm、および merlin-nonpxe_3.7.7-00.05_amd64.deb アドオンのアプリケーション ポリシーを作成して導入します。
10. シン クライアントを再起動します。
11. Wyse Management Suite サーバーにログインします。
12. ダウンロードしたイメージ (2.2.0.00 _3040_Merlin _16GB.exe ファイル) を<drive C>/wms/localrepo/repository/osimage /zipped/にコピーします。

    メモ: 圧縮フォルダー内のイメージが有効なフォルダーに抽出されます。抽出プロセスには 10 ~ 15 分かかる場合があります。
13. Wyse Management Suite コンソールにログインします。
14. **[アプリとデータ]** > **[OS イメージ リポジトリー]** > **[WES/ThinLinux]** の順に進み、ThinLinux のイメージが利用可能であることを確認します。
15. **[アプリとデータ]** > **[OS イメージ ポリシー (WES/ThinLinux)]** に移動して、[**ポリシーの追加**] をクリックします。
16. [ポリシーの追加] ウィンドウで、以下のオプションを設定します。
    - **OS タイプ** - ThinLinux
    - **OS サブ フィルター** - ThinLinux (ThinLinux)
    - **ルール** - アップグレードのみ/このバージョンを強制

    メモ: ポリシーの作成中にリポジトリーにコピーされた、引き出したイメージ/フレッシュ イメージを選択します。
17. 必要に応じて他の必須フィールドを更新し、[**保存**] をクリックします。
18. ジョブをスケジュールします。
19. クライアントで [**今すぐアップデート**] をクリックして、イメージをアップデートします。

ThinOS 8.x から 9.0 へのアップグレード

ThinOS ファームウェアを 9.0 にアップグレードするには、Wyse Management Suite バージョン 2.0 を使用する必要があります。

次の表に、ThinOS ファームウェア イメージを示します。

表 6. ファームウェア イメージ

プラットフォーム	ThinOS ファームウェア イメージ
Wyse 3040 Thin Client	A10Q_wnos
Wyse 5070 Thin Client - Celeron プロセッサー	X10_wnos
Wyse 5070 Thin Client - Pentium プロセッサー	X10_wnos
Wyse 5070 Extended Thin Client - Pentium プロセッサー	X10_wnos
Wyse 5470 Thin Client	X10_wnos
Wyse 5470 All-in-One Thin Client	X10_wnos

リポジトリーへの ThinOS ファームウェアの追加

手順

1. テナントの資格情報を使用して Wyse Management Suite にログインします。
2. **アプリ & データ** タブで、**OS イメージリポジトリ** の **ThinOS** をクリックします。
3. [**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 画面が表示されます。
4. ファイルを選択するには、[**参照**] をクリックしてファイルがある場所に移動します。
5. お使いのファイルの説明を入力します。
6. 既存のファイルを上書きする場合は、チェックボックスを選択します。
7. **アップロード** をクリックします。

メモ:

- **アップロードされたファームウェアは、ThinOS 8.6 から ThinOS 9.0 にアップグレードする場合にのみ使用できます。**
- **チェックボックスを選択すると、ファイルはリポジトリに追加されますが、グループまたはデバイスのいずれにも割り当てられません。デバイスまたはデバイスのグループにファームウェアを導入するには、それぞれのデバイスまたはグループの設定ページに移動します。**

ThinOS 8.6 から ThinOS 9.x へのアップグレード

前提条件

- ThinOS ファームウェア リポジトリーに、ThinOS 変換イメージを追加する必要があります。詳細については、「リポジトリーへの ThinOS ファームウェアの追加」を参照してください。
- グループ トークンで Wyse Management Suite 内にグループを作成します。このグループ トークンを使用して、ThinOS 8.6 デバイスを登録します。
- シン クライアントは Wyse Management Suite に登録する必要があります。

手順

1. [**グループ&設定**] ページに移動して、グループを選択します。
2. [**ポリシーの編集**] ドロップダウン メニューから [**ThinOS**] をクリックします。
   ThinOS 設定モードの選択 ウィンドウが表示されます。
3. [**詳細設定モード**] を選択します。
4. [**ファームウェアのアップグレード**] に移動して、[**この項目を設定する**] をクリックします。
5. [**ライブ アップグレードを無効にする**] および [**署名の検証**] オプションをオフにします。
6. [**プラットフォーム タイプ**] ドロップダウン リストから、プラットフォームを選択します。
7. [**自動導入のためのファームウェア**] ドロップダウン リストから、リポジトリーに追加するファームウェアを選択します。
8. [**保存して公開**] をクリックします。

ファームウェアが、シン クライアントに導入されます。変換プロセスには 15～20 秒かかり、シン クライアントは自動的に再起動されます。

メモ: ファームウェアをアップグレードした後、デバイスは自動的に Wyse Management Suite に登録されます。ファームウェアのアップグレード後、8.6 ビルドの設定は継承されません。

