

Dell Wyse Management Suite

バージョン 3.1 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。

章 1: Wyse Management Suite の紹介	9
Wyse Management Suite バージョン 3.1 の新機能.....	9
Wyse Management Suite のエディション.....	9
Wyse Management Suite の機能マトリックス.....	10
章 2: Wyse Management Suite を開始する	14
パブリック クラウドでの Wyse Management Suite へのログイン.....	14
プライベート クラウドに Wyse Management Suite を導入するための前提条件.....	15
管理コンソールの機能エリア.....	15
シンクライアントの設定および管理.....	16
Wyse Device Agent.....	17
Dell Client Agent.....	18
章 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	19
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.....	19
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.....	20
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.....	20
章 4: Wyse Management Suite を使用した新しいデバイスの登録と設定	22
Wyse Management Suite を使用した新しい Windows Embedded Standard デバイスの登録と設定.....	22
Wyse Management Suite を使用した新しい ThinOS 8.x デバイスの登録と設定.....	22
Wyse Management Suite を使用した新しい ThinOS 9.x デバイスの登録と設定.....	23
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.....	24
Wyse Management Suite を使用した新しい Wyse Software Thin Client の登録と設定.....	24
Wyse Management Suite を使用した Dell Hybrid Client の登録および設定.....	25
章 5: Wyse Management Suite ダッシュボード	27
アラートの表示.....	27
イベントリストの表示.....	28
デバイスステータスの表示.....	28
登録の検証を有効にする.....	28
ユーザープリファレンスの変更.....	28
オンラインヘルプへのアクセス.....	29
パスワードの変更.....	29
管理コンソールからのログアウト.....	29
章 6: グループ管理および設定	30
管理対象外グループの編集.....	31
デフォルトのデバイス ポリシー グループの作成.....	31
ThinOS 選択グループの作成.....	32
デフォルトのデバイス ポリシー グループの編集.....	32
ThinOS 選択グループの編集.....	32

ThinOS 選択グループの削除.....	32
ユーザー ポリシー グループの作成.....	33
ユーザー ポリシー グループの編集.....	35
グローバルレベルポリシーの設定.....	35
ユーザー ポリシー グループのインポート.....	35
グループの削除.....	36
デバイスレベルのポリシーの設定.....	36
グループ ポリシーのエクスポート.....	36
グループ ポリシーのインポート.....	37
[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.....	37
[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.....	37
ThinOS ポリシー設定の編集.....	38
ThinOS - ウィザードモード.....	39
ThinOS - 詳細モード.....	39
ThinOS 9.x ポリシー設定の編集.....	39
ThinOS 9.x の BIOS 設定.....	40
Wyse Management Suite を使用した ThinOS 9.x からそれ以降のバージョンへのアップグレード.....	41
BIOS パッケージのアップロードと公開.....	41
グループと構成を使用した ThinOS 9.x アプリケーション パッケージのアップロードと公開.....	42
Windows Embedded Standard ポリシー設定の編集.....	42
Windows Embedded デバイスの導入設定の構成.....	42
Linux ポリシー設定の編集.....	43
ThinLinux ポリシー設定の編集.....	43
ThinLinux デバイスの導入設定の構成.....	43
Wyse Software Thin Client ポリシー設定の編集.....	44
Cloud Connect のポリシー設定の編集.....	44
Dell Hybrid Client ポリシー設定の編集.....	44
Dell Hybrid Client 向け Wyse Management Suite クライアント設定の設定.....	46
Dell Hybrid Client デバイスの導入設定の構成.....	47
一括デバイス例外ファイルの作成とインポート.....	47

章 7: デバイスの管理.....51

デバイスを Wyse Management Suite に登録する方法.....	52
Dell Hybrid Client の手動登録.....	52
手動検出方法を使用した Dell Hybrid Client の登録.....	54
Wyse Device Agent を使用した ThinOS デバイスの登録.....	54
Wyse Device Agent を使用した Windows Embedded Standard Thin Client の Wyse Management Suite への登録.....	55
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.....	55
Wyse デバイス エージェントを使用した ThinLinux Thin Client の登録.....	56
FTP INI メソッドを使用した ThinOS デバイスの登録.....	56
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.....	57
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.....	57
DHCP オプションタグの使用によるデバイスの登録.....	58
DNS SRV レコードの使用によるデバイスの登録.....	59
フィルターの使用によるデバイスの検索.....	60
[デバイス] ページでのフィルターの保存.....	61
デバイス ステータスの問い合わせ.....	61
デバイスのロック.....	61

デバイスの再起動.....	62
デバイスの登録解除.....	62
登録の検証.....	62
デバイスの登録の検証.....	63
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.....	63
[デバイス] ページでのグループ割り当ての変更.....	63
デバイスへのメッセージの送信.....	63
Wake On LAN コマンド.....	64
デバイスの詳細の表示.....	64
ディスプレイ パラメーターの表示.....	64
仮想 NIC の詳細の表示.....	65
BIOS の詳細の表示.....	65
デバイスの概要の管理.....	66
システム情報の表示.....	66
デバイス イベントの表示.....	66
インストール済みアプリケーションの表示.....	66
シンクライアントの名前の変更.....	67
リモート シャドール接続の有効化.....	67
Dell Hybrid Client デバイスのリモート シャドール接続の設定.....	68
デバイスのシャットダウン.....	68
デバイスにタグを付ける.....	68
デバイスコンプライアンスステータス.....	69
Windows Embedded Standard または ThinLinux イメージの引き出し.....	69
ログ ファイルの要求.....	70
デバイスのトラブルシューティング.....	70
Dell Hybrid Client の再イメージ化.....	70
Dell Hybrid Client 向け設定ユーザー インターフェイス パッケージの取得.....	71
Dell Hybrid Client の工場出荷時設定へのリセット.....	71

章 8: アプリとデータ..... 72

アプリケーションポリシー.....	72
Thin Client アプリケーション インベントリ の設定.....	73
Wyse Software Thin Client のアプリケーション インベントリ の設定.....	73
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.....	73
Wyse Software シンクライアント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.....	74
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.....	75
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.....	76
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.....	77
Dell Hybrid 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.....	78
Dell Hybrid 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.....	79
イメージポリシー.....	81
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 への追加.....	81
リポジトリへの ThinOS ファームウェアの追加.....	81
リポジトリへの ThinOS BIOS ファイルの追加.....	82
リポジトリへの ThinOS パッケージ ファイルの追加.....	82
Windows Embedded Standard および ThinLinux のイメージ ポリシーの作成.....	82
リポジトリへの ThinOS ファームウェアの追加.....	83
リポジトリへの ThinOS アプリケーション パッケージの追加.....	83
Dell Hybrid Client イメージ ポリシーの作成.....	83

ファイル リポジトリの管理.....	84
章 9: ルールの管理.....	86
登録ルールの編集.....	86
管理対象外デバイスの自動割り当てルールの作成.....	87
管理対象外のデバイスの自動割り当てルールの編集.....	87
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.....	87
ルールの順序の保存.....	87
アラート通知のルールの追加.....	88
アラート通知ルールの編集.....	88
章 10: ジョブの管理.....	89
BIOS 管理者パスワードを同期する.....	90
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.....	90
デバイス コマンド ジョブのスケジュール.....	91
イメージ ポリシーのスケジュール.....	91
アプリケーション ポリシーのスケジュール.....	92
章 11: イベントの管理.....	93
フィルターを使用したイベントまたはアラートの検索.....	93
イベントの概要の表示.....	94
監査ログの表示.....	94
エンド ユーザー セッションのレポート作成.....	94
章 12: ユーザーの管理.....	95
管理者プロファイルの新規追加.....	96
Wyse Management Suite での WMS カスタム役割の作成.....	97
未割り当ての管理者またはクラウド接続ユーザーの一括インポート.....	97
管理者プロファイルの編集.....	98
管理者プロファイルのアクティブ化.....	98
管理者プロファイルの非アクティブ化.....	98
管理者プロファイルの削除.....	98
管理者プロファイルのアンロック.....	99
管理者プロファイルの非アクティブ化.....	99
管理対象外デバイスの自動割り当てルールの作成.....	99
エンド ユーザーの追加.....	99
エンド ユーザーの編集.....	100
エンド ユーザー ポリシーの設定.....	100
エンド ユーザーの一括インポート.....	100
エンド ユーザーの削除.....	100
ユーザー プロファイルの編集.....	101
章 13: ポータル管理.....	102
Active Directory によるパブリック クラウドへの未割り当てのユーザーまたはユーザー グループのインポート.....	102
Active Directory サーバ情報の追加.....	103
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.....	104
アラート分類.....	105
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.....	105

Wyse Management Suite ファイル リポジトリへのアクセス.....	105
サブネット マッピング.....	106
その他の設定.....	107
Teradici 設定の管理.....	107
二要素認証の有効化.....	108
マルチテナントアカウントの有効化.....	108
レポートの生成.....	108
カスタムブランド化の有効化.....	109
システム セットアップの管理.....	109
章 14: Dell Wyse 5070 デバイスおよび Dell OptiPlex 7070 Ultra の Dell Hybrid Client への変換.....	111
Dell Wyse 5070 の変換.....	111
Dell Hybrid Client イメージのリポジトリへの追加.....	112
Hybrid Client イメージ ポリシーの作成.....	112
イメージポリシーのスケジュール.....	113
Dell OptiPlex 7070 Ultra の変換.....	114
章 15: セキュリティ構成.....	115
Wyse Management Suite インストーラーでの TLS バージョンの設定のサポート.....	115
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.....	115
セキュア LDAP (LDAPS) セットアップの設定.....	116
廃止されたプロトコル.....	117
章 16: Teradici デバイス管理.....	118
Teradici デバイスの検出.....	118
CIFS のユースケースのシナリオ.....	121
章 17: ライセンスサブスクリプションの管理.....	122
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.....	122
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.....	122
Thin Client のライセンス割り当て.....	123
ライセンスの注文.....	123
章 18: ファームウェアアップグレード.....	124
ThinLinux 1.x から 2.1以降のバージョンへのアップグレード.....	124
ThinLinux 2.x イメージの準備.....	124
ThinLinux 1.x から 2.x へのアップグレード.....	125
ThinOS 8.x から 9.0 へのアップグレード.....	126
リポジトリへの ThinOS ファームウェアの追加.....	126
ThinOS 8.6 から ThinOS 9.x へのアップグレード.....	126
Wyse Management Suite を使用した ThinOS 9.x からそれ以降のバージョンへのアップグレード.....	127
章 19: リモートリポジトリ.....	128
Wyse Management Suite リポジトリサービスの管理.....	133
Wyse Management Suite リモート リポジトリのプロキシ サポート.....	133
章 20: デバイスのトラブルシューティング.....	134
Wyse Management Suite を使用したログ ファイルの要求.....	134
Wyse Management Suite を使用した監査ログの表示.....	134

WinHTTP プロキシ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.....	135
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.....	135
Wyse Management Suite から設定された WiFi 設定が複数の Wyse 5070 Thin Client 間で固定されない.....	135

章 21: FAQ (よくある質問) 137

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？.....	137
Wyse Management Suite ファイル リポジトリの使用方法を教えてください.....	137
.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？.....	138
Wyse Management Suite のバージョンの確認方法.....	138
DHCP オプション タグの作成方法と設定方法.....	138
DNS SRV レコードを作成して設定する方法.....	139
ホスト名を IP アドレスに変更する方法.....	140
自己署名リモート リポジトリを使用してデバイスをイメージングする方法.....	140

Wyse Management Suite の紹介

Wyse Management Suite は、Dell Hybrid Client 搭載のエンドポイントおよび Dell Thin Client を集中的に設定、監視、管理、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導入、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、構成管理、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、モニタリング、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 3.1 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 3.1 の新機能

- デバイス例外の設定を複数の ThinOS 9.x デバイスに導入。
- ThinOS 9.x の署名済みパッケージの EULA の詳細を表示。
- きめ細かな権限ロール ベースのアクセス。
- 構成 UI での静的パラメーターの検索。
- ThinOS 9.x での BIOS 列挙。
- Windows Embedded、ThinLinux、Dell Hybrid Client デバイス用のアプリケーションのサイレント導入の設定。
- 詳細アプリケーション ポリシーまたは標準アプリケーション ポリシーを使用した ThinLinux のスクリプト サポート。
- Wyse Management Suite サーバー、リポジトリ サーバー、インポート ツール インストーラーの EULA の変更。
- ディスプレイ パラメーターのレポート作成、プライマリー ディスプレイ パラメーター フィールドのハイライト表示。
- 仮想 NIC のパラメーターのレポート作成、プライマリー パラメーター フィールドのハイライト表示。
- Dell Hybrid Client デバイス用 VNC の設定。
- Dell Hybrid Client デバイス用 SSH の設定。
- リポジトリ サーバー用 SOCKS 5 プロキシ プロトコル。
- Dell Wyse 5070 デバイスの Dell Hybrid Client への変換。
- DCA-Enabler 1.1 を使用した、Dell OptiPlex 7070 Ultra の Dell Hybrid Client への変換。

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 は基本機能を提供し、プライベートクラウド導入環境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。このバージョンは、Dell Thin Client のみを管理できます。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、より堅牢なソリューションです。パブリッククラウドとプライベートクラウドの両方の導入環境で使用できます。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)。Pro ソリューションにより、組織は必要に応じてプライベートクラウドとパブリッククラウド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。このバージョンは、すべての Teradici ベースのデバイス、Wyse Converter for PCs ベースのシンクライアント、Dell Hybrid Client デバイス、Embedded PC、Edge Gateway デバイス用を管理するために必要です。また、Dell Thin Client を管理するための高度な機能も提供します。パブリッククラウド導入環境では、Pro Edition をホーム オフィス、サードパーティー、パートナー、モバイルシンクライアントなどの非企業ネットワーク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

① 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 Web 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 Pro のプライベート クラウド	Wyse Management Suite Pro のクラウド 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 1万台のデバイスまで無料	最大 12万台のデバイス	最大 100万台のデバイス
ライセンス条件	無料ダウンロード	シートあたりのサブスクリプション	シートあたりのサブスクリプション
ライセンス キー	不要	必須	必須
アーキテクチャ	プライベート クラウド	プライベート クラウド	パブリック クラウド
柔軟な導入またはハイブリッド クラウド	X	√	√
詳細インストーラ	X	√	√
マルチテナント	X	√	√
権限単位の委任管理	X	√	√
分散アーキテクチャをサポートするための複数リポジトリ	X	√	√
Wyse Management Suite サーバー エイリアスを設定するオプション	X	√	√
高可用性リファレンス アーキテクチャ	X	√	X
プロキシ サポート - SOCKS5	√	√	√
Dell ProSupport for Software 同梱	X	√	√
レポート作成およびモニタリング			
ローカライズされた管理コンソール	X	√	√
E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、イベント、および監査ログ	X	√	√

表 1. 各サブスクリプションタイプの機能マトリックス (続き)

機能	Wyse Management Suite Standard	Wyse Management Suite Pro のプライベートクラウド	Wyse Management Suite Pro のクラウドエディション
エンタープライズグレードのレポート作成	×	√	√

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 Dell Hybrid Client 管理機能についての情報を提供します。

表 2. Dell Hybrid Client 管理機能マトリックス

Dell Hybrid Client 管理機能	Wyse Management Suite Standard	Wyse Management Suite Pro のプライベートクラウド	Wyse Management Suite Pro のクラウドエディション
完全な資産の可視性			
自動デバイス検出	×	√	√
資産、インベントリ、およびシステム管理	×	√	√
継承後のデバイス Wyse Management Suite レベルでの有効な設定の表示	×	√	√
セキュリティ			
セキュア通信 (HTTPS)	×	√	√
多要素認証	×	√	√
ロールベースの管理のための Active Directory 認証	×	√	√
シングルサインオン	×	√	√
ロックダウン設定 (サポートされているエンドポイントのポートを有効化/無効化)	×	√	√
包括的な管理			
オペレーティングシステムのパッチおよびイメージの管理	×	√	√ *
スマートスケジューリング	×	√	√
サイレント導入	×	√	√
導入をシンプルに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	×	√	√
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	×	√	√
アプリケーションポリシーおよびサブネットマッピングへのリポジトリ割り当て	×	√	√
詳細なアプリ管理およびアプリポリシー	×	√	√
ユーザーグループの継承	×	√	√
エンドユーザーの例外	×	√	√
設定			

表 2. Dell Hybrid Client 管理機能マトリックス (続き)

Dell Hybrid Client 管理機能	Wyse Management Suite Standard	Wyse Management Suite Pro のプライベートクラウド	Wyse Management Suite Pro のクラウドエディション
Dell Hybrid Client ウィザードの設定	X	√	√
マルチモニターサポート	X	√	√
Follow-me プロファイル	X	√	√
アプリケーションの配信モードに優先順位を付けるためのファイル所属	X	√	√
BIOS 設定および構成サポート	X	√	√
ポリシー設定のエクスポートまたはインポート	X	√	√
デフォルトのユーザーグループポリシー	X	√	√
ブラウザーの設定	X	√	√
クラウドプロバイダーの設定	X	√	√
VNC の設定	X	√	√
SSH の設定	X	√	√

ⓘ **メモ:** *アスタリスクは、Dell Hybrid Client の場合、Wyse Management Suite パブリッククラウド環境を使用しているときにオンプレミスリポジトリが必要であることを示します。

次の表は、各サブスクリプションでサポートされている Wyse シンクライアントおよびゼロクライアントの管理機能に関する情報を提供します。

表 3. Wyse シンクライアントおよびゼロクライアントの管理機能マトリックス

Wyse シンクライアントおよびゼロクライアントの管理機能	Wyse Management Suite Standard	Wyse Management Suite Pro のプライベートクラウド	Wyse Management Suite Pro のクラウドエディション
完全な資産の可視性			
自動デバイス検出	√	√	√
資産、インベントリ、およびシステム管理	√	√	√
継承後のデバイスレベルでの有効な設定の表示	√	√	√
レポート作成およびモニタリング			
VNC を使用したリモートシャドウ	√	√	
設定可能なハートビートおよびチェックイン間隔	√	√	√
セキュリティ			
セキュア通信 (HTTPS)	√	√	√
802.1x 証明書の導入	√	√	√
2 要素認証	X	√	√

表 3. Wyse シンクライアントおよびゼロクライアントの管理機能マトリックス (続き)

Wyse シンクライアントおよびゼロクライアントの管理機能	Wyse Management Suite Standard	Wyse Management Suite Pro のプライベートクラウド	Wyse Management Suite Pro のクラウドエディション
ロールベースの管理のための Active Directory 認証	X	√	√
ドメイン参加機能 (Windows Embedded Standard)	X	√	√
ロックダウン設定 (サポートされているエンドポイントのポートを有効化/無効化)	X	√	√
包括的な管理			
オペレーティングシステムのパッチおよびイメージの管理	√	√	√ **
スマート スケジューリング	√	√	√
サイレント導入	√	√	√
導入をシンプルに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	√	√
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	√	√
アプリケーション ポリシーおよびサブネット マッピングへのリポジトリ割り当て	X	√	√
詳細なアプリ ポリシー	X	√	√
設定			
Wyse ThinOS 8.x ウィザードの設定	√	√	√
マルチモニターサポート	√	√	√
Wyse Easy Setup および Wyse Overlay Optimizer	√	√	√
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スクリプト作成のサポート	X	√	√
BIOS 設定および構成サポート	X	√	√
ポリシー設定のエクスポート/インポート	X	√	√
RSP パッケージサポート	X	√	√
WDM インポート ツール	X	√	X
一括デバイス例外	X	√	√