ThinOS 9.x からそれ以降のバージョンへのアップグレード

前提条件

- シン クライアントは Wyse Management Suite に登録する必要があります。
- グループ トークンで Wyse Management Suite 内にグループを作成します。このグループ トークンを使用して、ThinOS 9.x デバイスを登録します。

手順

1. [**グループ＆設定**] ページに移動して、グループを選択します。
2. [**ポリシーの編集**] ドロップダウン メニューから、[**ThinOS 9.x**] をクリックします。
   [**設定コントロール** | ThinOS] ウィンドウが表示されます。
3. [**詳細設定**] をクリックします。
4. [**ファームウェア**] フィールドで、[**OS ファームウェア プロパティ**] を選択します。
5. [**参照**] をクリックし、ファームウェアを参照してアップロードします。

   メモ: 一括では 5 個のファームウェア パッケージのみをアップロードできます。
6. [**導入する ThinOS ファームウェアの選択**] ドロップダウン メニューから、アップロード済みのファームウェアを選択します。
7. [**保存して公開**] をクリックします。
   シン クライアントは、ファームウェアをダウンロードして再起動します。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。

17

リモートリポジトリ

Wyse Management Suite では、アプリケーション、オペレーティングシステムイメージなどのために、ローカルリポジトリとリモートリポジトリを使用できます。ユーザーアカウントが地理的に分散している場合、デバイスがローカルリポジトリからイメージをダウンロードできるように、分散したユーザーアカウントごとに別のローカルリポジトリを配置する構成が効率的です。この柔軟性は、`WMS_Repo.exe` ソフトウェアで実現されます。`WMS_Repo.exe` は、Wyse Management Suite のファイルリポジトリソフトウェアであり、Wyse Management Suite に登録できる分散リモートリポジトリを作成する場合に役立ちます。`WMS_Repo.exe` は、**Pro** ライセンスのサブスクライバのみが使用できます。

前提条件

Wyse Management Suite リポジトリソフトウェアをインストールする場合のサーバ要件は次のとおりです。

- Windows 2012 R2 または Windows 2016 Server
- 4 CPU
- 8 GB RAM
- 40 GB ストレージ容量

このタスクについて

WMS-Repo ソフトウェアをインストールするには、次の手順を実行します。

手順

1. Dell Digital Locker から `WMS_Repo.exe` ファイルをダウンロードします。
2. **管理者**としてログインし、`WMS_Repo.exe` をリポジトリサーバにインストールします。
3. **次へ** をクリックして、画面に表示される指示に従ってインストールを完了します。
4. **起動** をクリックして、ウェブブラウザで **WMS リポジトリ登録** 画面を表示します。

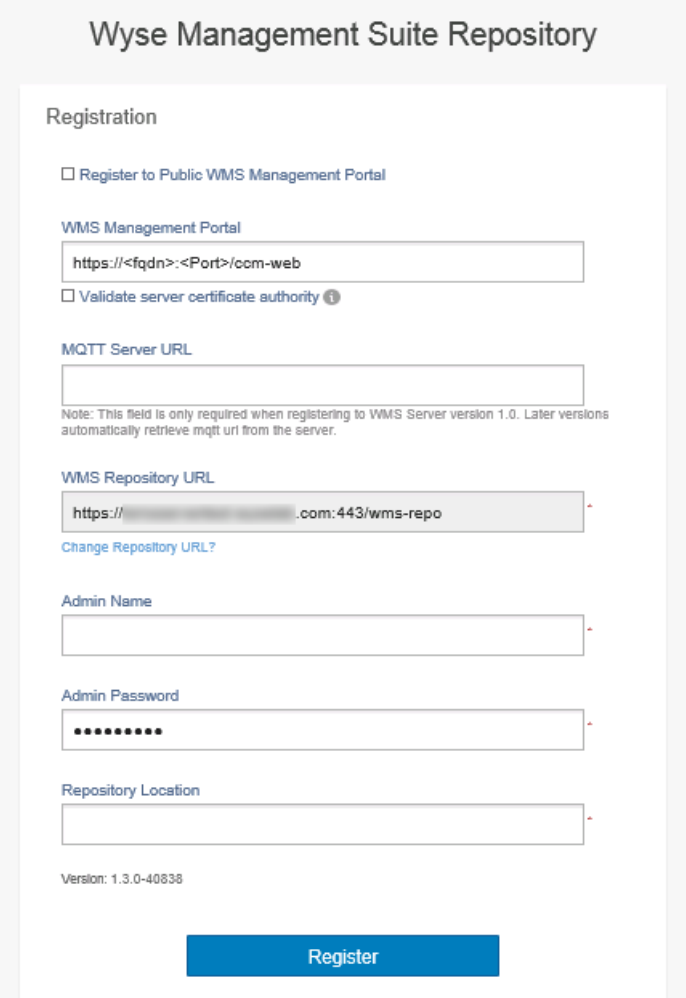


図 12. 登録の詳細

5. **登録** をクリックして登録を開始します。パブリッククラウドで登録を行っている場合は、**パブリック WMS 管理ポータルへの登録** を選択します。

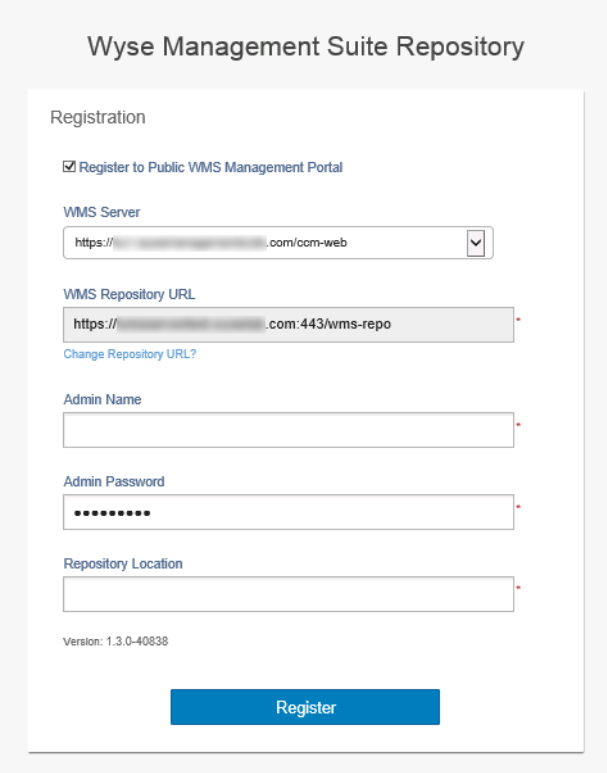


図 13. パブリッククラウドでの登録

6. 次の詳細情報を入力して、**登録** をクリックします。
   a) Wyse Management Suite サーバの URL

   メモ: Wyse Management Suite v1.0 に登録しないと、MQTT Server URL を使用することはできません。

   b)
   c) WMS リポジトリ URL (URL をドメイン名でアップデート)
   d) Wyse Management Suite 管理者のログインユーザー名情報
   e) Wyse Management Suite 管理者のログインパスワード情報
   f) リポジトリパス情報
7. 登録が成功すると、**登録** ウィンドウが表示されます。