メモ: **二重のアスタリスクは、ThinLinux および Windows 10 IoT Enterprise オペレーティングシステムの場合、Wyse Management Suite パブリッククラウド環境を使用するときにオンプレミス リポジトリが必要であることを示します。

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](#)
- [プライベートクラウドに Wyse Management Suite を導入するための前提条件](#)
- [管理コンソールの機能エリア](#)
- [シンクライアントの設定および管理](#)
- [Wyse Device Agent](#)
- [Dell Client Agent](#)

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.wysmanagementsuite.com/ccm-web
 - **EU データセンター**：eu1.wysmanagementsuite.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。

初めて Wyse Management Suite コンソールにログインした場合、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 Dell 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、次の操作を行います。

1. 管理コンソールの右上隅のアカウントリンクをクリックします。
2. **パスワードの変更** をクリックします。

- 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。

ログアウト

管理コンソールからログアウトするには、次の操作を行います。

1. 管理コンソールの右上隅のアカウントリンクをクリックします。
2. **サインアウト** をクリックします。

プライベートクラウドに Wyse Management Suite を導入するための前提条件

表 4. 前提条件

説明	デバイス 1 万台以下	デバイス 5 万台以下	デバイス 12 万台以下	Wyse Management Suite - ソフトウェアリポジトリ
オペレーティング システム	Windows Server 2012 R2、Windows Server 2016、または Windows Server 2019 Standard。 Wyse Management Suite Web サーバーには、Apache Tomcat Web サーバーが組み込まれています。Microsoft IIS、Apache Tomcat Web サーバーを個別にインストールしないようにしてください。 対応言語パック - 英語、フランス語、イタリア語、ドイツ語、スペイン語、日本語、繁体字中国語			
最小ディスク領域	40 GB	120 GB	200 GB	120 GB
最小メモリー (RAM)	8 GB	16 GB	32 GB	16 GB
最小 CPU 要件	4	4	16	4
ネットワーク通信ポート	Wyse Management Suite インストーラーは、Transmission Control Protocol (TCP) ポート 443、8080、1883 をファイアウォールの例外リストに追加します。これらのポートは、Wyse Management Suite コンソールにアクセスするため、およびシンクライアントにプッシュ通知を送信するために追加されます。 <ul style="list-style-type: none"> ● TCP 443 - HTTPS 通信 ● TCP 1883 - MQTT 通信 ● TCP 3306 - MariaDB (リモートの場合はオプション) ● TCP 27017 - MongoDB (リモートの場合はオプション) ● TCP 11211 — Memcached ● TCP 5172、49159 — エンドユーザー管理ソフトウェア開発キット (EMSDK) — Teradici デバイスを管理する場合にのみ必要なオプション インストーラーで使用されるデフォルトポートは、インストール時に別のポートに変更されている可能性があります。			Wyse Management Suite リポジトリインストーラーは、TCP ポート 443 および 8080 をファイアウォールの例外リストに追加します。ポートは、Wyse Management Suite によって管理されているオペレーティングシステムのイメージとアプリケーションイメージにアクセスするために追加されます。
対応ブラウザ	Internet Explorer バージョン 11 Google Chrome バージョン 58.0 以降 Mozilla Firefox バージョン 52.0 以降 Windows の Edge ブラウザー - 英語版のみ			

- Overlay Optimizer バージョン 1.0 およびインストール スクリプトは、Wyse Management Suite インストーラーに付属しています。Overlay Optimizer を Wyse Management Suite で有効にするには、管理者がスクリプトを実行する必要があります。
- Dell Secure Client バージョン 1.0 のインストール スクリプトは、Wyse Management Suite インストーラーに付属しています。管理者は、スクリプトを実行して、Dell Secure Client を Wyse Management Suite で有効にする必要があります。

メモ: WMS.exe および WMS_Repo.exe を 2 台の異なるサーバーにインストールする必要があります。パブリッククラウドの場合、Wyse Management Suite のリモートリポジトリをインストールする必要があります。プライベートクラウドの場合、Wyse Management Suite のリモートリポジトリとローカルリポジトリをインストールする必要があります。ソフトウェアは、物理または仮想マシンにインストールすることができます。またソフトウェアのリポジトリと Wyse Management Suite サーバーが同じオペレーティングシステムを使用している必要はありません。

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。また、エンドユーザーの管理のために **[エンドユーザー]** タブが追加されています。
- **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]** ページでは、デバイス アプリケーション、アプリケーション インベントリ、およびファイル リポジトリの管理を行うことができます。
- **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、WakeUp On LAN、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、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、Dell Hybrid Client のライセンス 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、設定パラメーターは、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。詳細な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、プリ/ポストインストール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シンクライアントへの導入は、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。グループかサブグループか、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かタイムゾーンかなど、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ーの他、各パラメーター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ー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。

Wyse Device Agent

Wyse Device Agent (WDA) は、すべてのシンクライアント管理ソリューション向けの統合エージェントです。WDA をインストールすると、Wyse Management Suite を使用してシンクライアントを管理できます。

Wyse Device Agent では、次の3種類のカスタマーセキュリティ環境がサポートされています。

- **非常に安全な環境** - 新しいデバイス検出の際に不正な DHCP または DNS サーバーに対するリスクを軽減するために、管理者は各デバイスに個別にログインし、Wyse Management Suite サーバー URL を設定する必要があります。CA 署名証明書または自己署名証明書のいずれかを使用できます。ただし、デルでは CA 署名付き証明書を使用することをお勧めします。自己署名証明書付き Wyse Management Suite プライベートクラウドソリューションでは、証明書はすべてのデバイスに手動で設定する必要があります。また、証明書をエージェント設定フォルダーにコピーして、証明書を保持し、デバイスを再イメージ化した後でも、不正な DHCP または DNS サーバーに対するリスクを軽減する必要があります。

エージェント設定フォルダーは、次の場所にあります。

- Windows Embedded Standard デバイスの場合 — %SYSTEMDRIVE%\Wyse\WCM\ConfigMgmt\Certificates
- ThinLinux デバイスの場合 - /etc/addons.d/WDA/certs
- ThinOS デバイスの場合 - wnos/cacerts/

メモ: USB ドライブまたは FTP パスを使用して、ThinOS オペレーティングシステムを実行しているシンクライアントに証明書をインポートする必要があります。

- **安全な環境** — 新しいデバイス検出の際に不正な DHCP または DNS サーバーに対するリスクを軽減するために、管理者は CA 署名証明書を使用して Wyse Management Suite サーバーを設定する必要があります。デバイスは、DHCP/DNS レコードから Wyse Management Suite サーバーの URL を取得し、CA 検証を実行できます。自己署名証明書付きの Wyse Management Suite プライベートクラウドソリューションでは、デバイスに登録前の証明書がない場合、最初の登録後に証明書をデバイスにプッシュする必要があります。この証明書は、デバイスを再イメージ化または再起動した後も保持され、不正な DHCP サーバーまたは DNS サーバーに対するリスクを軽減します。
- **通常環境** — デバイスは、CA 署名証明書または自己署名証明書で設定された Wyse Management Suite プライベートクラウドの DHCP/DNS レコードから Wyse Management Suite サーバーの URL を取得します。デバイスで CA 検証オプションが無効になっている場合、デバイスを初めて登録した後、Wyse Management Suite 管理者に通知されます。このシナリオでは、管理者はサーバーが自己署名証明書で設定されているデバイスに証明書をプッシュすることをお勧めします。この環境はパブリッククラウドでは使用できません。

Dell Client Agent

Dell Client Agent (DCA) は、Dell Hybrid Client 管理ソリューション向けの統合エージェントです。DCA をインストールすると、Wyse Management Suite を使用して Dell Hybrid Client を管理できます。

DCA Enabler は、OptiPlex 7070 Ultra デバイス上で Ubuntu バージョン 18.04 LTS 64 ビットを管理するためのクライアントエージェントです。Dell Hybrid Client ソフトウェアは、Dell Client Agent Enabler (DCAE) と一緒に事前にロードされています。DCA-Enabler を使用すると、Wyse Management Suite によって管理される次のアクションを実行できます。

- 登録
- リアルタイム コマンド (RTC) の導入
- サーバーからの登録解除
- 標準アプリケーション ポリシーの導入
- 証明書ポリシーの導入

Dell Hybrid Client を OptiPlex 7070 Ultra デバイスにインストールするには、次の手順に従います。

1. 検出方法 (DNS または DHCP) または **reg.json** の手動方法を使用して、Wyse Management Suite にデバイスを登録します。この方法については、「[Wyse Management Suite にデバイスを登録する方法](#)」を参照してください。
2. OptiPlex 7070 Ultra デバイスを再イメージ化します。方法については、「[Dell Hybrid Client の再イメージ化](#)」を参照してください。

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](#)
- ① **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。
- ① **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

手順

1. WDA.exe ファイルを Thin Client にコピーします。
2. WDA.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。
 - ① **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ーフェースに、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を使用している場合は、WDA.exe ファイルをリポジトリ内の thinClientApps フォルダにコピーします。

手順

1. WDA.exe ファイルをリポジトリにコピーした後、[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RPMは、ローカルリポジトリで使用できます。
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。

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

トピック：

- Wyse Management Suite を使用した新しい Windows Embedded Standard デバイスの登録と設定
- Wyse Management Suite を使用した新しい ThinOS 8.x デバイスの登録と設定
- Wyse Management Suite を使用した新しい ThinOS 9.x デバイスの登録と設定
- 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
- Wyse Management Suite を使用した新しい Wyse Software Thin Client の登録と設定
- Wyse Management Suite を使用した Dell Hybrid Client の登録および設定

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。
 - ① **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。
 - ① **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. セットアップを確認するには、[**キーの検証**] をクリックします。
 ⓘ **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サーバーの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 サーバー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. セットアップを確認するには、[**キーの検証**] をクリックします。
 ⓘ **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サーバーの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。

- Wyse Management Suite にログインします。
- 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。
- 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

- 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。
- 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。
- 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。
- 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

- 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。
- 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。
- 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。

- 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。


Wyse Management Suite を使用した Dell Hybrid Client の登録および設定

前提条件

デバイスを登録する前に、お使いのデバイスに Wyse Management Suite サーバーへのネットワーク接続があることを確認してください。

メモ: デバイスの登録または登録解除は、ゲスト ユーザー アカウントからのみ行うことができます。

手順

- Dell Hybrid Client にゲスト ユーザーとしてログインします。
- 最上部のバーで、 をクリックします。

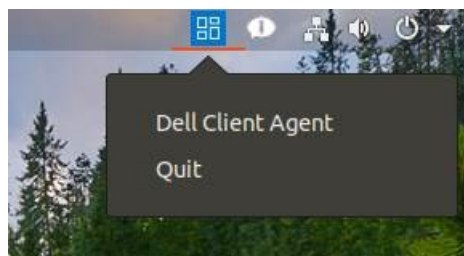


図 1. DCA アイコン

- [Dell Client Agent] をクリックします。
[Dell Client Agent] ダイアログ ボックスが表示されます。
- [登録] をクリックします。
デフォルト ステータスは、[検出進行中] と表示されます。
- 手動で登録するには、[キャンセル] ボタンをクリックします。
- [WMS サーバー] フィールドに、Wyse Management Suite サーバーの URL を入力します。
- [グループのトークン] フィールドで、グループの登録キーを入力します。グループ トークンは、デバイスをグループに直接登録するための固有のキーです。

メモ: [テナント] フィールドと [グループ] フィールドが空の場合は、デバイスは管理対象外グループに登録されます。ただし、グループ トークンは、パブリック クラウドにデバイスを登録するために必須です。

- [オン/オフ] ボタンをクリックして、[サーバー証明書 CA の検証] オプションを有効または無効にします。このオプションを有効にすると、すべてのデバイスとサーバー間の通信についてサーバー証明書の検証が実行されます。
CA 検証オプションは自動的に有効になり、パブリック クラウドの URL が入力された場合は無効にすることはできません。
- [登録] をクリックして、Wyse Management Suite サーバーに自分のハイブリッド クライアントに登録します。
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。

ハイブリッド クライアントが正常に登録されると、ステータスは [登録済み] として表示され、[登録ステータス] ラベルの横に緑色のチェック マークが表示されます。[登録] ボタンのキャプションが [登録解除] に変わります。

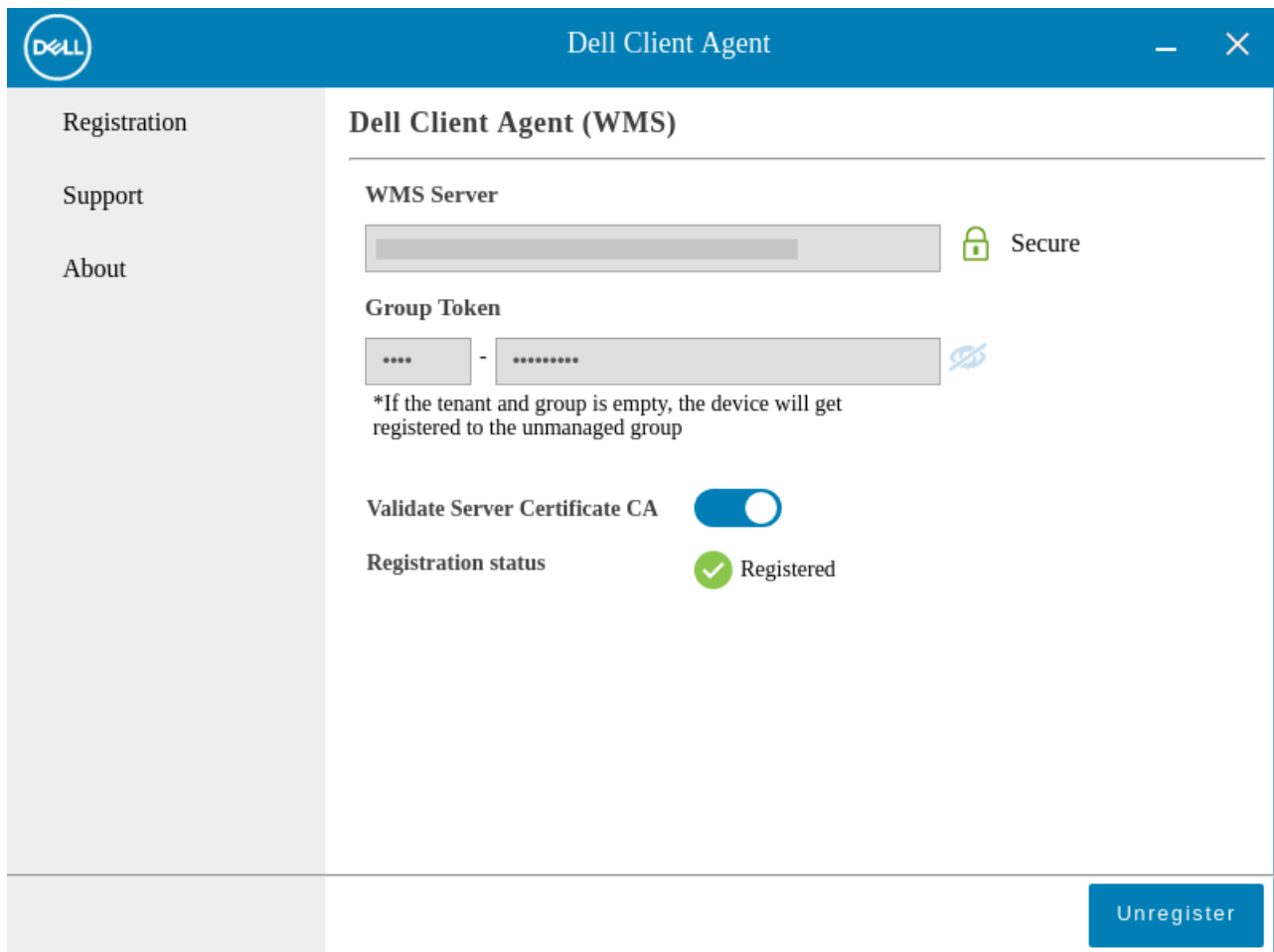


図 2. Dell Client Agent

10. Wyse Management Suite にログインします。
11. 目的のグループにデバイスを追加します (オプション)。方法については、「[グループ管理および設定](#)」を参照してください。
12. 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。
 - [\[グループと設定\]](#) ページを使用。方法については、「[Dell Hybrid 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。

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。

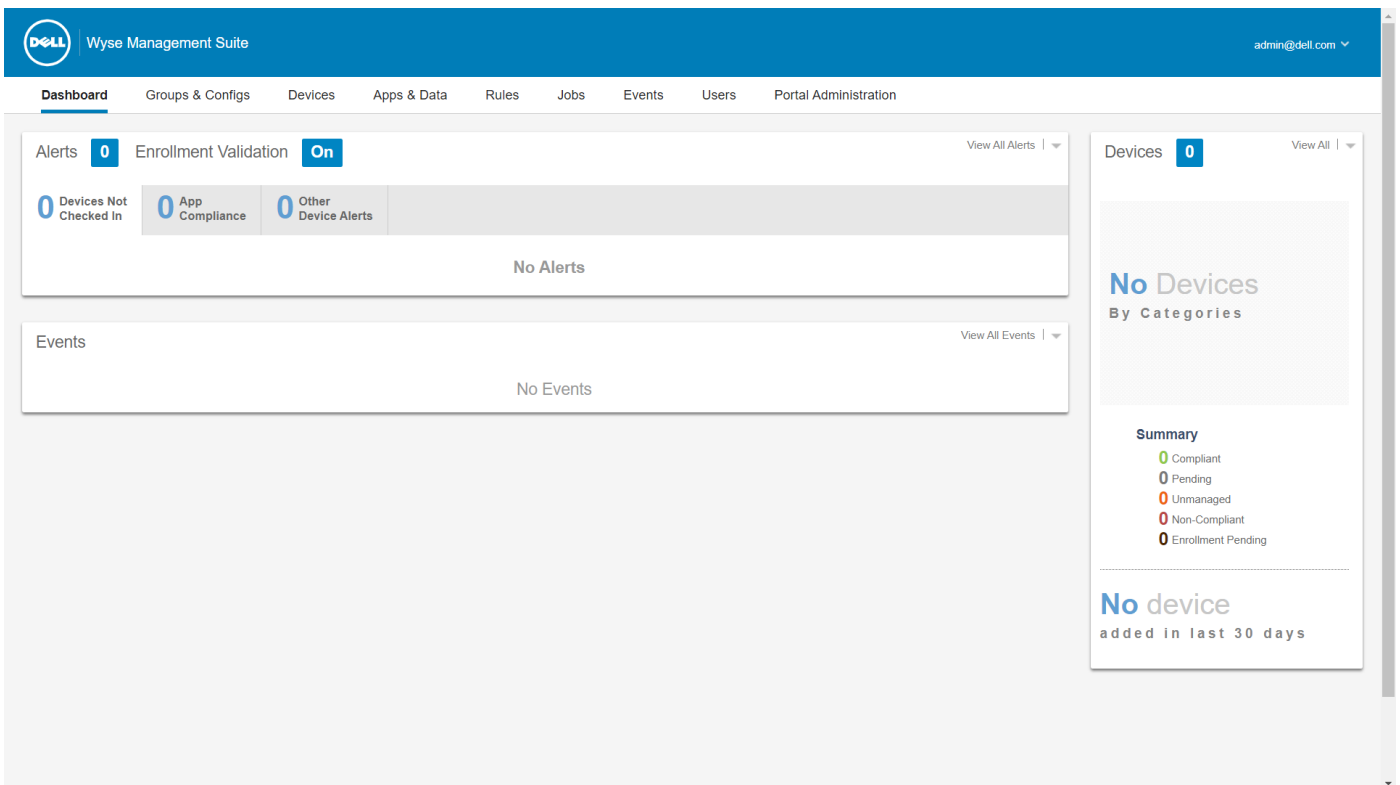


図 3. ダッシュボード

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、最近数日以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。
ユーザープリファランス 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。

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**
- **Hybrid 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。

特定の資産の設定が、設定されている場所の詳細（グローバル、グループ、およびデバイスレベル）とともに、この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。

i **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、ネットワーク、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。

i **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 レベル ポリシー
- デバイス グループ レベル ポリシー
- デバイスの例外
- ユーザー グループ レベル ポリシー
- ユーザーの例外
- ユーザーの個人設定

トピック：


- [管理対象外グループの編集](#)
- [デフォルトのデバイス ポリシー グループの作成](#)
- [ユーザー ポリシー グループの作成](#)
- [グローバルレベルポリシーの設定](#)
- [ユーザー ポリシー グループのインポート](#)
- [グループの削除](#)
- [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
- Dell Hybrid Client ポリシー設定の編集
- 一括デバイス例外ファイルの作成とインポート

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。

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。
4. 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。このステップはオプションです。
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。
5. [**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。
6. グループトークンを入力します。
7. [**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。
8. **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 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。
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。


デフォルトのデバイス 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 デバイス ポリシー グループ**] を選択します。
2. [**デフォルト デバイス ポリシー グループの編集**] ダイアログ ボックスで、必要なグループ情報を編集します。
3. **保存** をクリックします。

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.  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、左矢印をクリックします。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。

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. [グループ] 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ターゲット 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。
 - ① **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。
 - ① **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。

ユーザー ポリシー グループの作成

グローバル ユーザー グループ ポリシーのグループを作成し、ユーザー グループに応じてユーザーと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 ユーザー 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]、[説明]、[ドメイン]、[AD 属性] (AD グループまたは OU グループ)、[AD 属性名] (AD ドメインに存在する名前) を入力します。グループ名を AD 属性名として使用する必要があります。

Add New Group X

Group Name *

Description *

Parent Group **Default User Policy Group**

Domain *

AD Attribute AD group ?