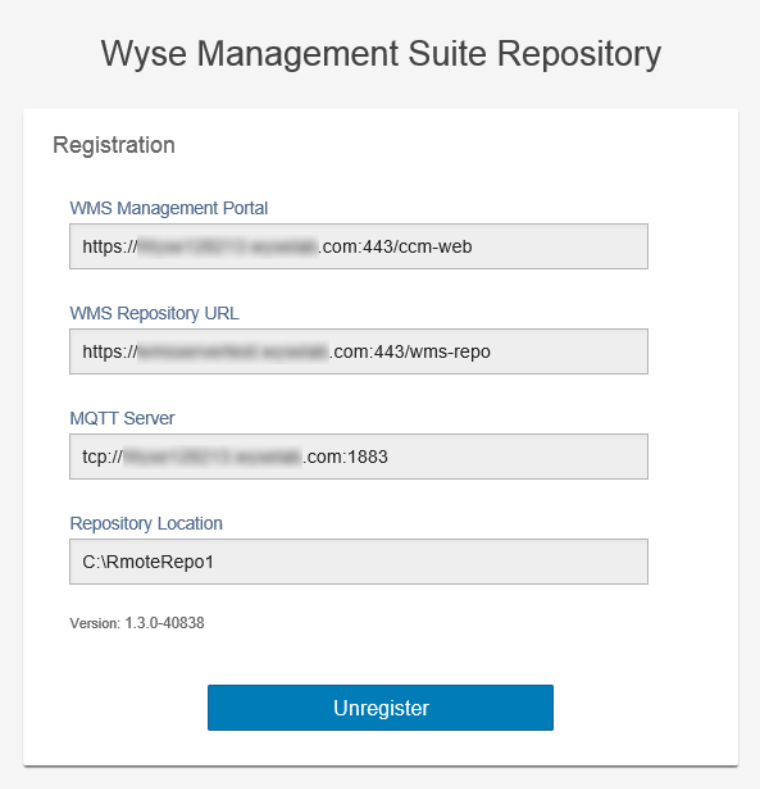


図 14. 登録に成功

8. Wyse Management Suite ポータルの次の画面で、リモートリポジトリの登録成功を確認します。

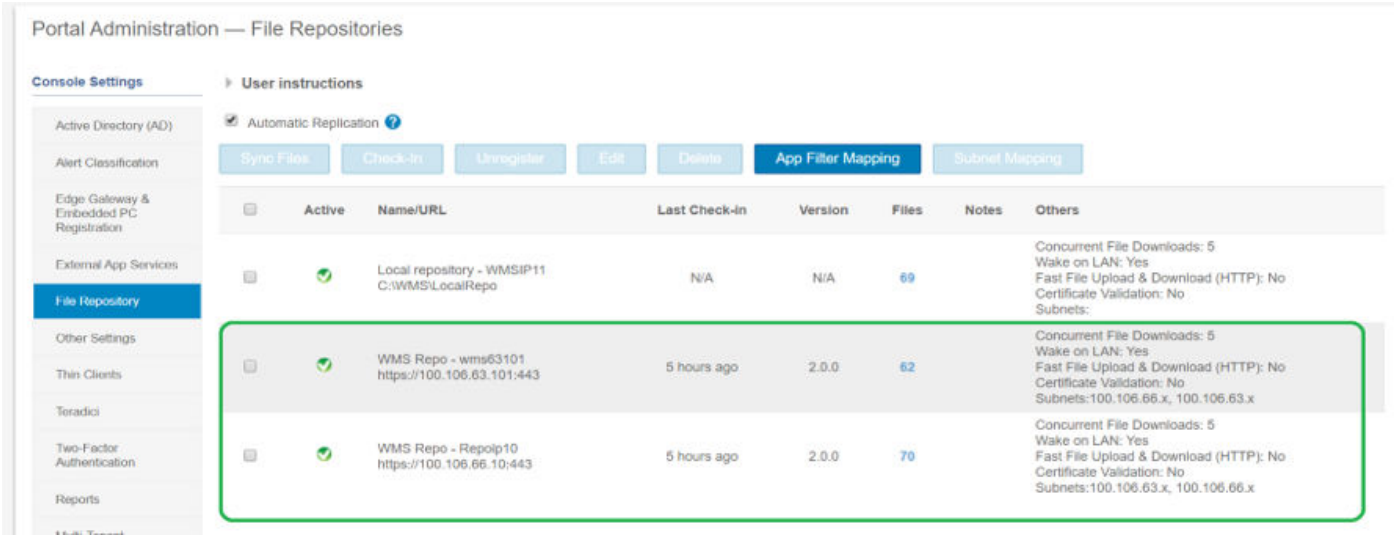


図 15. ポータルでの登録に成功

9. `WMS_Repo.exe` の場合、HTTPS はデフォルトで有効になっており、自己署名証明書とともにインストールされます。ドメイン固有の証明書を独自にインストールする場合は、登録ページを下にスクロールして、SSL 証明書をアップロードします。