AD Attribute Name *

Administration
Device Group Mapping

Select which group admin(s) will be managing this group (Optional).

Available Group Admins

>
<

Assigned Group Admins

Cancel
Save

図 4. 新規グループの追加

メモ: AD グループがドメイン内の OU グループに含まれている場合は、[AD 属性] として [OU グループ] を選択する必要があります。

4. 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。
5. **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。
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。

i **メモ:** ユーザー ポリシー グループは、AD グループまたは組織単位に割り当てる必要があります。ただし、AD グループまたは組織単位の両方に割り当てることはできません。


7. [**デバイス グループ マッピング**] オプションを選択してデバイス マッピングとともにユーザー グループをインポートすることで、デフォルトですべてのデバイス グループに適用される設定を制御できます。

Wyse Management Suite にインポートされる AD ユーザー グループは、それぞれのデバイス グループにマッピングすることができます。デバイスをマッピングすることによって、不要なユーザー グループ ポリシーを受信することはありません。

i **メモ:** デフォルトでは、ユーザー グループはデバイス グループにマッピングされません。[**デフォルト デバイス グループ**] のポリシーを選択した場合は、すべてのサブデバイス グループが選択されます。この機能は、Wyse Management Suite Pro ライセンスでのみ使用可能です。Wyse Management Suite には 100 ユーザー グループをインポートすることができます。

ユーザー 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、デフォルトのユーザー 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 ユーザー ポリシー グループの編集**] ダイアログ ボックスで、必要なグループ情報を編集します。
4. **保存** をクリックします。

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。

ユーザー ポリシー グループのインポート

手順

1. [**グループ & 設定**] ページで、[**デフォルト ユーザー 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. [**一括インポート**] ダイアログ ボックスで、[**参照**] をクリックして、.csv ファイルを選択します。

この.csv ファイルには、次の順序で詳細を含める必要があります。

- グループ名 - 表示名
- 説明
- ドメイン - ドメイン名
- AD 属性 - AD グループまたは OU グループ
- AD 属性名 - AD ドメインに存在するグループ名



i **メモ:** グループ名を AD 属性名として使用する必要があります。また、AD グループがドメイン内の OU グループに含まれている場合は、[**AD 属性**] として [**OU グループ**] を選択する必要があります。

4. .csv ファイルにヘッダー行が含まれている場合は、[**CSV ファイルにヘッダー行を含む**] チェック ボックスを選択します。
5. [**インポート**] をクリックします。

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、現在のグループ内のユーザーおよびデバイスを移動する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:** デバイス グループを削除すると、そのグループのすべてのデバイスが、選択したデバイス グループに移動されます。ユーザー グループが削除されると、それに関連付けられているデバイスまたはユーザーはなくなります。

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。
 **メモ:** ポリシーのインポートに失敗しないようにするには、ファイルにエクスポートする前に、パスワード、および証明書、壁紙、ファームウェア、ロゴなどのファイルへのすべての参照を削除してください。

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**] - この警告は、オペレーティング システム の設定をグループにインポートするときに、そのグループにその設定が含まない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]** - この警告は、新しいオペレーティング システム タイプの設定をグループにインポートするときに、そのグループにそのオペレーティング システム タイプの設定が含まれ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]** - この警告は、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際に表示されます。
8. [**インポート**] をクリックします。
 - ① **メモ:** インポートできるのは、選択したデバイス タイプの設定のみです。選択したデバイス タイプのターゲット グループで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を適用する前に削除されます。
 - ① **メモ:** グループ ポリシーのインポート中、パスワードと参照ファイルはインポートされません。ポリシーを公開する前に、管理者はこれらを選択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 - [参照] をクリックして、JSON ファイルを選択します。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**] - この警告は、グループにデバイス タイプの設定をインポートするときにグループにこのデバイス タイプの設定が含まれていない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]** - この警告は、グループにデバイス タイプの設定をインポートするときにグループにこのデバイス タイプの設定が含まれ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]** - この警告は、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際に表示されます。
 7. [**インポート**] をクリックします。
 - ① **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。
 - ① **メモ:** グループ ポリシーは、ファイルを使用してデバイスからユーザー グループに (その逆も)、またはグループから別のグループにインポートまたはエクスポートすることができます。BIOS、ドメイン参加などのサポートされていない設定は、ユーザー グループに設定をインポートする際に無視されます。

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。

- ① **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
 - ① **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。
 - ① **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。

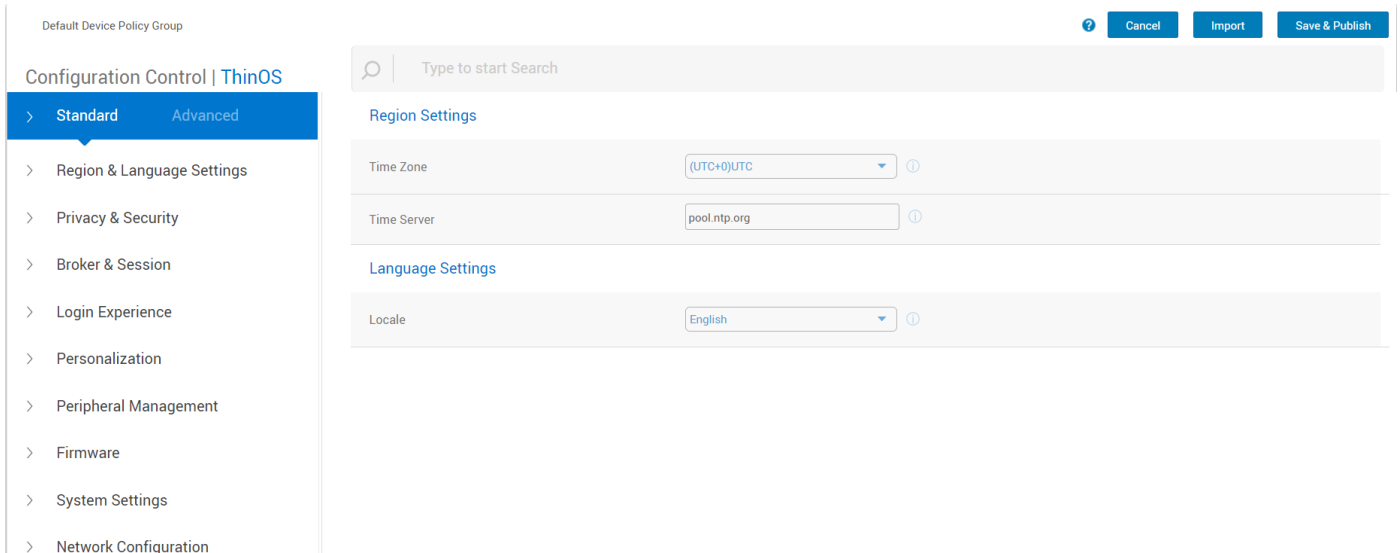


図 5. 構成制御 | ThinOS

3. 詳細設定または標準オプションをクリックします。
 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。
グローバル検索オプションを使用して、ポリシー設定で使用できる関連する設定またはパラメーターを検索することができます。検索結果には、次の順序で設定が表示されます。
 - 設定
 - パラメーター グループ
 - パラメーター サブグループ
 - パラメーター
 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.x の BIOS 設定

このタスクについて

BIOS 設定は、Wyse Management Suite 2.1 を使用した ThinOS 9.x デバイスに設定することができます。[グループ & 設定] ページ、またはサブネット マッピング オプションを使用して、BIOS パッケージを導入することができます。

メモ: この機能は、Wyse Management Suite Pro ライセンスでのみ使用可能です。

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。
[設定コントロール | ThinOS] ウィンドウが表示されます。
2. [ポリシーの編集] ドロップダウン メニューから、[ThinOS 9.x] をクリックします。
3. [詳細設定] をクリックします。
4. [BIOS] フィールドで、[プラットフォームの選択] をクリックして、BIOS 設定を構成するプラットフォームを選択します。

Wyse Management Suite を使用した 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

- グループ トークンを使用してグループを作成したことを確認します。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。
- シンクライアントが Wyse Management Suite に登録されていることを確認します。

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 アップデート** をクリックします。
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。
パッケージの EULA の詳細とベンダーの名前が表示されます。
6. 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。
 - EULA がパッケージに組み込まれている場合は、パッケージの EULA の詳細とベンダーの名前が表示されます。ベンダー名をクリックして、各ベンダーのライセンス契約を読むことができます。**承諾** をクリックしてパッケージをアップロードします。複数のパッケージをアップロードする場合は、各パッケージの EULA 詳細が表示されます。パッケージのライセンス契約には個別に同意する必要があります。
 - EULA に同意しない場合、ファームウェアはインストールされません。

i **メモ:** リモート リポジトリ、テナント クラウド リポジトリ、またはオペレーター クラウド リポジトリから、複数のファームウェア パッケージをアップロードして導入することができます。
7. **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。

i **メモ:** リモート リポジトリ、テナント クラウド リポジトリ、またはオペレーター クラウド リポジトリから、複数のファームウェア パッケージをアップロードして導入することができます。
8. [**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。

BIOS パッケージのアップロードと公開

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.x 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、[**BIOS ファームウェア アップデート**] をクリックします。
5. [**導入する ThinOS BIOS 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。

i **メモ:** リモート リポジトリ、テナント クラウド リポジトリ、またはオペレーター クラウド リポジトリから、複数のファームウェア パッケージをアップロードして導入することができます。テナント クラウド リポジトリから 10 個のパッケージをアップロードすることができます。
6. [**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。

また、次に説明する手順に従って、Wyse Management Suite 2.1の [アプリとデータ] から BIOS ファームウェアをアップロードすることもできます。

- a. [アプリとデータ] ページに移動します。
- b. [OS イメージリポジトリ] をクリックして、[ThinOS 9.x] を選択します。
- c. [BIOS ファイルの追加] をクリックして、リポジトリに追加するファイルを参照して追加します。

 **メモ:** この機能は、Wyse Management Suite Pro ライセンスでのみ使用可能です。


グループと構成を使用した ThinOS 9.x アプリケーション パッケージのアップロードと公開

前提条件

- グループ トークンを使用してグループを作成したことを確認します。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。
- 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 パッケージのアップデート] をクリックします。
5. 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。
 - EULA がパッケージに組み込まれている場合は、パッケージの EULA の詳細とベンダーの名前が表示されます。ベンダー名をクリックして、各ベンダーのライセンス契約を読むことができます。承諾をクリックしてパッケージをアップロードします。複数のパッケージをアップロードする場合は、各パッケージの EULA 詳細が表示されます。パッケージのライセンス契約には個別に同意する必要があります。
 - EULA がパッケージに組み込まれていない場合、手順 6 に進みます。

 **メモ:** リモートリポジトリ、テナントクラウドリポジトリ、またはオペレータークラウドリポジトリから、複数のファームウェア パッケージをアップロードして導入することができます。
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。

Windows Embedded デバイスの導入設定の構成

Wyse Management Suite 3.1 からは、Windows Embedded デバイスの導入設定を構成することができます。デバイスに構成をサイレント導入するように設定することができます。

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、**WES** または **ThinLinux** をクリックします。
 3. **導入設定** をクリックします。
 4. [**このアイテムを設定**] をクリックします。
 5. 次のオプションを設定します。
 - **すべての通知を有効化/無効化** - このオプションを無効にすると、すべてのオプションおよび通知が無効になります。
 - **設定アップデート通知** - このオプションを無効にすると、設定アップデートダイアログボックスがデバイスに表示されません。
 - **アプリケーション アップデート通知** - このオプションを無効にすると、アプリケーション ポリシーの導入時にユーザー通知が表示されません。
 - **イメージ アップデート通知** - このオプションを無効にすると、イメージ ポリシーの導入時にユーザー通知が表示されません。
 - **ログオフ通知** - このオプションを無効にすると、ユーザーがデバイスからログオフするためのユーザー通知が表示されません。
 - **再起動通知** - このオプションを無効にすると、デバイスの再起動設定の導入時にユーザー通知が表示されません。
 - **ディスプレイ ロック画面** - このオプションを無効にすると、アプリケーションおよびイメージのアップデート中にロック画面が表示されません。
-  **メモ:** すべてのオプションがデフォルトで有効に設定されています。
6. [**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。


ThinLinux デバイスの導入設定の構成

Wyse Management Suite 3.1 からは、ThinLinux デバイスの導入設定を構成することができます。デバイスに構成をサイレント導入するように設定することができます。

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 **ThinLinux** をクリックします。
3. **導入設定** をクリックします。
4. [**このアイテムを設定**] をクリックします。
5. 次のオプションのいずれかを設定します。
 - **すべての通知を有効化/無効化** - このオプションを無効にすると、すべてのオプションおよび通知が無効になります。
 - **設定アップデート通知** - このオプションを無効にすると、設定アップデートダイアログボックスがデバイスに表示されません。

- **アプリケーション アップデート通知** - このオプションを無効にすると、アプリケーション ポリシーの導入時にユーザー通知が表示されません。
- **イメージ アップデート通知** - このオプションを無効にすると、イメージ ポリシーの導入時にユーザー通知が表示されません。
- **ログオフ通知** - このオプションを無効にすると、ユーザーがデバイスからログオフするためのユーザー通知が表示されません。
- **再起動通知** - このオプションを無効にすると、デバイスの再起動設定の導入時にユーザー通知が表示されません。
- **ディスプレイ ロック画面** - このオプションを無効にすると、アプリケーションおよびイメージのアップデート中にロック画面が表示されません。

 **メモ:** すべてのオプションがデフォルトで有効に設定されています。

6. [**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。


Dell Hybrid Client 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。
- Dell Hybrid 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、[**Hybrid Client**] をクリックします。
[**設定コントロール | Hybrid Client**] 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。
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、設定をクリックし、必要に応じてオプションを設定します。
6. [**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。

次の表は、[**設定コントロール | Hybrid Client**] ウィンドウで設定できる機能セットの一覧です。

表 5. Hybrid Client ポリシー設定

特長	サブ機能 — ユーザー ポリシー グループ	サブ機能 — デバイス ポリシー グループ
周辺機器の管理	ディスプレイ 設定	ディスプレイ 設定
	プリンター	プリンター
	オーディオ	オーディオ
	マウス	マウス
	キーボード	キーボード
ネットワークの構成	ワイヤレス	ワイヤレス
		プロキシ
		Bluetooth
ブラウザの設定	Google Chrome の設定	ブラウザのショートカット
	Firefox の設定	
	ブラウザのショートカット	
	デフォルト ブラウザー	
地域と言語の設定	地域	地域
		タイム サーバー
		言語
カスタマイズ	デスクトップ	デスクトップ
		デバイス情報
サインオン	適用なし	ドメイン参加
		以前にログインしたユーザーのリスト
プライバシーとセキュリティ	適用なし	証明書
		ゲスト ユーザー アカウントのプロパティ
		USB ロック ダウン
		GRUB パスワード
		Bremen パスワード
		VNC サーバ
		SSH サーバー
電源設定	省電力	省電力
	サスペンドおよび電源ボタン	サスペンドおよび電源ボタン
Citrix Workspace	Citrix ブローカ セッション	Citrix ブローカ セッション
	Citrix グローバル設定	Citrix グローバル設定
VMware ViewClient	VMware ViewClient ブローカ セッション	VMware ViewClient ブローカ セッション
	VMware グローバル設定	VMware グローバル設定
RDP	RDP ブローカ セッション	RDP ブローカ セッション
Dell Hybrid Client モード	Dell Hybrid Client モード	Dell Hybrid Client モード
WMS 設定	適用なし	WMS クライアント設定
		導入設定

表 5. Hybrid Client ポリシー設定（続き）

特長	サブ機能 — ユーザー ポリシー グループ	サブ機能 — デバイス ポリシー グループ
アプリケーション セキュリティ	VLC Media Player	VLC Media Player
	イメージ ビューア	イメージ ビューア
	Libre Office	Libre Office
ネットワーク ドライブ	ネットワーク ドライブ リスト	ネットワーク ドライブ リスト
BIOS	適用なし	お使いのプラットフォームを選択します： <ul style="list-style-type: none"> ● DHC 5070 ● DHC 7070

メモ: 壁紙、証明書、広告ロゴファイルなどのリソース ファイル名に特殊文字を使用したり、スペースを追加したりしないでください。

Dell Hybrid Client を設定する方法の詳細については、www.dell.com/support にある『Dell Hybrid Client 管理者ガイド』を参照してください。

Dell Hybrid Client 向け Wyse Management Suite クライアント設定の設定

管理者は、Dell Hybrid Client の設定について、Wyse Management Suite エージェントの動作を設定できます。また、管理者は、営業時間外に構成を適用するようにデバイスを設定できます。

手順

- [**グループ & 設定**] ページに移動して、グループを選択します。
- [**ポリシーの編集**] ドロップダウン メニューから、[**Hybrid Client**] をクリックします。
[**設定コントロール | Hybrid Client**] ウィンドウが表示されます。
- [**Standard**] オプションをクリックします。
- [**WMS 設定**] > [**WMS クライアント設定**] の順に移動します。
- デバイス グループの営業時間および営業日を設定するには、[**営業時間**] フィールドで [**行の追加**] をクリックして、[**営業日**] ドロップダウン メニューから曜日をクリックします。
- エージェントによるユーザーセッションのレポート作成を有効にするには、[**セッションのレポート作成の有効化**] オプションを有効にして、[**セッションのレポート作成**] ドロップダウン メニューからタイミングを選択します。利用できるオプションは次のとおりです。
 - [**ユーザーセッションを実行時に送信**] — ユーザーがデバイスからログオフするたびに、Dell Client Agent からユーザーセッションレポートが送信されます。
 - [**ユーザーセッションをチェックイン時に送信**] - Dell Client Agent は、8 時間ごとにユーザーセッションレポートを送信します。
 - [**ユーザーセッションを営業時間外に送信**] - Dell Client Agent は、手順 5 で設定された営業時間外にユーザーセッションレポートを送信します。
- ユーザーレベルの設定に基づいてデバイスに設定を導入するには、[**ユーザー個人設定のローミングの有効化**] オプションを有効にします。このオプションが有効な場合、デバイス上でユーザーによって構成された設定は、Wyse Management Suite サーバーに保存され、ユーザーが別のデバイスにログインすると、設定が自動的に適用されます。設定された設定は、他のすべての設定よりも優先されます。
- デバイスでの通知を有効にするには、[**プッシュ通知の有効化**] オプションを有効にします。このオプションが有効な場合、[**保存して公開**] をクリックするとすぐに設定された設定が適用されます。このオプションを無効にすると、デバイスがハートビート信号を送信したときに設定が適用されます。

メモ: このオプションを無効にすると、Wyse Management Suite が Dell Hybrid Client にプッシュ通知を送信しないため、アプリケーションの導入がエラー状態になる場合があります。
- 指定された営業時間外に設定を適用するには、ドロップダウン メニューからオプションを選択します。利用できるオプションは次のとおりです。
 - [**即時**] - このオプションを選択すると、[**保存して公開**] をクリックした直後に設定が適用されます。
 - **指定された営業時間外** - このオプションを選択すると、手順 5 で設定された営業時間外に設定が適用されます。

- [一定期間ユーザーがデバイスにログオンしていない場合] - このオプションを選択すると、定義された時間内にデバイスにログインしたユーザーがないときに設定が適用されます。デバイスに設定が適用されるまでのアイドル時間を指定できません。
- ① メモ:** また、[デバイス] ページから、特定のデバイスに対してこれらの設定を行うこともできます。詳細については、「[デバイス レベル ポリシーの設定](#)」を参照してください。

Dell Hybrid Client デバイスの導入設定の構成

Wyse Management Suite 3.1 からは、Dell Hybrid Client デバイスの導入設定を構成することができます。デバイスに構成をサイレント導入するように設定することができます。

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、[Hybrid Client] をクリックします。
3. **WMS 設定 > 導入設定**の順に移動します。
4. 次のオプションを選択します。
 - **設定アップデート通知** - このオプションを無効にすると、設定アップデート ダイアログ ボックスがデバイスに表示されません。
 - **アプリケーション アップデート通知** - このオプションを無効にすると、アプリケーション ポリシーの導入時にユーザー通知が表示されません。
 - **イメージ アップデート通知** - このオプションを無効にすると、イメージ ポリシーの導入時にユーザー通知が表示されません。
 - **ログオフ通知** - このオプションを無効にすると、ユーザーがデバイスからログオフするためのユーザー通知が表示されません。
 - **再起動通知** - このオプションを無効にすると、デバイスの再起動設定の導入時にユーザー通知が表示されません。
 - **ディスプレイ ロック画面** - このオプションを無効にすると、アプリケーションおよびイメージのアップデート中にロック画面が表示されません。

① メモ: すべてのオプションおよび通知を有効化する場合、**すべての通知を有効化/無効化**オプションを有効にします。

① メモ: **設定アップデート通知**と**ディスプレイ ロック画面**は、デフォルトで無効になっています。
5. [保存して公開] をクリックします。

一括デバイス例外ファイルの作成とインポート

Wyse Management Suite 3.1 からは、複数の ThinOS 9.x デバイスにデバイス例外設定を導入することができます。

手順

1. 一括デバイス例外ファイルを作成します。ファイルを作成するには、次のいずれかを実行します。
 - テスト グループのグループ ポリシーを作成し、そのポリシーをファイルにエクスポートします。構成にパスワードが含まれている場合、エクスポートされたファイルでは「*」に置き換えられます。たとえば、次のとおりです。

```
{
  "WMSVersion": "4.6.8",
  "exportedDate": "1581466633677",
  "deviceTypes": [
    {
      "type": 6,
      "configurations": {
        "version": "0.0.1",
        "sequence": 1581466506281,
        "parameters": {
          "AdminModeUsername": {
            "value": "admin",
            "updatedAt": "1581466506234"
          },
          "AdminModePassword": {
            "value": "*****",

```

```

        "updatedAt": "1581466506234"
      },
      "TerminalName": {
        "value": "outpatient",
        "updatedAt": "1581466506234"
      },
      "TimeServer": {
        "value": "10.10.10.10",
        "updatedAt": "1581466506234"
      },
      "timeZone": {
        "value": "America/Phoenix",
        "updatedAt": "1581466506234"
      },
      "TerminalNameCapital": {
        "value": "yes",
        "updatedAt": "1581466506234"
      },
      "DeviceNICDefault": {
        "value": "Wlan",
        "updatedAt": "1581466506234"
      },
      "AdminMode": {
        "value": "yes",
        "updatedAt": "1581466506234"
      }
    }
  }
}
]
}

```

- 次の形式を使用して.json ファイルを作成します。

```

{
  "devices": {
    <serialnumber>: {
      "parameters": {
        "<parametername>": {
          "value": <value>
        },
        "<parametername>": {
          "value": <value>
        }
      },
      configurations: [<configuration name>]
    }
  },
  "configurations": {
    <configurationName>: {
      "<parametername>": {
        "value": <value>
      },
      "<parametername>": {

```

```

    "value": <value>
  }
}
}
}

```

たとえば、次のとおりです。

```

{
  "devices": {
    "9EPDL900051": {
      "parameters": {
        "TerminalName": {
          "value" : "Cubical 5 - Floor 3"
        },
        "TerminalNameCapital": {
          "value": "no"
        }
      },
      "configurations": ["westWingExceptions"]
    },
    "5LGDO600108": {
      "parameters": {
        "TerminalName": {
          "value" : "Cubical 15 - Floor 2"
        },
        "TerminalNameCapital": {
          "value": "no"
        }
      },
      "configurations": ["westWingExceptions"]
    }
  },
  "configurations": {
    "westWingExceptions": {
      "DeviceNICDefault": {
        "value": "Wlan"
      },
      "timeZone": {
        "value": "America/Phoenix"
      },
      "TimeServer": {
        "value": "10.10.10.10"
      },
      "TerminalNameCapital": {
        "value": "yes"
      },
      "AdminMode": {
        "value": "yes"
      },
      "AdminModeUsername": {
        "value": "admin"
      },
      "AdminModePassword": {
        "value": "password"
      }
    }
  }
}

```

2. ファイルを圧縮して暗号化します。

i **メモ:** 7-zip ソフトウェアを使用して、ファイルを圧縮および暗号化できます。

i **メモ:** ファイルのサイズは 1MB を超えることはできません。

3. **グループと設定**に移動して、**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。

4. **デバイスの一括例外**を選択します。
5. **参照**をクリックして、パスワードで暗号化された.zip ファイルを選択します。
6. [**次へ**] をクリックします。
[**インポートするデバイス タイプの設定の選択**] ページが表示されます。
7. [**次へ**] をクリックします。
 - ① **メモ:** ThinOS 9.x デバイスのデバイス例外ファイルを一括インポートすることができるため、ページ内のオプションを設定することはできません。
8. .json ファイルの圧縮に使用した.zip ファイルのパスワードを入力します。
9. [**次へ**] をクリックします。
デバイスの一括例外のインポートの概要が表示されます。
10. [**インポート**] をクリックします。
設定がインポートされると、レポート生成リンクが [**グループと設定**] ページに生成され、ダウンロードできるようになります。
成功メッセージが [**グループと設定**] ページに表示されます。
 - ① **メモ:** デバイスが未登録で設定がインポートされると、デバイスが次の 30 日以内にプリロードされたシリアル番号デバイスのいずれかに登録された場合にのみ、例外が適用されます。
 - ① **メモ:** デバイスがすでに登録済みで、デバイスのシリアル番号を使用して設定をインポートした場合、デバイス例外はデバイスに適用されます。
 - ① **メモ:** インポートされたファイルはパスワードで保護されています。AES-256 および ZipCrypto 暗号化がサポートされています。
 - ① **メモ:** 証明書、壁紙、ロゴなど、それらのリソースが関連付けられた構成はインポートされません。

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ーと、各パラメーター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ーを設定できます。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。

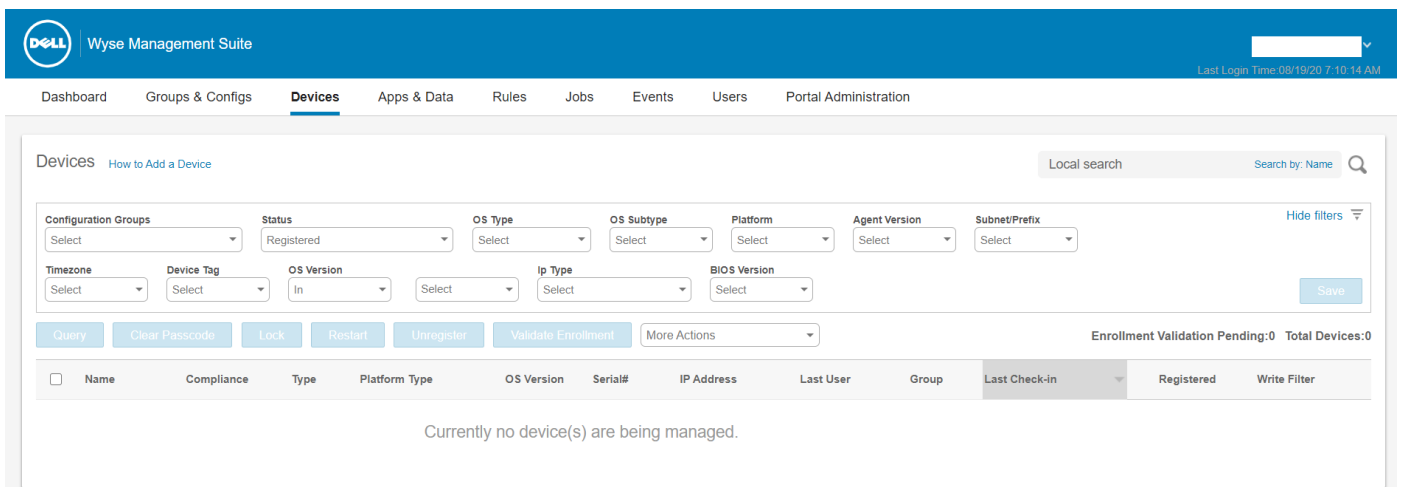


図 6. [デバイス] ページ

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
- 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
- Wake On LAN コマンド
- デバイスの詳細の表示
- ディスプレイ パラメーターの表示
- 仮想 NIC の詳細の表示
- BIOS 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
- リモートシャド接続の有効化
- Dell Hybrid Client デバイスのリモート シャド接続の設定
- 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
- Dell Hybrid Client の再イメージ化
- Dell Hybrid Client 向け設定ユーザー インターフェイス パッケージの取得
- Dell Hybrid Client の工場出荷時設定へのリセット

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ーフェイ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。


Dell Hybrid Client の手動登録

前提条件

デバイスを登録する前に、お使いのデバイスに Wyse Management Suite サーバーへのネットワーク接続があることを確認してください。

 **メモ:** デバイスの登録または登録解除は、ゲスト ユーザー アカウントからのみ行うことができます。

手順

1. Dell Hybrid Client にゲスト ユーザーとしてログインします。デフォルトでは、ユーザー名は **guest** です。
2. 最上部のバーで、 をクリックします。

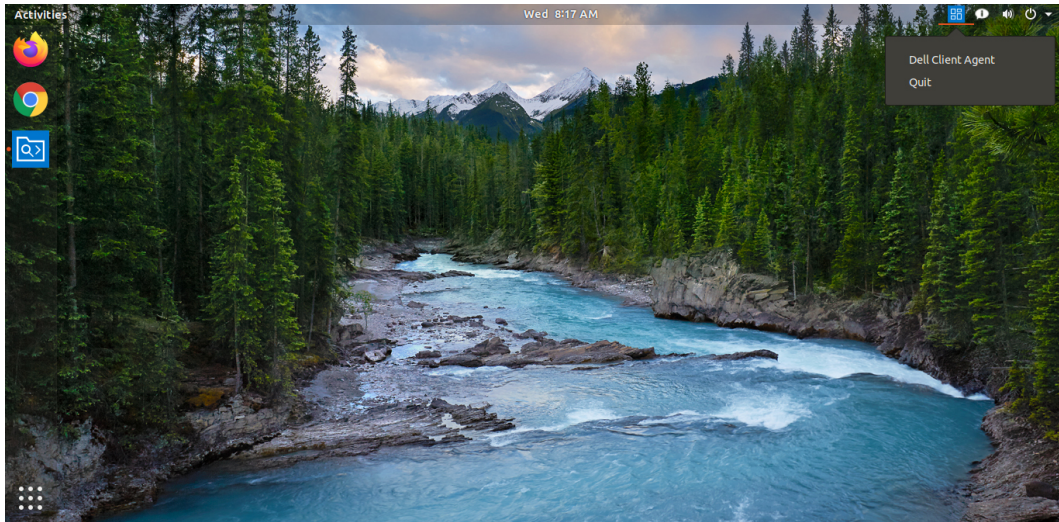


図 7. Dell Client Agent アイコン

3. [**Dell Client Agent**] をクリックします。
[**Dell Client Agent**] ウィンドウが表示されます。
4. [**登録**] をクリックします。
デフォルト ステータスは、[**検出進行中**] と表示されます。
5. 手動で登録するには、[**キャンセル**] ボタンをクリックします。
6. [**WMS サーバー**] フィールドに、Wyse Management Suite サーバーの URL を入力します。
7. [**グループのトークン**] フィールドで、グループの登録キーを入力します。グループ トークンは、デバイスをグループに直接登録するための固有のキーです。
メモ: [**テナント**] フィールドと [**グループ**] フィールドが空の場合は、デバイスは管理対象外グループに登録されます。ただし、グループトークンは、パブリック クラウドにデバイスを登録するために必須です。
8. [**オン/オフ**] ボタンをクリックして、[**サーバー証明書 CA の検証**] オプションを有効または無効にします。このオプションを有効にすると、すべてのデバイスとサーバー間の通信についてサーバー証明書の検証が実行されます。
CA 検証オプションは自動的に有効になり、パブリック クラウドの URL が入力された場合は無効にすることはできません。
9. [**登録**] をクリックして、Wyse Management Suite サーバーにデバイスを登録します。
デバイスが正常に登録されると、ステータスが [**登録済み**] として表示され、[**登録ステータス**] ラベルの横に緑色のチェックマークが表示されます。[**登録**] ボタンのキャプションが [**登録解除**] に変わります。

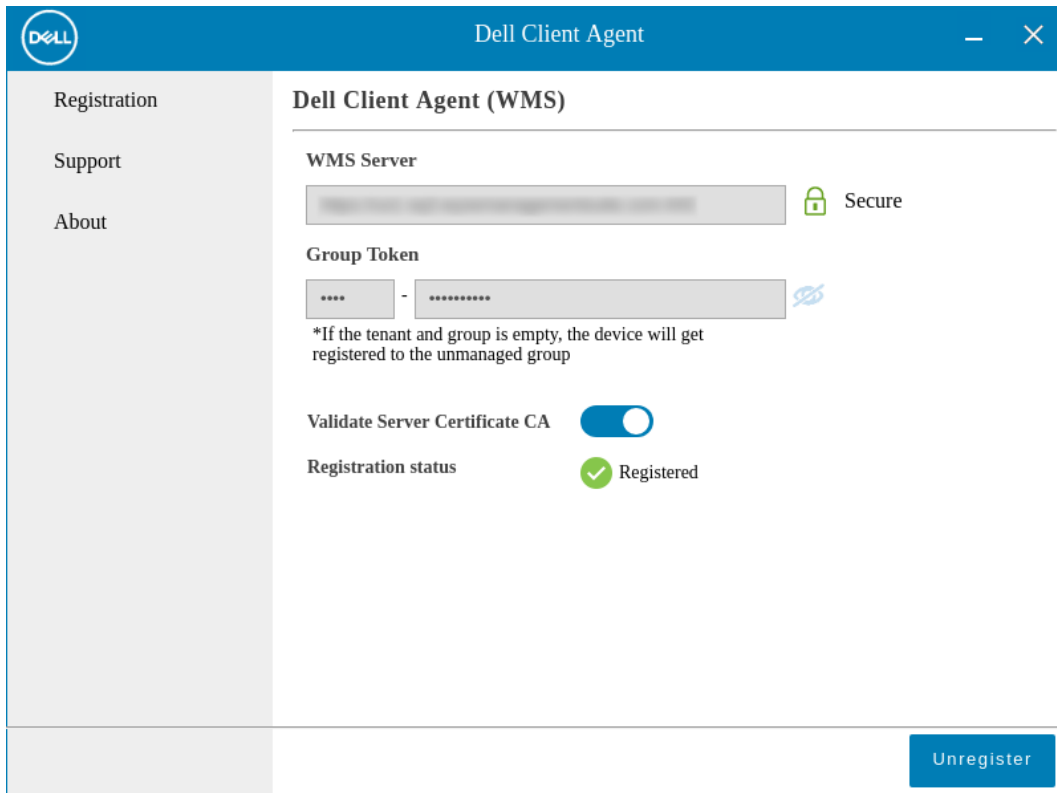


図 8. Dell Client Agent

手動検出方法を使用した Dell Hybrid Client の登録

手動検出方法を使用して、Dell Client Agent Enabler エージェントにより、Ubuntu バージョン 18.04 LTS 64 ビットを実行している OptiPlex 7070 Ultra デバイスを Wyse Management Suite に登録することができます。

手順

1. 次のテンプレートを使用して reg.json ファイルを作成します。

```
{ "ccm":
  { "ccmserver": "WMSserverURL.Domain.com", "ccmport": "443", "usessl": "true", "mqttserver": "
WMSserverURL.Domain.com
", "mqttport": "1883", "grouptoken": "GroupToken", "isCaValidationOn": "false" } }
```

2. reg.json ファイルを /etc/dcae/config にコピーします。
3. デバイスを再起動します。

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。

i **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。

i **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。
i **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。
i **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。
i **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