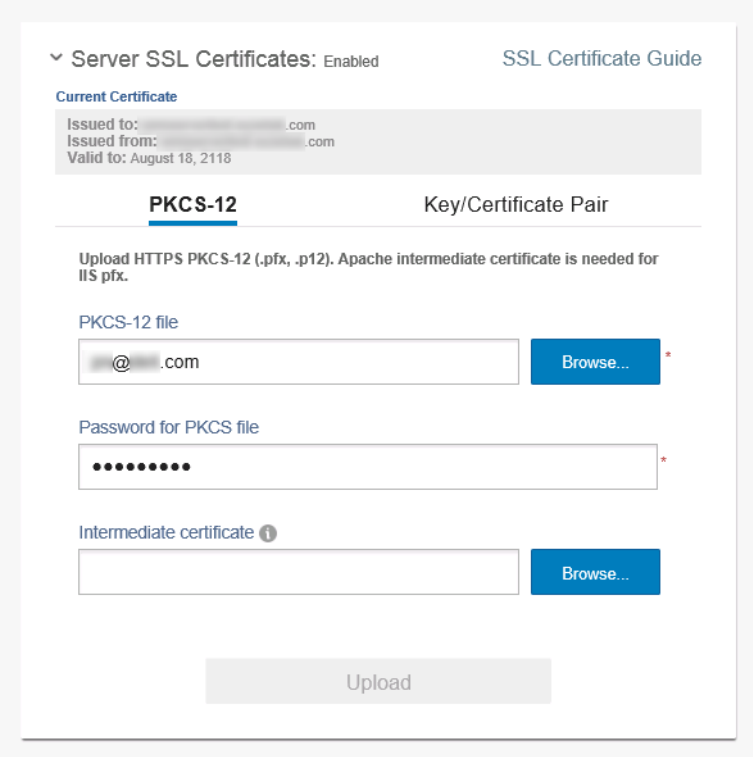


図 16. 証明書のアップロード

10. サーバが再起動し、アップロードされた証明書が表示されます。

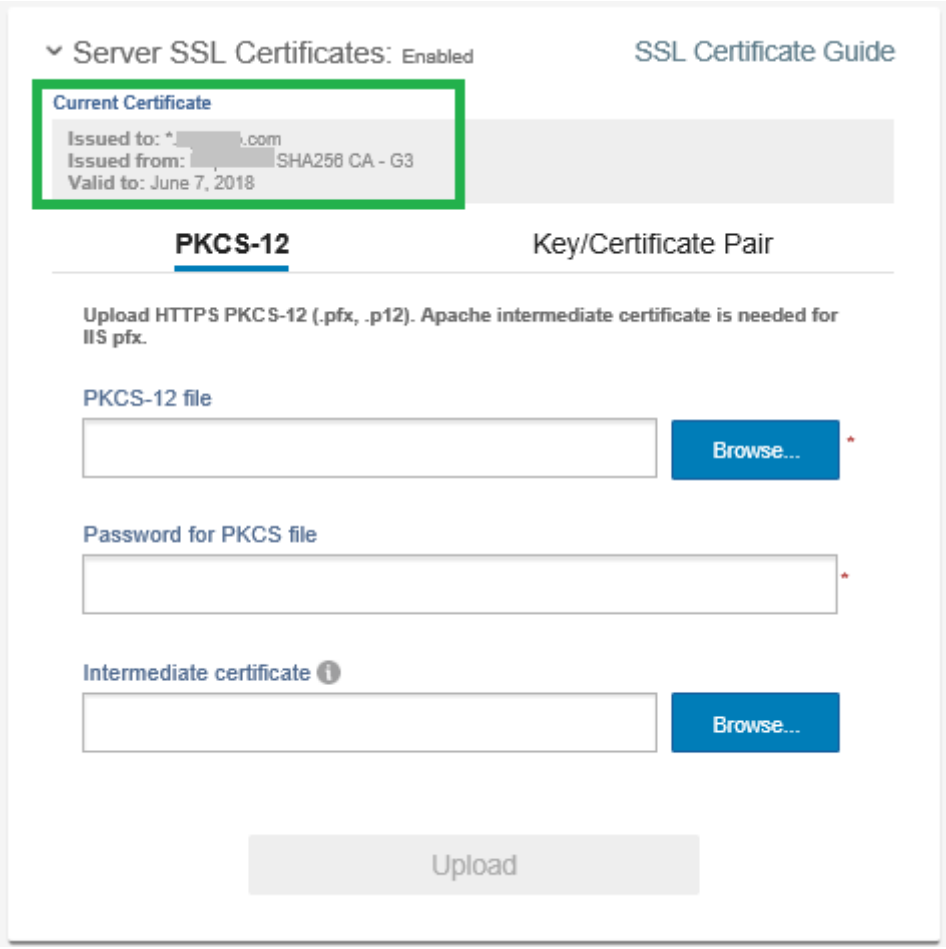


図 17. SSL 証明書の有効化

11. Wyse Management Suite が自己署名証明書またはプライベートドメイン証明書で有効になっている場合は、Wyse Management Suite リポジトリサーバに証明書をアップロードして、Wyse Management Suite CA の資格情報を検証できます。

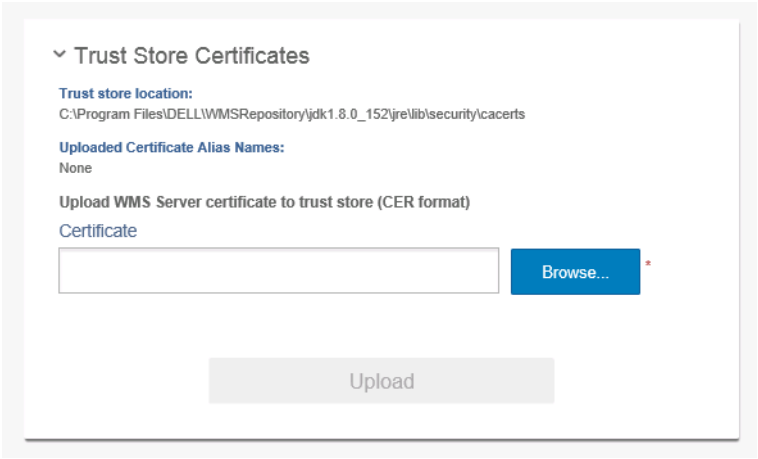


図 18. トラストストア証明書

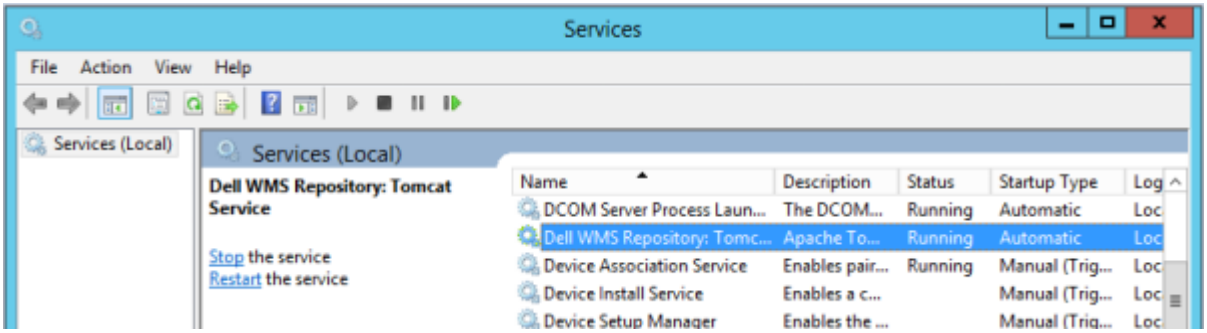
12. 登録時に入力した `C:\wmsrepo` に移動し、すべてのリポジトリファイルが保存され、管理されているフォルダを表示することができます。

トピック：

- Wyse Management Suite リポジトリサービスの管理

Wyse Management Suite リポジトリサービスの管理

Wyse Management Suite リポジトリーは、Windows ローカル サービス ウィンドウに [**Dell WMS Repository: Tomcat Service**] として表示されます。また、サーバーの再起動時に自動的に開始されるように、次のように設定されています。



18

デバイスのトラブルシューティング

[**デバイス**] ページを使用して、トラブルシューティング情報を表示および管理できます。

手順

1. **デバイスの詳細** ページで、**トラブルシューティング** タブをクリックします。
2. **スクリーンショットの要求** をクリックします。
   クライアントのアクセス許可の有無にかかわらず、Thin Client のスクリーンショットをキャプチャすることができます。[**ユーザーの受け入れが必要です**] チェック ボックスを選択した場合、クライアントにメッセージが表示されます。このオプションは、Windows Embedded Standard、Linux、および ThinLinux デバイスにのみ適用されます。
3. Thin Client 上で稼動するプロセスのリストを表示するには、**プロセスリストの要求** をクリックします。
4. Thin Client 上で稼動するサービスのリストを表示するには、**サービスリストの要求** をクリックします。
5. パフォーマンスメトリック コンソールにアクセスするには、**監視の開始** をクリックします。
   パフォーマンスメトリック コンソールには、次の詳細が表示されます。
   - 過去 1 分間の平均 CPU
   - 過去 1 分間の平均メモリー使用量

トピック：

Wyse Management Suite を使用したログ ファイルの要求

前提条件

ログファイルを取得するにはデバイスを有効にする必要があります。

手順

1. **デバイス** ページに進み、特定のデバイスをクリックします。
   デバイスの詳細が表示されます。
2. **デバイスのログ** タブをクリックします。
3. **ログファイルの要求** をクリックします。
4. Wyse Management Suite サーバーにログ ファイルをアップロードした後で、[**ここをクリック**] リンクをクリックし、ログをダウンロードします。

   メモ: ThinOS デバイスはシステムログをアップロードします。

Wyse Management Suite を使用した監査ログの表示

手順

1. **イベント** > **監査** の順に移動します。

2. **設定グループ** ドロップダウンリストから、監査ログを表示するグループを選択します。
3. **時間枠** ドロップダウンリストから、該当する期間中に発生したイベントを表示する期間を選択します。
   監査 ウィンドウでは、情報を標準的な監査ログ表示に整列します。タイムスタンプ、イベントタイプ、ソース、および各イベントの説明を時間順に表示できます。

WinHTTP プロキシーが設定されていると Wyse Management Suite へのデバイスの登録が失敗する

WDA は WinHTTP クライアントであり、ローカル システムから WinHTTP プロキシー情報を取得します。

WinHTTP プロキシーが設定されており、デバイスが Wyse Management Suite サーバーに接続できない場合は、次の手順を実行して、システム レベルで使用できるプロキシー情報を有効にします。

- **ケース 1：** デバイスがドメインに追加されている場合は、ドメインのグループ ポリシーで各ユーザーの IE-プロキシー設定を有効にします。各ユーザーではなく各クライアントの IE-プロキシー設定を有効にする場合は、ドメイン コントローラーでグループ ポリシーを設定する必要があります。

  `Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Make proxy settings per-machine` に移動して、[**有効にする**] を選択します。また、Internet Explorer で、[`IE` 設定]＞[**インターネット オプション**]＞[接続]＞[`LAN` の設定]の順に選択して、[**設定を自動的に検出する**] を有効にする方法もあります。
- **ケース 2：** デバイスがドメインに追加されていない場合は、`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings` に移動し、「**ProxySettingsPerUser**」という名前の **32 ビット DWORD** を作成して、これを 0 に設定します。また、Internet Explorer で、[`IE` 設定]＞[**インターネット オプション**]＞[接続]＞[`LAN` の設定]の順に選択して、[**設定を自動的に検出する**] を有効にする方法もあります。

RemoteFX USB リダイレクト ポリシーが USB 大容量ストレージ デバイスには適用されない

手順

1. 管理者としてデバイスにログインします。
2. 書き込みフィルターを無効にします。
3. [**ファイル名を指定して実行**] コマンドで、「`Regedit`」と入力します。
4. `HKLM\Software\Policies\Microsoft\Windows NT\Terminal Services\Client\UsbSelectDeviceByInterfaces` に進みます。
5. 文字列のレジストリ キーとして `100` を追加し、大容量ストレージ デバイスの値として `{53F56307-B6BF-11D0-94F2-00A0C91EFB8B} for CD ROM : {53F56308-B6BF-11D0-94F2-00A0C91EFB8B}` を設定します。

   メモ: 波括弧は必須です。

19

FAQ (よくある質問)

適用される設定が競合している場合、Wyse Management Suite と ThinOS UI ではどちらが優先されますか？

Wyse Management Suite を使用して作成された設定は、ThinOS クライアント上でローカルに作成された設定、または管理ポリシー ツールを使用して公開された設定よりも優先されます。