- wlx.ini ファイルを wyse\wllx フォルダに配置します。
- 設定に移動し、ThinLinux Thin Client で admin に切り替えます。
- [管理] > [INI] の順に移動します。
- FTP サーバの URL を入力します。
- [保存] をクリックして、Thin Client を再起動します。
- [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 6. 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
<p>名前 - WMS</p> <p>データタイプ - 文字列</p> <p>コード - 165</p> <p>説明 - WMS サーバ FQDN</p>	<p>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 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。</p> <p>① メモ: サーバの URL で https://FQDN や FQDN:443 を使用しないでください。使用すると、シンクライアントが Wyse Management Suite に登録されません。</p>
<p>名前 - MQTT</p> <p>データタイプ - 文字列</p> <p>コード - 166</p> <p>説明 - MQTT サーバ</p>	<p>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。</p> <p>デバイスを Wyse Management Suite のパブリッククラウドに登録するには、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。</p> <p>US1 : us1-pns.wysemanagementsuite.com EU1 : eu1-pns.wysemanagementsuite.com</p> <p>以前のバージョンの ThinOS および Windows 組み込みデバイスに Wyse Device Agent の詳細を設定する場合は、MQTT サーバの詳細を入力する必要があります。MQTT は、シンクライアントに通知する必要がある WMS のコンポーネントです。URL (MQTT の詳細があるおよびない) は、Wyse Management Suite のパブリッククラウド環境の許可リストに追加する必要があります。</p> <p>① メモ: MQTT URL を使用して Wyse Management Suite にログインすることはできません。</p>
<p>名前 - CA 検証</p> <p>データタイプ - 文字列</p> <p>コード - 167</p> <p>説明 - 認証局の検証</p>	<p>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。</p> <p>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。</p> <p>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。</p>
<p>名前 - GroupToken</p> <p>データタイプ - 文字列</p> <p>コード - 199</p> <p>説明 - グループトークン</p>	<p>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。</p> <p>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。</p>

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 サーバー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 7. 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 - <code>_WMS_MGMT</code> レコード FQDN - <code>_WMS_MGMT._tcp.<ドメイン名></code> レコードタイプ - SRV	このレコードは、Wyse Management Suite サーバー URL をポイントします。たとえば、 <code>wmserver.acme.com</code> であれば、 <code>wmserver.acme.com</code> は、Wyse Management Suite がインストールされているサーバーの完全修飾ドメイン名です。 メモ: サーバーの URL で <code>https://FQDN</code> や <code>FQDN:443</code> を使用しないでください。使用すると、シンクライアントが Wyse Management Suite に登録されません。
レコード名 - <code>_WMS_MQTT</code> レコード FQDN - <code>_WMS_MQTT._tcp.<ドメイン名></code> 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ー (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 サーバー上の MQTT サービスに向けられます。例： <code>wmservername.domain.com:1883</code> 。 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) サーバー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。 <code>US1 - us1-pns.wysemanagementsuite.com</code> <code>EU1 - eu1-pns.wysemanagementsuite.com</code> 以前のバージョンの ThinOS および Windows 組み込みデバイスに Wyse Device Agent の詳細を設定する場合は、MQTT サーバーの詳細を入力する必要があります。MQTT は、シンクライアントに通知する必要がある WMS のコンポーネントです。URL (MQTT の詳細があるおよびない) は、Wyse Management Suite のパブリッククラウド環境の許可リストに追加する必要があります。 メモ: MQTT URL を使用して Wyse Management Suite にログインすることはできません。
レコード名 - <code>_WMS_GROUPTOKEN</code> レコード FQDN - <code>_WMS_GROUPTOKEN._tcp.<ドメイン名></code> 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。

表 7. DNS SRV レコードの使用によるデバイスの設定 (続き)

URL/ タグ	説明
	<p>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。</p> <p>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。</p>
<p>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</p>	<p>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せん。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。</p> <p>クライアントと Wyse Management Suite サーバー間の 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。</p> <p>クライアントと Wyse Management Suite サーバー間の 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。</p> <p>メモ: CA 検証は、最新バージョンの Wyse Management Suite では任意です。</p>

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

- **Hybrid Client**

- Hybrid 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、オペレーティング システム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/プレフィックス**] 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。
11. [**IP タイプ**] ドロップダウン リストから、IP タイプを選択します。
12. [**BIOS バージョン**] ドロップダウン リストから、BIOS のバージョンを選択します。

[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。このオプションは、ThinOS オペレーティング システムが稼働するシンクライアントに適用できます。

前提条件

デバイスが VDI 接続に接続され、ユーザーはそのデバイスにログインしている必要があります。

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。

① 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。

① 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。

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。

Wake On LAN コマンド

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。

ディスプレイパラメーターの表示

Wyse Management Suite 3.1 以降では、Windows Embedded および ThinLinux オペレーティングシステムを実行しているデバイスのディスプレイ設定を表示することができます。ディスプレイセットアップのベンダー名、モデル番号、シリアル番号、解像度、アスペクト比、モード、位置合わせ、ローテーションの詳細を表示することができます。

手順

1. デバイス ページに移動します。
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** > **周辺機器** の順に移動します。
ディスプレイセットアップの詳細を表示できます。

▼ Peripherals							
Monitor							
Vendor	Model	Serial Number	Resolution	Aspect Ratio	Rotation	Mode	Alignment
DELL	UP3017	216L	2560x1600	16:10	normal	Span	3840,0
DELL	P2415Q	J0V0B(Primary)	3840x2160	16:9	normal	Span	0,0
DELL	P2415Q	V0D4L	3840x2160	16:9	normal	Span	6400,0
DELL	UP3017	211L	2560x1600	16:10	normal	Span	10240,0
DELL	P2415Q	YRB	0x0	0:0	normal	Span	12800,0
DELL	P2415Q	D5L	0x0	0:0	normal	Span	12800,0

図 9. ディスプレイ パラメーター

仮想 NIC の詳細の表示

Wyse Management Suite 3.1 以降では、Windows Embedded および ThinLinux オペレーティングシステムを実行しているデバイスのネットワークアダプターの詳細を表示することができます。ネットワークアダプターの名前、MAC アドレス、IP アドレス、ゲートウェイ IP アドレス、DNS サーバーの詳細を確認できます。

手順

1. デバイスページに移動します。
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 > ネットワークの詳細 - ネットワーク アダプターの順に移動します。
[ネットワークの詳細 - ネットワーク アダプター] セクションでは仮想 NIC の詳細を確認できます。

▼ Network Details – Network Adapters					
Adapter Name	MAC Address	IP Address	IPV6 Address	Gateway IP Address	DNS Server
eth0	E8:B0	10.150.		10.150.	10.150., 10.150.
eth1	E8:B0	10.150.		10.150.	10.150., 10.150.

図 10. ネットワークの詳細 - ネットワーク アダプター

BIOS の詳細の表示

Wyse Management Suite 3.1 からは、[デバイスの詳細] ページで BIOS パラメーター値を表示することができます。

手順

1. デバイスページに移動します。
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。[システム情報] タブの [BIOS 設定] セクションで、BIOS の詳細を表示することができます。

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。

- 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。
- 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

- デバイス ページで、該当デバイスをクリックします。
- 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。
- 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。

- 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。


- 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 シャドール接続の有効化


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

- デバイス ページで、該当デバイスをクリックします。
- その他のオプション ドロップダウンリストから、**リモートシャドール (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、**リモートシャドール (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。

- ターゲット Thin Client のポート番号を変更します (オプション)。
- 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ルセッションをサポートします。

Dell Hybrid Client デバイスのリモート シャドー接続の設定

このページを使用して、グローバル管理者およびグループ管理者が、Dell Hybrid Client デバイスのセッションにリモートでアクセスできるようにします。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. 標準または詳細アプリケーション ポリシーを使用して Wyse Management Suite から VNC アドオン パッケージを導入する - 「[アプリケーション ポリシー](#)」を参照してください。
アドオンがインストールされ、デバイスが再起動します。
2. Wyse Management Suite から VNC サーバー オプションを設定して導入します。VNC サーバー オプションを設定するには、次の手順を実行します。
 - a. [**グループ & 設定**] ページに移動して、グループを選択します。
 - b. [**ポリシーの編集**] ドロップダウン メニューから、[**Hybrid Client**] をクリックします。
[**設定コントロール | Hybrid Client**] ウィンドウが表示されます。
 - c. **標準**または**詳細設定** オプションをクリックします。
 - d. **プライバシーとセキュリティ > VNC サーバー**の順に移動して、オプションを設定します。
 - e. [**保存して公開**] をクリックします。

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。
- ローカル リポジトリを使用している場合は、サーバーが実行されている仮想マシンに、プルを実行して Wyse Management Suite に必要なサービスを実行するのに十分なメモリーがあることを確認してください。

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。

i **メモ:** このオプションは、Windows Embedded Standard デバイ스에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。

i **メモ:** デバイス ログは Hostname-timestamp 形式です。ログファイルは、Dell Hybrid Client、Linux、ThinLinux では .tar 形式でアップロードされます。Windows と ThinOS 9.x システムでは .zip 形式でアップロードされます。

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 上で稼働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 上で稼働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

Dell Hybrid Client の再イメージ化

コマンドを送信して、Dell Hybrid Client を再イメージ化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. [その他のアクション] ドロップダウン メニューから、[再イメージ化] をクリックします。
[アラート] ウィンドウが表示されます。
5. コマンドの送信 をクリックします。
このアクションにより、デバイスのリカバリー イメージ機能が実行されます。

Dell Hybrid Client 向け設定ユーザー インターフェイス パッケージの取得

Dell Hybrid Client の設定スキーマのバージョンが Wyse Management Suite サーバーに存在するバージョンよりも新しい場合は、最新の設定ユーザー インターフェイス パッケージを取得できます。

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. 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。
4. [追加アクション] ドロップダウン メニューから、[設定 UI パッケージの取得] 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。

Dell Hybrid Client の工場出荷時設定へのリセット

コマンドを送信して、Dell Hybrid Client を工場出荷時設定にリセットできます。

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. Dell Hybrid Client 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。

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。

シンクライアント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。

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 インベントリの設定
- Wyse Software Thin Client のアプリケーション インベントリの設定
- 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、%systemdrive%\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、%systemdrive%\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、デバイスがさらにもう 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、失敗と見なされません。

- 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。[**リポジトリ名**]列には、アプリケーションが存在するリポジトリの数が表示されます。列の上にカーソルを置くと、リポジトリの名前を表示できます。また、リポジトリ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ーのインターフェイ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で使用可能な場合、リポジトリの数がファイル名の横に表示されます。

メモ: Wyse Management Suite 3.1 からは、ThinLinux デバイスにアプリケーションをインストールするためのスクリプトを追加することができます。ThinLinux のスクリプトに有効なシバンがあるかどうかを確認する必要があります。

- 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。
 - [**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、選択したグループまたはデバイスに属するデバイス、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。このオプションを選択すると、グループに登録されるすべての新しいデバイスにポリシーが適用されます。グループに存在する既存のデバイス上でジョブを実行するには、ポリシーのスケジュールを設定する必要があります。ポリシーをスケジュールすると、ジョブのステータスには、グループにすでに存在しているデバイスの数が表示されます。新たに追加されて登録されているデバイスのジョブステータスは表示されません。
 - 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。このオプションを選択すると、グループ内にあるすべてのデバイスにポリシーが適用されます。グループに存在する既存のデバイス上ですぐにジョブを実行する、またはデバイスチェックイン前にスケジュールされた時刻にジョブを実行するには、ポリシーをスケジュールする必要があります。ポリシーをスケジュールすると、ジョブのステータスには、グループにすでに存在しているデバイスの数が表示されます。
- メモ:** Wyse Management Suite にチェックインされている、新たに追加されたデバイスのジョブステータスは表示されません。
- 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。

- 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 シンクライアント、Linux、Thin Linux デバイスにのみ適用されます。

- 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。
- 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。
- 次のオプションを任意に選択します。
 - 即時** - サーバー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。
- 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。
- [**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 シンクライアント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

- 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。
- [**アプリとデータ**] > [**アプリ インベントリ**] > [**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ーフェイスに表示されるまで約 2 分かかります。
- 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。
- ポリシー名** を入力します。
- [**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。
- [**タスク**] ドロップダウン リストから、タスクを選択します。
- [**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で使用可能な場合、リポジトリ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、選択したグループまたはデバイスに属するデバイス、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。このオプションを選択すると、グループに登録されるすべての新しいデバイスにポリシーが適用されます。グループに存在する既存のデバイス上でジョブを実行するには、ポリシーのスケジュールを設定する必要があります。ポリシーをスケジュールすると、ジョブのステータスには、グループにすでに存在しているデバイスの数が表示されます。新たに追加されて登録されているデバイスのジョブステータスは表示されません。
 - **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。このオプションを選択すると、グループ内にあるすべてのデバイスにポリシーが適用されます。グループに存在する既存のデバイス上ですぐにジョブを実行する、またはデバイス チェックイン前にスケジュールされた時刻にジョブを実行するには、ポリシーをスケジュールする必要があります。ポリシーをスケジュールすると、ジョブのステータスには、グループにすでに存在しているデバイスの数が表示されます。
- メモ:** Wyse Management Suite にチェックインされている、新たに追加されたデバイスのジョブステータスは表示されません。
- 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** - サーバー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)をシンクライアントにコピーします。
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フォルダーに保存します。
3. [アプリとデータ] > [アプリインベントリ] > [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。

メモ: Wyse Management Suite 3.1 からは、ThinLinux デバイスにアプリケーションをインストールするためのスクリプトを追加することができます。ThinLinux のスクリプトに有効なシバンがあるかどうかを確認する必要があります。

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で使用可能な場合、リポジトリ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、選択したグループまたはデバイスに属するデバイス、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。このオプションを選択すると、グループに登録されるすべての新しいデバイスにポリシーが適用されます。グループに存在する既存のデバイス上でジョブを実行するには、ポリシーのスケジュールを設定する必要があります。ポリシーをスケジュールすると、ジョブのステータスには、グループにすでに存在しているデバイスの数が表示されます。新たに追加されて登録されているデバイスのジョブステータスは表示されません。
 - **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。このオプションを選択すると、グループ内にあるすべてのデバイスにポリシーが適用されます。グループに存在する既存のデバイス上ですぐにジョブを実行する、またはデバイスチェックイン前にスケジュールされた時刻にジョブを実行するには、ポリシーをスケジュールする必要があります。ポリシーをスケジュールすると、ジョブのステータスには、グループにすでに存在しているデバイスの数が表示されます。

① **メモ:** Wyse Management Suite にチェックインされている、新たに追加されたデバイスのジョブステータスは表示されません。

① **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스에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。

① **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** - サーバー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または Wyse Management Suite リポジトリの softwareTcApps 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] > [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。
① **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で使用可能な場合、リポジトリ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、選択したグループまたはデバイスに属するデバイス、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。このオプションを選択すると、グループに登録されるすべての新しいデバイスにポリシーが適用されます。グループに存在する既存のデバイス上でジョブを実行するには、ポリシーのスケジュールを設定する必要があります。ポリシーをスケジュールすると、ジョブのステータスには、グループにすでに存在しているデバイスの数が表示されます。新たに追加されて登録されているデバイスのジョブステータスは表示されません。
 - **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。このオプションを選択すると、グループ内にあるすべてのデバイスにポリシーが適用されます。グループに存在する既存のデバイス上ですぐにジョブを実行する、またはデバイスチェックイン前にスケジュールされた時刻にジョブを実行するには、ポリシーをスケジュールする必要があります。ポリシーをスケジュールすると、ジョブのステータスには、グループにすでに存在しているデバイスの数が表示されます。

i **メモ:** Wyse Management Suite にチェックインされている、新たに追加されたデバイスのジョブステータスは表示されません。

i **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。

i **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** - サーバー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。

Dell Hybrid 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、**hybridClientApps** に移動して、アプリケーションをフォルダーにコピーします。

i **メモ:** デルの署名済みアプリケーションのみを Dell Hybrid Client に導入し、インストールすることができます。

2. [アプリとデータ] > [アプリ インベントリ] > [Hybrid 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] のインターフェイ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] > [Hybrid 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**] 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で使用可能な場合、リポジトリ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. [**インストール パラメーター**] フィールドに、選択したアプリケーションのインストール パラメーターを入力します。

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**] - 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、選択したグループまたはデバイスに属するデバイス、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。このオプションを選択すると、グループに登録されるすべての新しいデバイスにポリシーが適用されます。グループに存在する既存のデバイス上でジョブを実行するには、ポリシーのスケジュールを設定する必要があります。ポリシーをスケジュールすると、ジョブのステータスには、グループにすでに存在しているデバイスの数が表示されます。新たに追加されて登録されているデバイスのジョブステータスは表示されません。
- **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。このオプションを選択すると、グループ内にあるすべてのデバイスにポリシーが適用されます。グループに存在する既存のデバイス上ですぐにジョブを実行する、またはデバイスチェックイン前にスケジュールされた時刻にジョブを実行するには、ポリシーをスケジュールする必要があります。ポリシーをスケジュールすると、ジョブのステータスには、グループにすでに存在しているデバイスの数が表示されます。

メモ: Wyse Management Suite にチェックインされている、新たに追加されたデバイスのジョブステータスは表示されません。

13. **タイムアウト (1 ~ 999 分)** ボックスに、クライアントにメッセージダイアログボックスを表示する時間 (分) を指定します。タイムアウト では、クライアントにメッセージが表示され、インストール開始前に作業を保存する時間を提供します。

14. 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。

15. **保存** を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。

16. 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。

17. 次のオプションを任意に選択します。

- **即時** - サーバー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。

18. 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。

19. [**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。


Dell Hybrid 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インストール スクリプト (必要な場合) をシンクライアントにコピーします。


メモ: デルの署名済みアプリケーションとスクリプトのみを Dell Hybrid Client に導入し、インストールすることができます。

2. アプリケーションおよびインストール 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 hybridClientApps 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**] > [**Hybrid 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**] > [**Hybrid 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で使用可能な場合、リポジトリ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**] - 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、選択したグループまたはデバイスに属するデバイス、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。このオプションを選択すると、グループに登録されるすべての新しいデバイスにポリシーが適用されます。グループに存在する既存のデバイス上でジョブを実行するには、ポリシーのスケジュールを設定する必要があります。ポリシーをスケジュールすると、ジョブのステータスには、グループにすでに存在しているデバイスの数が表示されます。新たに追加されて登録されているデバイスのジョブステータスは表示されません。
 - **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。このオプションを選択すると、グループ内にあるすべてのデバイスにポリシーが適用されます。グループに存在する既存のデバイス上ですぐにジョブを実行する、またはデバイスチェックイン前にスケジュールされた時刻にジョブを実行するには、ポリシーをスケジュールする必要があります。ポリシーをスケジュールすると、ジョブのステータスには、グループにすでに存在しているデバイスの数が表示されます。

 **メモ:** Wyse Management Suite にチェックインされている、新たに追加されたデバイスのジョブステータスは表示されません。

19. **タイムアウト (1 ~ 999 分)** ボックスに、クライアントにメッセージダイアログボックスを表示する時間 (分) を指定します。タイムアウト では、クライアントにメッセージが表示され、インストール開始前に作業を保存する時間を提供します。
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。
21. **保存** を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. 次のオプションのいずれかを選択します。
 - **即時** - サーバー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への追加
- リポジトリへの ThinOS ファームウェアの追加
- リポジトリへの ThinOS パッケージ ファイルの追加
- リポジトリへの ThinOS BIOS ファイルの追加
- リポジトリへの 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
- Dell Hybrid Client 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 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**] > [**WES/ThinLinux**] の順に進みます。

リポジトリへの 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。

リポジトリへの 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 9.1 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。

リポジトリへの ThinOS アプリケーション パッケージの追加

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. [**アプリとデータ**] タブで、[**OS イメージ** リポジトリ] の [**ThinOS 9.x**] をクリックします。
3. [**パッケージ ファイルの追加**] をクリックします。
パッケージ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。
 - EULA がパッケージに組み込まれている場合は、パッケージの EULA の詳細とベンダーの名前が表示されます。ベンダー名をクリックして、各ベンダーのライセンス契約を読むことができます。**承諾** をクリックしてパッケージをアップロードします。同じベンダーの EULA の詳細を表示したくない場合は、**今後表示しない** を選択できます。パッケージのライセンス契約には個別に同意する必要があります。**拒否** をクリックすると、パッケージはアップロードされません。
 - EULA がパッケージに組み込まれていない場合、手順 5 に進みます。
5. **アップロード** をクリックします。