ThinOS の設定では、優先順位が次の順序になっています。

Wyse Management Suite ポリシー > 管理ポリシー ツール > ローカル ThinOS UI

Wyse Management Suite ファイル リポジトリーの使用方法を教えてください

手順

1. パブリッククラウドのコンソールから Wyse Management Suite リポジトリをダウンロードします。
2. インストールプロセスの後、アプリケーションを起動します。
3. [Wyse Management Suite リポジトリー] ページで資格情報を入力して、Wyse Management Suite リポジトリーを Wyse Management Suite サーバーに登録します。
4. リポジトリーを Wyse Management Suite パブリック クラウドに登録するには、[**パブリック WMS 管理ポータルへの登録**] オプションを有効にします。
5. **ファイルの同期** オプションをクリックして、ファイルの同期コマンドを送信します。
6. **チェックイン** をクリックしてから、**コマンドの送信** をクリックして、デバイスにデバイス情報コマンドを送信します。
7. **登録解除** オプションをクリックして、オンプレミスサービスを登録解除します。
8. **編集** をクリックしてファイルを編集します。
   a) **ファイルの同時ダウンロード** オプションのドロップダウンリストから、ファイルの数を選択します。
   b) **Wake on LAN** オプションを有効または無効にします。
   c) **ファイルの高速アップロードおよびダウンロード (HTTP)** オプションを有効または無効にします。
      - HTTP が有効な場合、ファイルのアップロードおよびダウンロードは HTTP 経由で実行されます。
      - HTTP が有効ではない場合、ファイルのアップロードおよびダウンロードは HTTPS 経由で実行されます。
   d) [**証明書の検証**] チェック ボックスを選択して、パブリック クラウドの CA 検証を有効にします。

      メモ:

      - **Wyse Management Suite サーバーからの CA 検証が有効になっている場合、クライアントに証明書が存在する必要があります。アプリおよびデータ、イメージのプル/プッシュなど、すべての操作が成功します。クライアントに証明書が存在しない場合、Wyse Management Suite サーバーの [イベント] ページに、[認証局の検証に失敗しました] という汎用監査イベント メッセージが表示されます。アプリおよびデータ、イメージのプル/プッシュなど、すべての操作が失敗します。**
      - **Wyse Management Suite サーバーからの CA 検証が無効になっている場合、サーバーおよびクライアントからの通信はセキュアなチャネルで、証明書署名の検証を行わずに実行されます。**

   e) 所定のボックスにメモを追加します。
   f) **設定の保存** をクリックします。

.csv ファイルからユーザーをインポートするにはどうすればよいですか？

手順

1. **ユーザー** をクリックします。
   ユーザー ページが表示されます。
2. **割り当て解除された管理者** オプションを選択します。
3. **一括インポート** をクリックします。
   一括インポート ウィンドウが表示されます。
4. [**参照**] をクリックして、.csv ファイルを選択します。
5. **インポート** をクリックします。

Wyse Management Suite のバージョンの確認方法

手順

1. Wyse Management Suite にログインします。
2. **[ポータル管理]** > **[サブスクリプション]** の順に移動します。
   Wyse Management Suite のバージョンが [**サーバー情報**] フィールドに表示されます。

DHCP オプション タグの作成方法と設定方法

手順

1. サーバマネージャ を開きます。
2. **ツール** に移動して、**DHCP オプション** をクリックします。
3. **[FQDN]** > **[IPv4]** の順に移動して、[**IPv4**] を右クリックします。
4. **既定のオプションの設定** をクリックします。
   既定のオプションと値 ウィンドウが表示されます。
5. **オプションクラス** ドロップダウンリストから、**DHCP 標準オプション** 値を選択します。
6. **追加** をクリックします。
   オプションタイプ ウィンドウが表示されます。
7. 必要な DHCP オプション タグを設定します。
   - 165 Wyse Management Suite サーバ URL オプションタグを作成するには、次の手順を実行します。
     a. 次の値を入力し、**OK** をクリックします。
        - 名前 - WMS
        - データタイプ - 文字列
        - コード - 165
        - 説明 - WMS_Server

     b. 次の値を入力し、**OK** をクリックします。

        文字列 - `WMS FQDN`

        例：`WMSServerName.YourDomain.Com:443`
   - 166 MQTT サーバ URL オプションタグを作成するには、次の手順を実行します。
     a. 次の値を入力し、**OK** をクリックします。
        - 名前 - MQTT
        - データタイプ - 文字列
        - コード - 166
        - 説明 - MQTT サーバ

     b. 次の値を入力し、**OK** をクリックします。

文字列 - MQTT FQDN

例：WMSServerName.YourDomain.Com:1883

- 167 Wyse Management Suite CA 検証サーバ URL オプションタグを作成するには、次の手順を実行します。
  a. 次の値を入力し、**OK** をクリックします。
     - 名前 - CA 検証
     - データタイプ - 文字列
     - コード - 167
     - 説明 - CA 検証
  b. 次の値を入力し、**OK** をクリックします。