Dell Hybrid Client イメージ ポリシーの作成





Windows 10 IoT Enterprise、ThinLinux 2.x、ThinOS 8.x オペレーティングシステムを実行している Wyse 5070 シンクライアントを Dell Hybrid Client デバイスに変換するための、Dell Hybrid Client イメージポリシーを作成することができます。

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、**Hybrid Client** をクリックします。

2. ポリシーの追加 をクリックします。
3. [Hybrid Client 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、このバージョンを強制を選択します。
 - 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。


4. 保存 をクリックします。

-  **メモ:** DHC ライセンスの数は Dell Hybrid Client に変換される Wyse 5070 シンクライアントの数以上でなければなりません。
-  **メモ:** 圧縮または exe 形式で提供された DHC 変換 OS イメージを \repository\osImages\zipped フォルダにコピーする必要があります。リポジトリの同期後に、DHC OS のイメージが **アプリとデータ > OS イメージ リポジトリ > Hybrid Client** に表示されます。
-  **メモ:** Windows Embedded、ThinLinux、ThinOS を実行している Wyse 5070 シンクライアントや PCoIP オペレーティングシステムを実行している ThinOS に DHC 変換イメージを展開するには、OS イメージポリシーを作成する必要があります。
-  **メモ:** Windows 10 IoT Enterprise および ThinLinux 2.x オペレーティングシステムを実行しているシンクライアントについては、merlin パッケージが 408 以降にアップデートされていることを確認してください。

ファイル リポジトリの管理

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 リポジトリのインベントリ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。

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

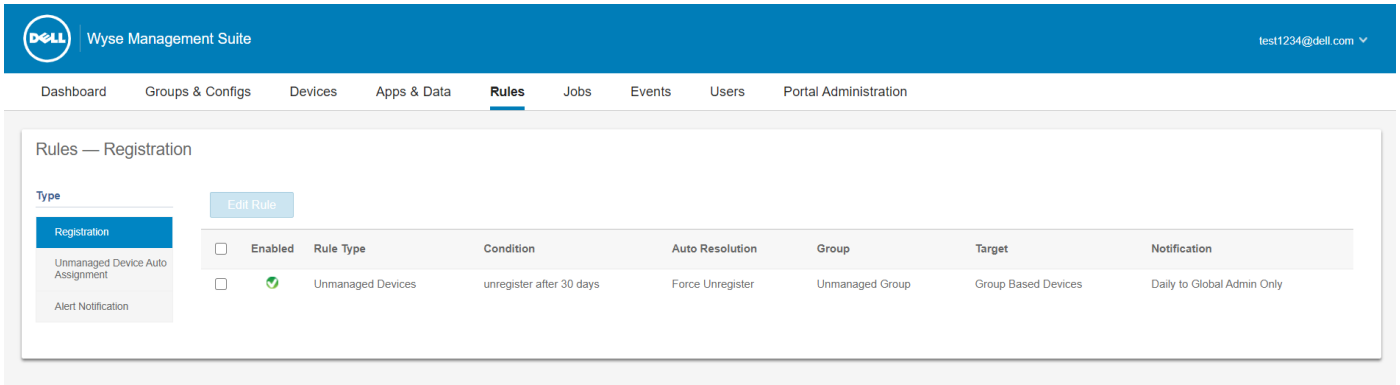


図 11. ルール ページ

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arget
 - 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。

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
 - Hybrid 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。

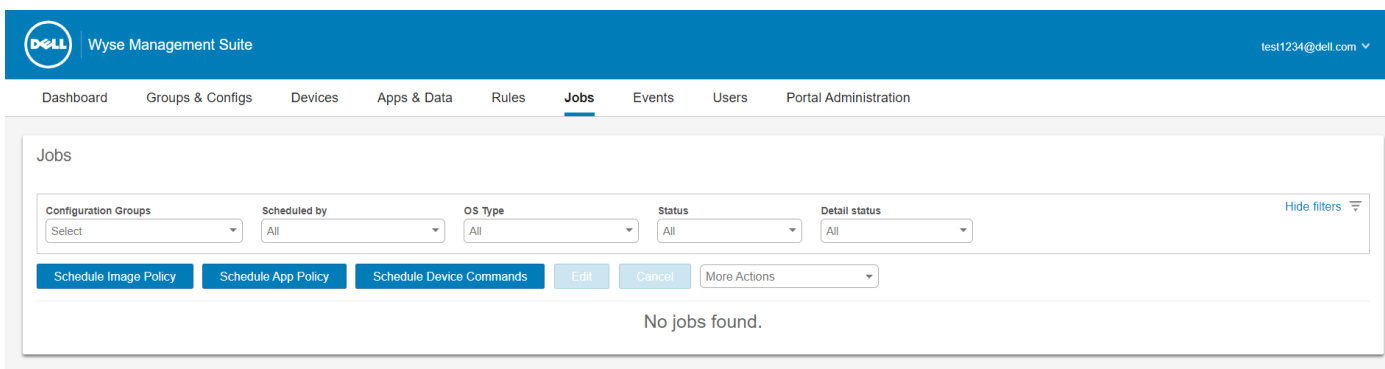


図 12. [ジョブ] ページ

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

- Dell Hybrid Client
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。

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。

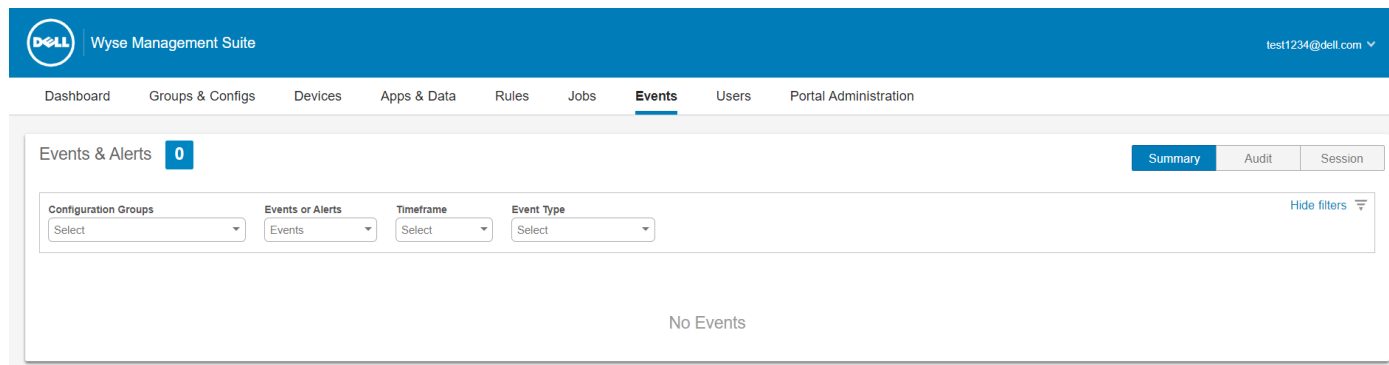


図 13. [イベント] ページ

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
- エンド ユーザー セッションのレポート作成

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。

エンド ユーザー セッションのレポート作成

エンド ユーザー セッションのレポート作成オプションを使用して、さまざまな時間間隔でユーザー セッションを報告することができます。

前提条件

[セッションのレポート作成の有効化] オプションを有効にする必要があります。詳細については、「[Dell Hybrid Client 向け Wyse Management Suite クライアント設定の設定](#)」を参照してください。

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. [セッション] をクリックします。
[エンド ユーザー セッション] ページが表示されます。
3. [時間枠] ドロップダウン メニューから、イベントを表示するオプションを選択します。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

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3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。

- ユーザーの追加
 - 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
- [**エンドユーザー**] - [**エンドユーザー**] タブを使用して、Wyse Management Suite に個々のユーザーを追加することができます。個々のユーザーに設定を構成して、導入することができます。設定はユーザーアカウントに適用され、ユーザーがログインしたときにシンクライアントに適用されます。このオプションは、ThinOS 9.x オペレーティングシステムが稼動するシンクライアントおよび Dell Hybrid Client にのみ適用できます。

- **メモ** : CSV ファイルからのみユーザーを一括でインポートできます。Active Directory からエンドユーザーを一括インポートすることはできません。

The screenshot shows the 'Users' management interface in the Wyse Management Suite. The page title is 'Users — Unassigned Admins / Cloud Connect Users'. There are navigation tabs for 'Dashboard', 'Groups & Configs', 'Devices', 'Apps & Data', 'Rules', 'Jobs', 'Events', 'Users', and 'Portal Administration'. The 'Users' tab is active. Below the navigation, there are buttons for 'Add User', 'Edit User', 'Activate User(s)', 'Deactivate User(s)', 'Delete User(s)', and 'Bulk Import'. A table lists users with columns for 'Name', 'Group', 'Created', and 'Active'. The table contains one entry: 'Default Device Policy Group' with a creation date of '07/09/20' and an 'Active' status of 'Yes'. On the left, there is a 'Type' filter menu with options for 'Administrator(s)', 'Unassigned Admins / Cloud Connect Users' (which is selected), and 'End Users'. A 'Local search' input field is also present.

図 14. [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

- Wyse Management Suite での WMS カスタム役割の作成
- 未割り当ての管理者またはクラウド接続ユーザーの一括インポート
- 管理者プロファイルの編集
- 管理者プロファイルのアクティブ化
- 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
- 管理者プロファイルのアンロック
- 管理者プロファイルの非アクティブ化
- 管理対象外デバイスの自動割り当てルールの作成
- エンドユーザーの追加
- エンドユーザーの編集
- エンドユーザーポリシーの設定
- エンドユーザーの一括インポート
- エンドユーザーの削除
- ユーザープロファイルの編集

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. Eメールに記載されているも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

① 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、カスタム パスワードを入力します。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。

Wyse Management Suite での WMS カスタム役割の作成

Wyse Management Suite 3.1 以降のバージョンを使用すると、グローバル管理者は、新しい管理者の役割を作成し、Wyse Management Suite のさまざまな機能に対してきめ細かい権限を付与することができます。カスタム グローバル管理者の役割を使用して、複数のユーザーを作成できます。

手順

1. ユーザータブに移動します。
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. E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. **役割** をクリックします。
6. **役割** ドロップダウン リストから、**カスタム WMS 役割** を選択します。
7. 各カテゴリの下で、ユーザーに実行を許可する適切な機能を選択します。
8. **保存** をクリックします。

次の表は、カスタム役割に割り当てることができる、サポート対象およびサポート対象外の権限の詳細を示しています。

表 8. カスタム役割の権限

対応	非対応
設定の編集または削除	一括デバイス例外
グループの追加、編集、削除	グループ管理者の作成
リファレンス ファイルのアップロード	グローバル管理者の作成
デバイス詳細例外の作成	ビューアー管理者の作成
ルール	割り当て解除された管理者への役割の割り当て
アプリとデータ	サブスクリプション (ライセンスのエクスポートおよびインポート)
エンド ユーザーの一括インポート	WMS サーバー URL の変更
リモート リポジトリの管理	MQTT URL の変更
Reports (レポート)	構成 UI のアップロード
その他	カスタム ブランド化
ポータル管理ページの Active Directory	


未割り当ての管理者またはクラウド接続ユーザーの一括インポート

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. インポートしたユーザーを割り当てる必要のあるユーザー グループを選択します。
6. **インポート** をクリックします。

管理者プロフィールの編集

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、カスタム パスワードを入力します。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。

管理者プロフィールのアクティブ化

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. アクティブ化するプロフィールを選択します。
4. **[管理者のアクティブ化]** をクリックします。

管理者プロフィールの非アクティブ化

管理者プロフィー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。

管理者プロフィールの削除

このタスクについて

プロフィールを削除するには、先に管理者を非アクティブ化しておく必要があります。管理者プロフィールを削除するには、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。

管理者プロフィールのアンロック

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. アンロックする管理者を選択します。
4. [管理者のアンロック] をクリックします。

管理者プロフィールの非アクティブ化

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. 非アクティブ化する管理者を選択します。
4. [管理者の非アクティブ化] 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。

エンドユーザーの追加

手順

1. [ユーザー] タブをクリックします。
2. [エンドユーザー] をクリックします。
3. [ユーザーの追加] をクリックします。
4. ユーザー名、ドメイン、姓、名、Eメール アドレス、役職、電話番号を入力します。
5. [保存] をクリックします。

エンドユーザーの編集

手順


1. [ユーザー] タブをクリックします。
2. [エンドユーザー] をクリックします。
3. [エンドユーザーの編集] をクリックします。
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. [保存] をクリックします。

エンドユーザーポリシーの設定

個々のユーザーに設定を構成して、導入することができます。設定はユーザーアカウントに適用され、ユーザーがログインしたときにシンクライアントに適用されます。このオプションは、ThinOS 9.x オペレーティングシステムが稼動するシンクライアントおよび Dell Hybrid Client にのみ適用できます。

手順

1. [ユーザー] タブをクリックします。
2. [エンドユーザー] をクリックします。
3. ユーザーを選択します。
[エンドユーザーの詳細] ページが表示されます。
4. [ポリシーの編集] ドロップダウンメニューをクリックして、オペレーティングシステムを選択します。
5. 必要なポリシーを設定し、[保存して公開] をクリックします。


 **メモ:** オンプレミス環境のユーザー数に制限はありません。パブリッククラウド環境では 10,000 ユーザーを追加することができます。

エンドユーザーの一括インポート

手順

1. [ユーザー] タブをクリックします。
2. [エンドユーザー] をクリックします。
3. [一括インポート] をクリックします。
4. [参照] をクリックして、.csv ファイルを選択します。
5. .csv ファイルにヘッダーが含まれている場合は、[CSV ファイルにヘッダー行を含む] オプションを選択します。
6. [ユーザーグループの選択] ドロップダウンリストから、ユーザーを追加するユーザーグループを選択します。
7. [インポート] をクリックします。

 **メモ:** Wyse Management Suite には、ファイルごとに最大 100 のユーザーを追加することができ、.csv ファイルのファイルサイズは 150 KB を超えないようにする必要があります。

 **メモ:** パブリッククラウドには、最大 10,000 ユーザーを追加することができます。プライベートクラウドに追加できるユーザー数に制限はありません。

エンドユーザーの削除


手順

1. [エンドユーザー] タブをクリックします。
2. [エンドユーザーの削除] をクリックします。
アラートウィンドウが表示されます。削除の理由を入力して削除リンクを有効にします。

3. **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**] タブをクリックして、次の詳細情報を入力します。
 - 名
 - 姓
 - 役職
 - 携帯電話番号
 - [**役割**] タブをクリックして、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、カスタム パスワードを入力します。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。

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。

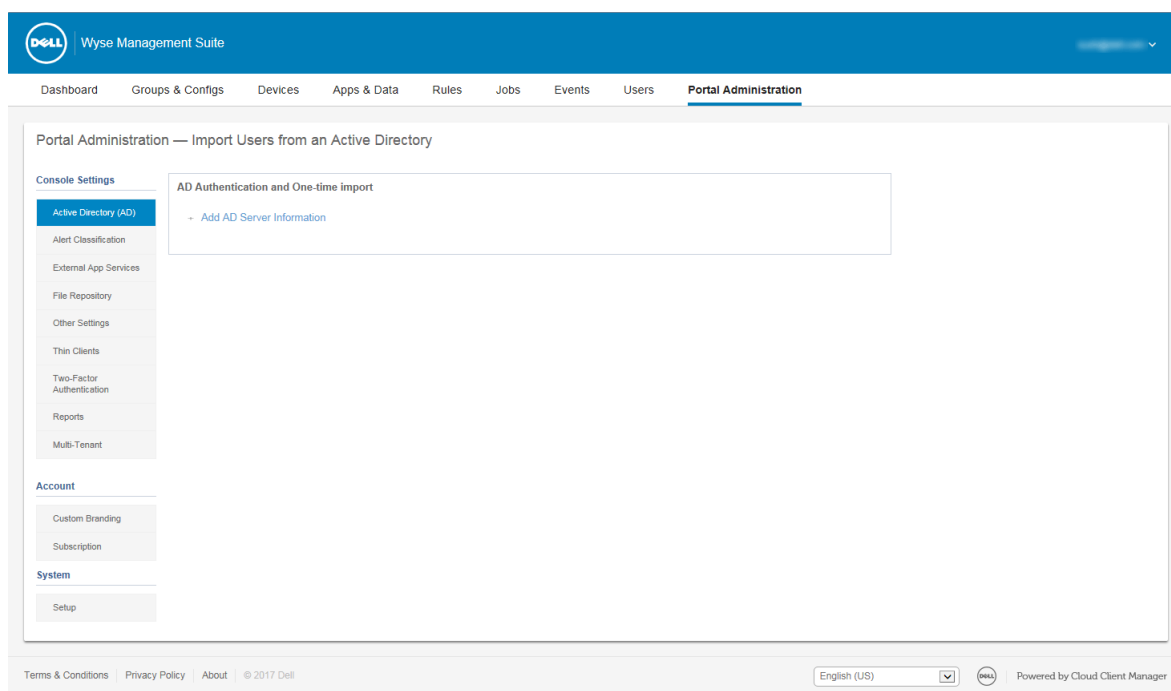


図 15. ポータル管理

トピック：

- Active Directory によるパブリック クラウドへの未割り当てのユーザーまたはユーザー グループのインポート
- Active Directory サーバ情報の追加
- 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

Active Directory によるパブリック クラウドへの未割り当てのユーザーまたはユーザー グループのインポート

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 を設定します。

Active Directory サーバ情報の追加

Active Directory ユーザーおよびユーザーグループを 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 サーバー名**、**ドメイン名**、**サーバー URL**、**ポート**などのサーバー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
 - ① **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ーを適用します。次のように値を入力します。
 - 「OU=<OU Name>」、たとえば、「OU=TestOU」
 - 「DC=<Child Domain>, DC=<Parent Domain>, DC=com,」、たとえば、「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. [ユーザー名コンテンツ] フィールドにユーザー名を入力します。
 13. [ユーザーのインポート] または [グループのインポート] をクリックします。
 - ① **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 ユーザーの数を含み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-0358EA52H8H" -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](https://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。

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ーフェイス (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** - 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**] の順に移動して、Wyse Management Suite リポジトリ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 リポジトリに追加されたファイルを他のリポジトリ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 リポジトリにレプリケートできます。

リポジトリ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。新しいリポジトリが登録されると、すべてのファイルが新しいリポジトリにコピーされます。[**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。

イメージ プル テンプレートは、他のリポジトリ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でのみサポートされています。

リモート リポジトリ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 リポジトリからローカル リポジトリ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 サーバからの CA 検証が無効になっている場合、サーバ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 リポジトリを最大 25 のサブネットまたは範囲に関連付けることができます。またリポジトリに関連付けられたサブネットに対して優先順位を設定できます。

Wyse Management Suite 2.1 のサブネット マッピングを使用して、BIOS パッケージを導入することができます。リモート リポジトリ、テナント クラウド リポジトリ、またはオペレーター クラウド リポジトリから、複数のファームウェア パッケージをアップロードして導入することができます。この機能は、Wyse Management Suite Pro ライセンスでのみ適用可能です。

メモ: Subnet Proximity は、ThinOS 9.x デバイスではサポートされていません。

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**] の順に移動します。

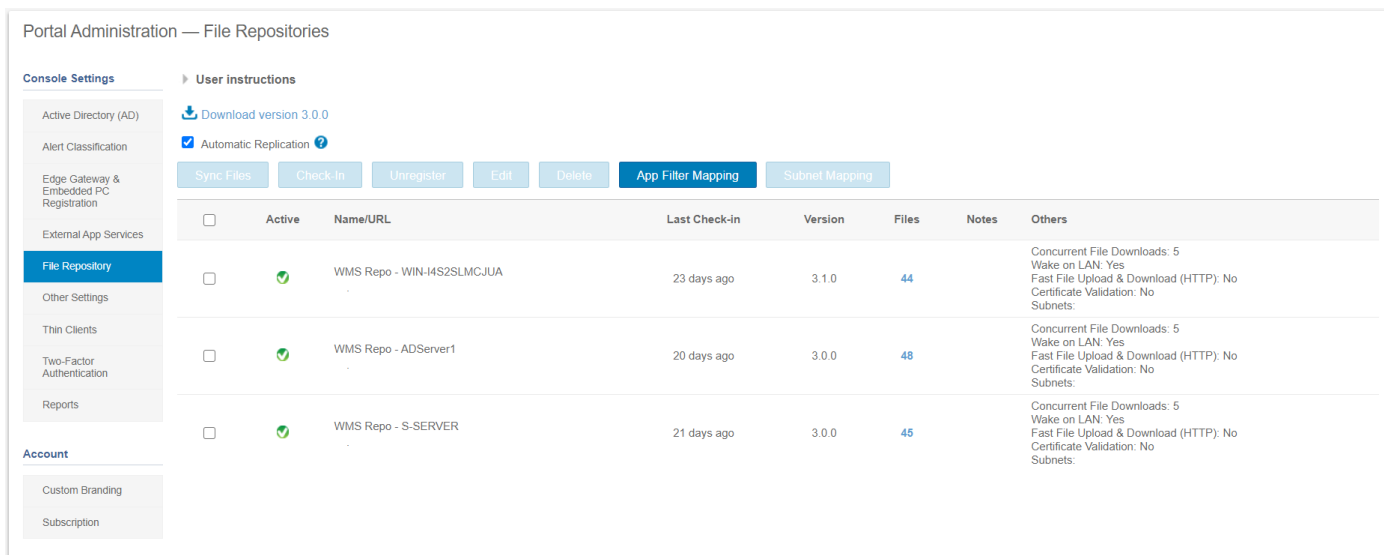


図 16. ファイル リポジトリ

2. ファイル リポジトリを選択します。
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。この機能は、ThinOS 9.x デバイスではサポートされていません。

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**、およびその他のセルフサービスの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 2.1 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ー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ー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。

i **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。

i **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。

Dell Wyse 5070 デバイスおよび Dell OptiPlex 7070 Ultra の Dell Hybrid Client への変換

Wyse Management Suite Pro 3.1以降のバージョンでは、Windows 10 IoT Enterprise LTSP、Windows 10 IoT Enterprise LTSC、ThinLinux 2.x、ThinOS 8.6 を実行している Dell Wyse 5070 デバイスを Dell Hybrid Client に変換することができます。また、Wyse Management Suite Pro 3.1以降のバージョンでは、Ubuntu 18.04 または Windows 10 を実行している Dell OptiPlex 7070 Ultra システムを Dell Hybrid Client に変換することもできます。

トピック：

- [Dell Wyse 5070 の変換](#)
- [Dell OptiPlex 7070 Ultra の変換](#)

Dell Wyse 5070 の変換

前提条件

- Windows 10 または ThinLinux 2.x のいずれかを実行している Wyse 5070 デバイスに 4.0.8 以降の最新の Boot Agent がない場合は、[Dell サポート サイト](#) からダウンロードします。
- ThinOS 8.6_511 を実行している Wyse 5070 デバイスに 4.0.8 以降の最新の Boot Agent がない場合は、[Dell サポート サイト](#) からダウンロードします。
- Windows 10 IoT Enterprise デバイスを変換する場合は、[Dell サポート サイト](#) から Dell Hybrid Client イメージ (DHC_Wyse_5070_Conversion_Merlin_Image_xxxx_32GB.exe) をダウンロードします。
- ThinLinux 2.x または ThinOS 8.6 デバイスを変換する場合は、[Dell サポート サイト](#) から Dell Hybrid Client イメージ (DHC_Wyse_5070_Conversion_Merlin_Image_xxxx_16GB.exe) をダウンロードします。
- Wyse Management Suite Pro 3.1 以降のバージョンを使用していることを確認します。
- Hybrid Client ライセンスの数が、Dell Hybrid Client に変換する必要があるデバイスの数以上であることを確認します。Dell Hybrid Client ライセンスは、Wyse Management Suite にインポートできます。
- パブリッククラウドに Wyse Management Suite が設定されていて、変換イメージをパブリッククラウドに登録する場合は、オンプレミスのリポジトリを設定して、ローカルに構成する必要があります。詳細については、「[リモートリポジトリ](#)」を参照してください。

このタスクについて

Windows 10 IoT Enterprise LTSP、Windows 10 IoT Enterprise LTSC、ThinLinux 2.x、ThinOS 8.6 を Dell Hybrid Client に変換するプロセスでは、既存のドライブの内容とパーティション構造が削除されます。この変換プロセスでは、Wyse Management Suite にデバイスを登録するために必要な証明書と設定のみが保存されます。他のすべてのデータ、証明書、構成設定は保存されません。Dell Hybrid Client に変換した後に、デバイスを元の状態に戻すことはできません。ただし、[Dell サポート サイト](#) から Dell Wyse USB イメージングツールを使用して、元のオペレーティングシステムを復元することはできます。既存のデータと設定は復元されません。

手順

1. Dell Hybrid Client イメージを Wyse Management Suite に登録します。登録方法の詳細については、「[Hybrid Client イメージのリポジトリへの追加](#)」を参照してください。
 - デバイスのストレージサイズが 16 GB を超える場合は、DHC_CONVERSION_5070.exe を使用します。
 - デバイスのストレージサイズが 16 GB の場合は、DHC_CONVERSION_5070_16GB.exe を使用します。
2. Dell Hybrid Client イメージポリシーを作成します。Hybrid Client イメージポリシーの作成方法の詳細については、「[Hybrid Client イメージポリシーの作成](#)」を参照してください。
3. デバイスを Dell Hybrid Client に変換します。イメージのスケジューリング設定方法の詳細については、「[イメージポリシーのスケジューリング](#)」を参照してください。
 - デバイスはイメージのアップデート通知を受け取ります。Boot Agent は、Wyse Management Suite リポジトリからイメージをダウンロードし、Dell リカバリーツールを内部でトリガーすることによって Dell Hybrid Client イメージをインストールします。イメージングが完了すると、デバイスで Dell Hybrid Client が起動されます。

- Dell クライアント エージェントは、デバイスを Dell Hybrid Client として Wyse Management Suite に登録します。
- Wyse Management Suite は、デバイスを Dell Hybrid Client デバイスとして管理します。

Dell Hybrid Client イメージのリポジトリへの追加

手順

1. Wyse Management Suite を使用して、Dell Hybrid Client 変換イメージをリポジトリの場所またはオペレーティングシステムのイメージフォルダーにコピーします。

メモ: イメージファイルは、まずローカルシステムにコピーしてから、Wyse Management Suite リポジトリの場所にコピーすることをお勧めします。Wyse Management Suite は、ファイルを圧縮フォルダーから解凍し、リポジトリの場所またはオペレーティングシステムのイメージフォルダーにアップロードします。

イメージがリポジトリに追加されます。

2. アプリとデータ、OS イメージリポジトリ、Hybrid Client の順に移動して、保存されたイメージを表示します。

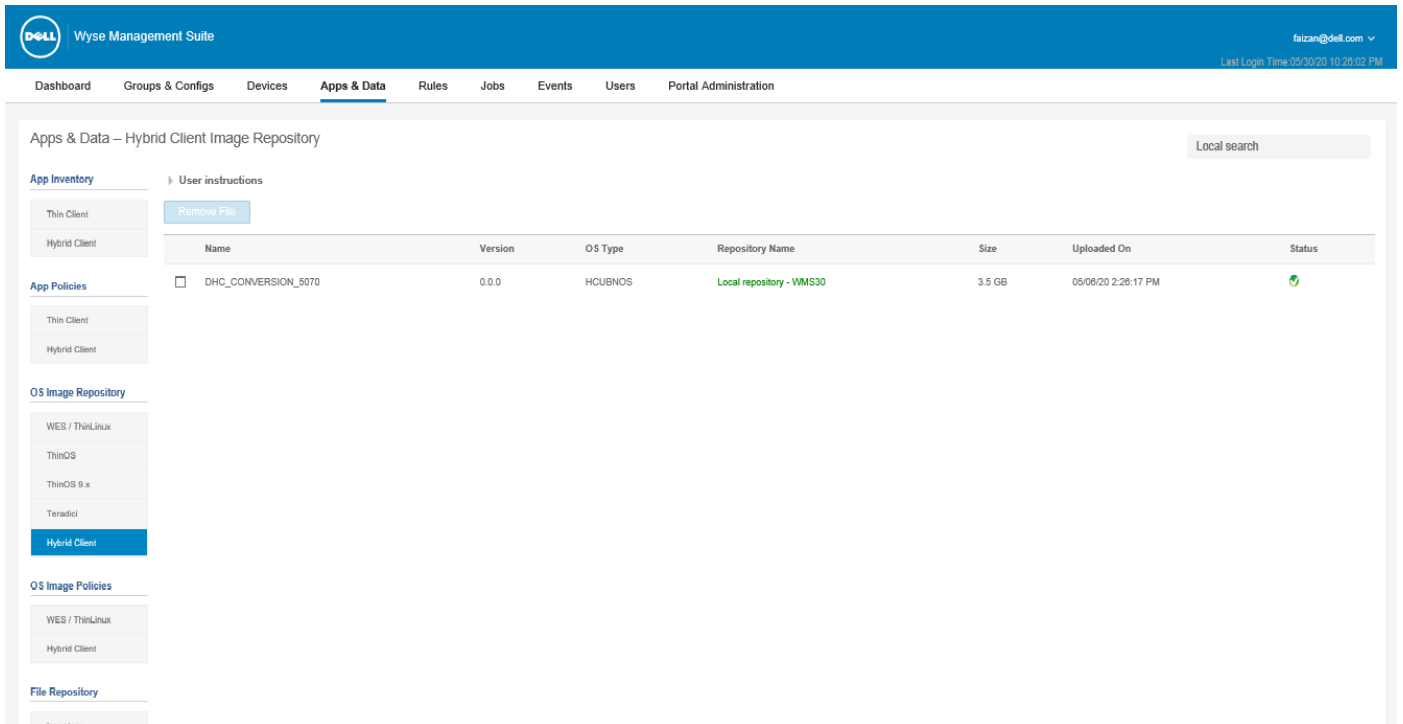


図 17. Dell Hybrid Client イメージのリポジトリへの追加

Hybrid Client イメージポリシーの作成

手順

1. アプリとデータに移動し、OS イメージポリシーの下の Hybrid Client をクリックします。
2. ポリシーの追加をクリックして、Hybrid Client ポリシーの編集タブに移動します。
3. ポリシー名を入力し、グループタブのドロップダウンメニューからグループを選択します。
4. OS タイプタブの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のタイプを選択します。
5. OS サブタイプフィルタータブの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のサブタイプフィルターを選択します。

メモ: 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ーまたはプラットフォームフィルターを選択します。

6. OS イメージタブのドロップダウンメニューからイメージファイルを選択します。

7. ルールタブのドロップダウンメニューから、[このバージョンを強制] を選択します。
8. ポリシーを自動的に適用タブの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。
9. 保存 をクリックします。

図 18. Hybrid Client イメージポリシーの作成

イメージポリシーのスケジュール

手順

1. ジョブに移動し、イメージポリシーのスケジュールタブをクリックします。
イメージアップデートジョブタブが表示されます。
2. ポリシータブのドロップダウンメニューからポリシーを選択します。
3. 説明タブで、ジョブの説明を入力します。
4. 実行タブのドロップダウンリストから、次のように日付または時刻を選択します。
 - 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。
5. プレビューをクリックし、スケジュールされたジョブの詳細を表示します。
6. スケジュールをクリックし、ジョブを開始します。

図 19. ジョブをスケジュールする


Dell OptiPlex 7070 Ultra の変換

前提条件

- Dell OptiPlex 7070 Ultra デバイスの Ubuntu 18.04 を Dell Hybrid Client に変換するには、DCA Enabler バージョン 1.1 または 1.0 が必要です。
- デバイスに DCA Enabler バージョン 1.0 がインストールされている場合は、1.1 にアップグレードする必要があります。DCA Enabler をアップグレードするには、デバイスを Wyse Management Suite 3.1 に登録し、Wyse Management Suite を使用して DCA_Enabler_Package 1.1.0-17 をデバイスにプッシュしてから DCA-Enabler 1.1.0-17 を導入する必要があります。

手順

1. DCA Enabler 1.1 を使用して Wyse Management Suite にデバイスを登録します。
2. OptiPlex 7070 Ultra デバイスを再イメージ化します。方法については、「[Dell Hybrid Client の再イメージ化](#)」を参照してください。Dell Hybrid Client パッケージを導入するアプリケーション ポリシーをスケジュールできます。詳細については、「[Dell Hybrid 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:** 標準アプリケーション ポリシーを Dell Hybrid Client デバイスに導入するには、最新の Dell Hybrid Client 1.1 または 1.0 のバンドルをローカルまたはリモートのリポジトリにアップロードする必要があります。

セキュリティ構成

このセクションでは、Wyse Management Suite の主なセキュリティ機能について説明し、データ保護と適切なアクセス制御を確実にするために必要な手順について説明します。

トピック：

- Wyse Management Suite インストーラーでの TLS バージョンの設定のサポート
- 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
- セキュア LDAP (LDAPS) セットアップの設定
- 廃止されたプロトコル

Wyse Management Suite インストーラーでの TLS バージョンの設定のサポート

Wyse Management Suite 3.0 以降では、Wyse Management Suite のインストール時またはアップグレード時に、TLS バージョンを選択するようにオンプレミスのインストーラーが改善されています。

メモ: TLS の推奨バージョンは 1.2 です。デバイス エージェントおよび merlin イメージに基づいて、TLS の適切なバージョンをすべて選択していることを確認してください。Windows Embedded システムの旧バージョン、Wyse デバイス エージェント (バージョン WDA_14.4.0.135_Unified)、32 ビットの merlin イメージ バージョンは TLSv1.0 とのみ互換性があります。また、インポート ツールは、TLSv1.0 とのみ互換性があります。

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

前提条件

- サーバーに Notepad++ またはそれに相当する任意のアプリケーションがインストールされている必要があります。
- サーバーに ADFS がインストールされている必要があります。

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. [**WMS の詳細を ADFS に提供**] セクションで、**WMS xml ファイルのダウンロード** をクリックします。CCM_SP_Metadata.xml ファイルがダウンロードされます。
3. ダウンロードしたファイルを右クリックして、**Notepad++** で **編集** を選択します。
4. ID 値をファイルからコピーします (例 : ccm-sq3)。
5. ADFS セットアップ コンソールに移動します。
6. **証明書利用者信頼** を右クリックして、**証明書利用者信頼の追加** を選択します。[**証明書利用者信頼の追加**] ウィンドウが表示されます。
7. [**スタート**] をクリックします。**データソースの選択** ウィンドウが表示されます。
8. **ファイルから証明書利用者に関するデータをインポート** オプションを選択し、ダウンロードした CCM_SP_Metadata.xml ファイルを参照します。c
9. [**次へ**] をクリックします。
10. **表示名** フィールドに ID 値 (ccm-sq3) を入力し、**次へ** をクリックします。
11. **アクセス制御ポリシーの選択** ページで、**次へ** をクリックします。
12. **信頼の追加の準備完了** ページで、**次へ** をクリックします。

13. **閉じる** をクリックします。
作成された証明書利用者信頼は、**証明書利用者信頼** コンソールにリストされます。
14. Wyse Management Suite パブリッククラウドサーバにログインします。
15. **ポータル管理 > Active Directory** の順に移動し、**WMS ルールの表示** をクリックします。
16. [**WMS ルール**] ウィンドウに表示されている内容をコピーします。
17. ADFS コンソールに移動し、証明書利用者信頼を右クリックして、**要求発行ポリシーの編集** を選択します。
18. [**発行変換ルール**] タブで、**ルールの追加** をクリックします。
19. **OK** をクリックします。
[**ルール テンプレートの選択**] ウィンドウが表示されます。
20. **要求ルール テンプレート** ドロップダウン リストから、**カスタム ルール** を使用して **要求を送信オプション** を選択し、**次へ** をクリックします。
21. **ルールの追加** をクリックします。
22. **要求ルール名** に入力し、手順 16 でコピーしたコンテンツを **カスタム ルール** フィールドに貼り付けます。
23. **終了** をクリックします。
24. **適用**、**OK** の順にクリックします。
25. **ポータル管理 > Active Directory** の順に移動して、**構成の追加** をクリックします。
26. シンクライアントに保存されている 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` にあります。
27. **設定のアップデート** をクリックします。
28. 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) 標準仕様に従いません。
29. 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。
30. ADFS 資格情報を入力し、**サインイン** をクリックします。
ADFS の設定後、**テストの成功** メッセージが表示されます。
31. リモート リポジトリの AD ドメイン 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。
32. **ユーザー** ページに移動し、インポートされた AD ドメイン ユーザーに役割を割り当てます。
33. Wyse Management Suite パブリック クラウド ポータルに移動し、**ドメイン 資格情報** を使用して **サインインリンク** をクリックします。
34. インポートした AD ドメイン ユーザーの E メール アドレスを入力し、**サインイン** をクリックします。
ADFS にログインした後、Wyse Management Suite サーバーにリダイレクトされます。

セキュア LDAP (LDAPS) セットアップの設定

Active Directory 証明書サービスのルート証明書を要求してセキュア LDAP (LDAPS) セットアップを設定するには、次の手順を実行します。

手順

1. Active Directory ドメイン サーバーに移動します。
2. **開始 > 実行** の順に移動します。
3. **mmc** と入力して **OK** をクリックします。
[**コンソール 1**] ウィンドウが表示されます。
4. **ファイル > スナップインの追加と削除** をクリックします。
5. ローカル システムに証明書を追加し、**OK** をクリックします。
6. 左パネルの **Personal** フォルダーを展開します。
7. 証明書を右クリックして、**すべてのタスク > 新しい証明書の要求** の順に移動します。
[**証明書登録**] ウィンドウが表示されます。
8. [**次へ**] をクリックします。
9. [**証明書登録ポリシーの選択**] タブで、**次へ** をクリックします。
10. **ドメイン コントローラー** を選択し、**次へ** をクリックします。
ドメイン証明書が、ドメイン コントローラーにインストールされます。
11. **終了** をクリックします。