     文字列 - TRUE または FALSE
- 199 Wyse Management Suite CA グループトークンサーバ URL オプションタグを作成するには、次の手順を実行します。
  a. 次の値を入力し、**OK** をクリックします。
     - 名前 - グループトークン
     - データタイプ - 文字列
     - コード - 199
     - 説明 - グループトークン
  b. 次の値を入力し、**OK** をクリックします。

     文字列 - defa-quarantine

メモ: オプションは、DHCP サーバのサーバオプション、または DHCP スコープのスコープオプションのいずれかに追加する必要があります。

DNS SRV レコードを作成して設定する方法

手順

1. サーバマネージャ を開きます。
2. [**ツール**] に移動して、[**DNS**] をクリックします。
3. **[DNS]** > **[DNS サーバー ホスト名]** > **[前方参照ゾーン]** > **[ドメイン]** > **[_tcp]** の順に移動し、[**_tcp option**] を右クリックします。
4. **その他の新しいレコード** をクリックします。
   リソースレコードの種類 ウィンドウが表示されます。
5. **サービスロケーション (SRV)** を選択し、**レコードの作成** をクリックして、次の手順を実行します。
   a) Wyse Management Suite サーバのレコードを作成するには、次の詳細を入力し、**OK** をクリックします。
      - サービス - _WMS_MGMT
      - プロトコル - _tcp
      - ポート番号 - 443
      - このサービスを提供するホスト - WMS サーバの FQDN

   b) MQTT サーバレコードを作成するには次の値を入力し、**OK** をクリックします。
      - サービス - _WMS_MQTT
      - プロトコル - _tcp
      - ポート番号 - 1883
      - このサービスを提供するホスト - MQTT サーバの FQDN
6. **[DNS]** > **[DNS サービス ホスト名]** > **[前方参照ゾーン]** > **[ドメイン]** の順に移動し、ドメインを右クリックします。
7. **その他の新しいレコード** をクリックします。
8. **テキスト (TXT)** を選択し、**レコードの作成** をクリックして、次の手順を実行します。
   a) Wyse Management Suite グループトークンのレコードを作成するには、次の値を入力し、**OK** をクリックします。
      - レコード名 - _WMS_GROUPTOKEN
      - テキスト - WMS グループトークン

   b) Wyse Management Suite CA 証明書のレコードを作成するには、次の値を入力して、**OK** をクリックします。
      - レコード名 - _WMS_CAVALIDATION
      - テキスト - TRUE/FALSE

ホスト名を IP アドレスに変更する方法

このタスクについて

ホスト名の解決に失敗した場合は、ホスト名を IP アドレスに変更する必要があります。

手順

1. 上級の管理モードで DOS プロンプトを開きます。
2. ディレクトリを `C:\Program Files\DELL\WMS\MongoDB\bin` に変更します。
3. 次のコマンドを入力します：`mongo localhost -username stratus -p --authenticationDatabase admin`
   出力 — MongoDB shell version v3.4.10
4. パスワードを入力します。
   出力 —
   - connecting to: mongodb://127.0.0.1:27017/localhost
   - MongoDB server version: 3.4.10
5. 入力：use stratus
   出力 — switched to db stratus
6. 次のコマンドを入力します：`> db.bootstrapProperties.updateOne( {'name': 'stratusapp.server.url'}, {$set : {'value' : "https://IP:443/ccm-web"}} )`
   出力 — { "acknowledged" : true, "matchedCount" : 1, "modifiedCount" : 1 }
7. 次のコマンドを入力します： `> db.getCollection('bootstrapProperties').find({'name': 'stratusapp.server.url'})`
   出力 — { "_id" : ObjectId("5b97905e48b7b7e99ad22aa6"), "name" : "stratusapp.server.url", "value" : "https://IP:443/ccm-web", "isActive" : true, "committed" : true }

自己署名リモート リポジトリーを使用してデバイスをイメージングする方法

Windows Embedded Standard デバイスおよび ThinLinux デバイスのイメージングは、プライベート クラウドのローカル リポジトリー、またはパブリック クラウドのリモート リポジトリーから実行できます。

前提条件

イメージをプライベート クラウドのローカル リポジトリーから、または自己署名証明書を使用してパブリック クラウドのリモート リポジトリーから導入する場合に、CA 検証が有効になっているときは、管理者は自己署名証明書を Thin Client にプッシュして、イメージングを実行する必要があります。

手順

1. Internet Explorer または MMC から自己署名証明書をエクスポートします。
2. Wyse Management Suite に証明書をアップロードします。「イメージ ポリシー」を参照してください。
3. セキュリティ ポリシーを使用して、ターゲットのクライアントまたはクライアント グループに証明書をプッシュします。
   設定ポリシー ジョブが完了するまで待ちます。
4. プライベート クラウドのローカル リポジトリーから、またはパブリック クラウドのリモート リポジトリーから、CA 検証を有効にします。
5. イメージ ポリシーを作成して、グループにスケジュールを設定します。