ドメイン コントローラーに発行された証明書が、証明書ページに表示されます。

12. 証明書を右クリックして、デスクトップに証明書をエクスポートします。
13. Wyse Management Suite サーバーのセットアップで、AD ドメイン サーバー証明書を Wyse Management Suite java キー ストアに手動でインポートします。証明書をインポートするには、以下の手順を実行します。
 - a. Wyse Management Suite がインストールされているサーバーに移動します。
 - b. **コマンド プロンプト**を開き、<C:\Program Files\DELL\WMS\jdk-11.0.7\bin>keytool.exe> -importcert -alias <certificate name> -keystore "<C:\Program Files\Dell\WMS\jdk-11.0.7\lib\security\cacerts>" -storepass changeit -file "C:\<certificate name>コマンドを実行します。
14. 証明書がインストールされたら、Wyse Management Suite Tomcat サービスを再起動します。
15. Wyse Management Suite サーバーにログインします。
16. **ポータル管理 > Active Directory (AD)** の順に移動します。
17. **AD サーバー情報の追加**リンクをクリックします。
18. AD ドメイン名を入力します。
19. サーバー URL を **ldaps://hostname.domain.com** として入力します (例 : **ldaps://WMS-DC97.WMSAD97.com**)。
20. ポート名を **636** と入力します。
21. **保存** をクリックします。
22. [**インポート**] をクリックします。
23. ユーザー名とパスワードを入力します
24. **ログイン** をクリックします。
25. **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。
26. [**検索**] フィールドに選択するグループ名を入力します。
27. 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。
28. **ユーザー名**コンテンツフィールドにユーザー名を入力します。
29. [**ユーザーのインポート**] または [**グループのインポート**] をクリックします。
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 > 割り当て解除された管理者**にリストされます。

廃止されたプロトコル

Server Message Block (SMB) プロトコル バージョン 2.0 は廃止されています。

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](#)
- [CIFS のユースケースのシナリオ](#)

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いること。
- 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 9. 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 **サービスローケーション (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。
 - ① **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。
 - ① **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。

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](#) プライベート クラウドへのライセンスのエクスポート
- Thin Client のライセンス割り当て
- ライセンスの注文

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
 - Hybrid 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。
 - ① **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。
 - ① **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。
 - ① **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。

- ① **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。

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] ドロップダウン リストから、ファイル リポジトリを選択します。
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 リポジトリを使用している場合、XML ファイルはリポジトリで使用できません。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] > [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 以降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 10. 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	X10_wnos
Wyse 5070 Thin Client - Pentium プロセッサ	X10_wnos
Wyse 5070 Extended Thin Client - Pentium プロセッサ	X10_wnos
Wyse 5470 Thin Client	X10_wnos
Wyse 5470 All-in-One Thin Client	X10_wnos

リポジトリへの 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 9.1 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。
- Wyse Management Suite では、壁紙の設定は行わないでください。

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。

Wyse Management Suite を使用した 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

- シンクライアントに ThinOS v9.1.1036 イメージがインストールされていることを確認します。
- グループ トークンで Wyse Management Suite 内にグループを作成したことを確認します。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。
- シンクライアントが Wyse Management Suite に登録されていることを確認します。

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 アップデート**] 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。
パッケージの EULA の詳細とベンダーの名前が表示されます。
6. ベンダー名をクリックして、各ベンダーのライセンス契約を読み、**承諾** をクリックしてパッケージをアップロードします。
同じベンダーの EULA の詳細を表示したくない場合は、**今後表示しない** を選択できます。
メモ: 複数のパッケージをアップロードした場合、各パッケージの EULA の詳細が表示されます。パッケージのライセンス契約には個別に同意する必要があります。**拒否** をクリックすると、ファームウェアはアップロードされません。
7. [**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。
8. [**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せん。

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リイバのみが使用できます。

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。**ダウンロード バージョン x.x** をクリックして、WMS_Repo.exe ファイルをダウンロードします。
- 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ー要件は次のとおりです。
 - Windows 2012 R2 または Windows 2016 Server Standard
 - 4 CPU
 - 8 GB RAM
 - 40 GB ストレージ スペース

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. **管理者**としてログインし、WMS_Repo.exe をリポジトリサーバーにインストールします。
2. **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。
3. **[起動]** をクリックして、Web ブラウザーで **[WMS リポジトリ登録]** 画面を表示します。
4. 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。

Wyse Management Suite Repository

Registration

Register to Public WMS Management Portal

WMS Server

WMS Repository URL
 *

[Change Repository URL?](#)

Admin Name
 *


Admin Password
 *

Repository Location
 *

Version: 3.0.0-33

Register

図 20. パブリック クラウドでの登録

5. 次の詳細を入力します。
 - a. Wyse Management Suite サーバーの URL
 **メモ:** Wyse Management Suite バージョン 1.0 に登録しないと、MQTT Server URL を使用することはできません。
 - b. WMS リポジトリ URL (URL をドメイン名でアップデート)
 - c. Wyse Management Suite 管理者のログインユーザー名情報
 - d. Wyse Management Suite 管理者のログインパスワード情報
 - e. リポジトリパス情報
6. **登録** をクリックします。
7. 登録が成功すると、**登録** ウィンドウが表示されます。

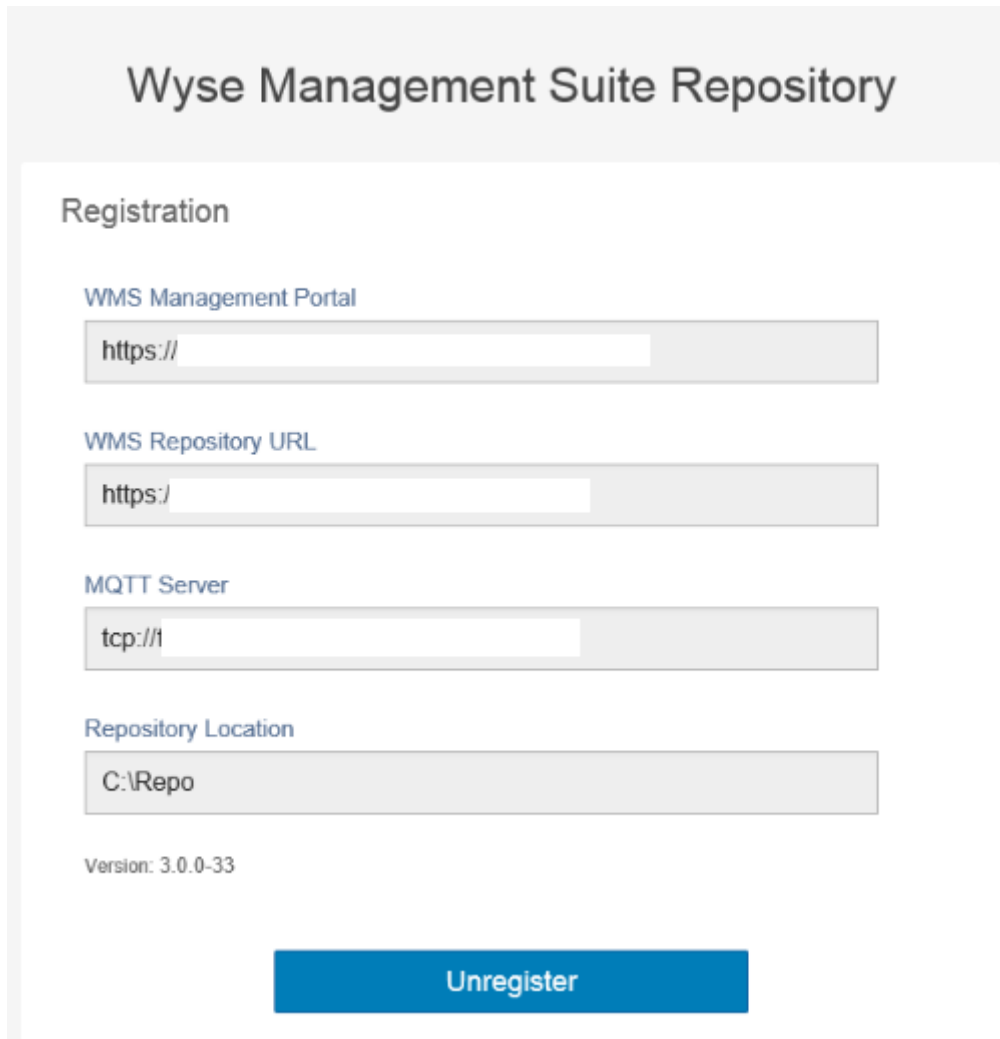


図 21. 登録に成功

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。

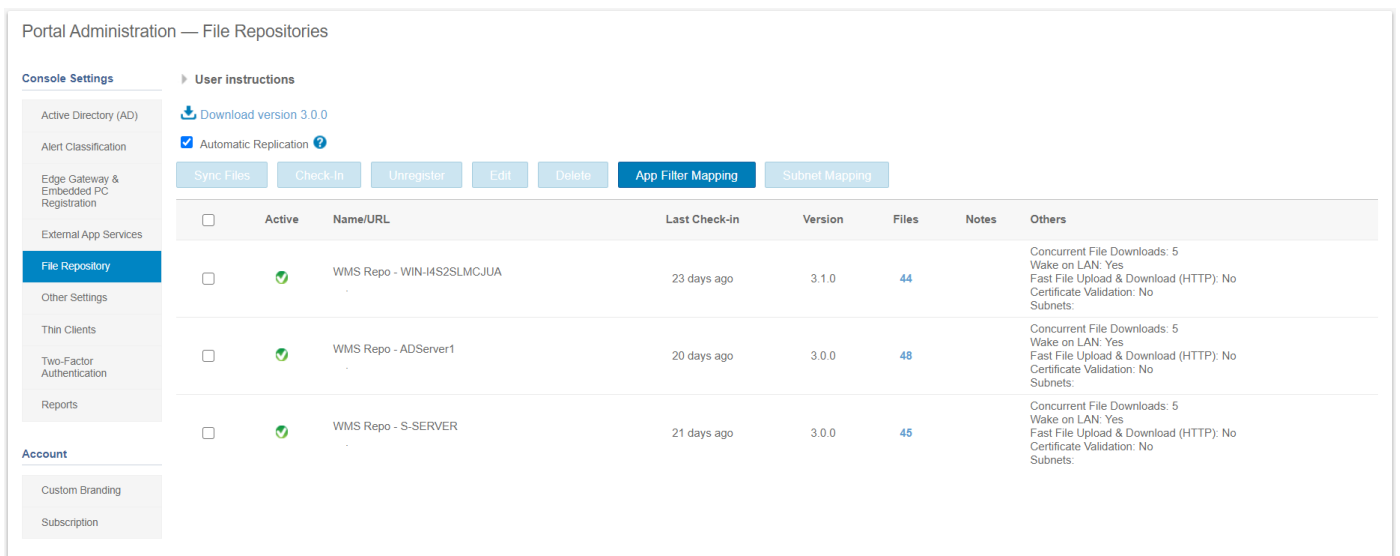


図 22. ポータルでの登録に成功

9. WMS_Repo.exe を使用すると、HTTPS が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。

▼ Server SSL Certificates: Enabled SSL Certificate Guide

Current Certificate

Issued to: [redacted].com
Issued from: [redacted].com
Valid to: August 18, 2118

PKCS-12 Key/Certificate Pair

Upload HTTPS PKCS-12 (.pfx, .p12). Apache intermediate certificate is needed for IIS pfx.

PKCS-12 file

Browse... *

Password for PKCS file

*

Intermediate certificate ⓘ

Browse...

図 23. 証明書のアップロード

10. サーバーが再起動し、アップロードされた証明書が表示されます。

Server SSL Certificates: Enabled SSL Certificate Guide

Current Certificate

Issued to: *.com
 Issued from: SHA256 CA - G3
 Valid to: June 7, 2018

PKCS-12 Key/Certificate Pair

Upload HTTPS PKCS-12 (.pfx, .p12). Apache intermediate certificate is needed for IIS pfx.

PKCS-12 file

Password for PKCS file

Intermediate certificate

図 24. 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 サーバーに証明書をアップロードして、Wyse Management Suite CA の認証情報を検証できます。

Trust Store Certificates

Trust store location:
 C:\Program Files\IDELL\WMSRepository\jdk1.8.0_152\jre\lib\security\cacerts

Uploaded Certificate Alias Names:
 None

Upload WMS Server certificate to trust store (CER format)

Certificate

図 25. トラストストア証明書

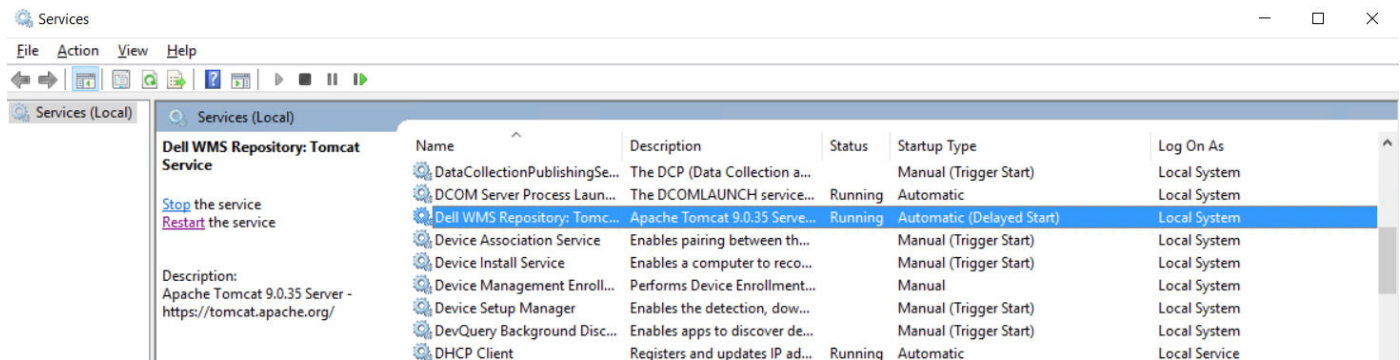
12. 登録時に入力した `C:\wmsrepo` に移動すると、すべてのリポジトリ ファイルが保存および管理されているフォルダーを表示することができます。

トピック：

- [Wyse Management Suite リポジトリサービスの管理](#)
- [Wyse Management Suite リモート リポジトリのプロキシ サポート](#)

Wyse Management Suite リポジトリサービスの管理

Wyse Management Suite リポジトリは、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するように設定されています。



Wyse Management Suite リモート リポジトリのプロキシサポート

Wyse Management Suite 3.1 以降のリモート リポジトリは、Wyse Management Suite に対するすべての HTTPS および MQTT 通信の SOCKS5 プロキシをサポートします。

リモート リポジトリは Windows サービスとして実行されるため、システム全体のプロキシのみがサポートされています。また、AD 認証または認証なしのプロキシのみがサポートされています。プロキシ サーバーは任意の方法を使用して構成できます。プロキシ サーバー情報を構成する方法については、次の例を参照してください。

- Netsh コマンドを使用 - 次のコマンドを使用してプロキシ サーバー情報を設定することができます。

```
netsh winhttp set proxy proxy-server="socks=localhost:9090" bypass-list="localhost"

C:\Users\administrator.WMSAD61>netsh winhttp set proxy proxy-server="socks=<proxy server IP>" bypass-list="localhost"

Current WinHTTP proxy settings:

Proxy Server(s) : socks=<proxy server IP>
Bypass List    : localhost
```

- DHCP で構成された WPAD ファイルを使用 - Wyse Management Suite リポジトリ サーバーを DHCP IP アドレスを使用して設定し、Internet Explorer を自動検出に設定する必要があります。WPAD.pac ファイルを使用して DHCP の 252 オプション タグを構成してください。PAC ファイルのコンテンツの例を次に示します。

```
function FindProxyForURL(url, host)
{
    if (shExpMatch(host, "*wysemanagementsuite.com*")) {
        return "SOCKS <proxy server IP>";
    }
    return "DIRECT";
}
```

グループ ポリシーを使用してプロキシ設定を構成することもできます。

- ① **メモ:** プロキシ設定は、リポジトリ サービスの開始時に読み取られます。プロキシ設定に後で変更を加えた場合は、リポジトリ サービスを再起動する必要があります。

- ① **メモ:** SOCKS4 プロキシを使用している場合、ホスト名の解決は設定されません。Wyse Management Suite リポジトリがインストールされているサーバー上のパブリック クラウド URL/ホスト名を解決するには、C:\Windows\System32\drivers\etcにあるホスト ファイルをアップデートする必要があります。SOCKS5 プロキシが使用されている場合、ホスト名はサーバーのネットワーク設定で構成された DNS を使用して解決されます。

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

トピック：

- [Wyse Management Suite を使用したログ ファイルの要求](#)
- [Wyse Management Suite を使用した監査ログの表示](#)
- [WinHTTP プロキシ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](#)
- [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](#)
- [Wyse Management Suite から設定された WiFi 設定が複数の Wyse 5070 Thin Client 間で固定されない](#)


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 プロキシ情報を取得します。

WinHTTP プロキシが設定されており、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。


① **メモ:** 波括弧は必須です。

Wyse Management Suite から設定された WiFi 設定が複数の Wyse 5070 Thin Client 間で固定されない

Wyse 5070 Thin Client で WiFi 接続を設定すると、パスワードを入力せずに、特定のワイヤレス ネットワーク (SSID) に接続されます。同じ設定が Wyse Management Suite にエクスポートされ、他の Wyse 5070 Thin Client に導入されると、その設定が適用され、同じワイヤレス ネットワークに接続するためのパスワードを入力するように求められます。WiFi 設定を固定するには、次の手順を実行します。

手順

1. Wyse 5070 Thin Client をワイヤレス ネットワークに接続します。
2. DWirelessProfileEditor.exe ファイルを実行します。
[**ワイヤレス プロファイル パスワード エディター**] ウィンドウが表示されます。
3. 宛先パスを参照して、プロファイルを xml ファイルとして保存し、[**保存**] をクリックします。

4. [ワイヤレス プロファイル パスワード エディター] ウィンドウで、[WiFi プロファイルのエクスポート] ボタンをクリックします。
5. [プロファイル] ドロップダウン リストから、設定を導入するプロファイルを選択します。
6. [パスワード] フィールドをクリアし、パスワードを再度入力します。
7. パスワードの**変更** をクリックします。
 **メモ:** [WiFi プロファイルのエクスポート] ボタンを再度クリックしないでください。
8. [ワイヤレス プロファイル パスワード エディター] ウィンドウを閉じます。
9. Wyse Management Suite にログインします。
10. [アプリとデータ] > [ファイル リポジトリ] > [インベントリー] の順に移動します。
11. **ファイルの追加** をクリックします。
12. xml ファイルを参照します。
13. [タイプ] ドロップダウン リストから、[Windows ワイヤレス プロファイル] を選択します。
14. 説明を入力します。
15. 現在の設定を上書きする場合は、[既存ファイルの上書き] オプションを選択します。
16. **アップロード** をクリックします。
17. [グループ & 設定] > [プロファイルの編集] > [WES] > [ネットワーク] の順に移動します。
18. [このアイテムを設定] をクリックします。
19. [Windows ワイヤレス プロファイル] ドロップダウン リストから、アップロードしたファイルを選択します。
20. [保存して公開] をクリックします。

FAQ (よくある質問)

トピック：

- 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 ファイル リポジトリの使用方法を教えてください
- .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？
- Wyse Management Suite のバージョンの確認方法
- DHCP オプション タグの作成方法と設定方法
- DNS SRV レコードを作成して設定する方法
- ホスト名を IP アドレスに変更する方法
- 自己署名リモート リポジトリを使用してデバイスをイメージングする方法

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] 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 サーバーに登録します。
4. リポジトリを 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

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. **サーバー マネージャー**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 サーバー 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
 - 166 MQTT サーバー 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 サーバー
- 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 検証サーバー 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 グループトークン サーバー 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 サーバーのサーバー 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_CAVVALIDATION
 - 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: mongod://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、またはパブリック クラウドのリモート リポジトリから実行できます。

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 リポジトリから、またはパブリック クラウドのリモート リポジトリから、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。