Dell Wyse Management Suite

Guide de l'administrateur version 3.2

Mars 2021
Rév. A00

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

PRÉCAUTION : ATTENTION vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : un AVERTISSEMENT signale un risque d'endommagement du matériel, de blessure corporelle, voire de décès.

Table des matières

1

Présentation de Wyse Management Suite

Wyse Management Suite est la solution de gestion de nouvelle génération qui vous permet de configurer, surveiller, gérer et optimiser de façon centralisée vos points de terminaison fonctionnant avec Dell Hybrid Client et les clients légers Dell. Elle offre également des fonctionnalités avancées, telles que le Cloud, ainsi que le déploiement sur site, une option de gestion depuis tout lieu à l'aide d'une application mobile et une sécurité optimisée, notamment grâce à la configuration du BIOS et au verrouillage des ports. D'autres fonctionnalités comprennent la découverte et l'enregistrement d'appareils, la gestion des ressources et de l'inventaire, la gestion de la configuration, le déploiement des systèmes d'exploitation et des applications, les commandes en temps réel, la surveillance, les alertes, les rapports et le dépannage des points de terminaison.

Sujets :

Éditions de Wyse Management Suite

Wyse Management Suite est disponible dans les éditions suivantes :

- **Standard (gratuite)** : l'édition Standard de la Wyse Management Suite offre des fonctionnalités de base et n'est disponible que pour un déploiement en Cloud privé. Vous n'avez pas besoin de clé de licence pour utiliser l'édition Standard. Cette version gère uniquement les clients légers Dell. L'édition Standard est adaptée aux petites et moyennes entreprises.
- **Pro (payante)** : l'édition Pro de Wyse Management Suite est une solution plus robuste. Disponible pour le déploiement de Cloud public et privé. Une clé de licence est obligatoire pour l'utilisation de l'édition Pro (licences par abonnement). Avec la solution Pro, les entreprises peuvent adopter un modèle hybride et bénéficient si nécessaire de licences flottantes entre les Clouds privés et publics. Cette version est requise pour gérer les appareils basés sur Teradici, les clients légers basés sur Wyse Covert for PC, les appareils Dell Hybrid Client, les PC embarqués et les appareils Edge Gateway. Offre également des fonctionnalités plus avancées pour gérer les clients légers Dell. Pour un déploiement dans le Cloud public, l'édition Pro peut être gérée sur les réseaux qui n'appartiennent pas à l'entreprise tels que bureau à domicile, tiers, partenaires, clients légers mobiles, etc.

  REMARQUE : Les licences peuvent être facilement basculées entre le Cloud et l'installation sur site.

  L'édition Pro de Wyse Management Suite fournit également :
  - Une application mobile pour afficher les alertes critiques et les notifications, et envoyer des commandes en temps réel.
  - Une sécurité renforcée grâce à l'identification à deux facteurs et à l'authentification Active Directory pour une administration basée sur les rôles.
  - Politique d'application avancée et création de rapports

  REMARQUE : Les services Cloud sont hébergés aux États-Unis et en Allemagne. Il se peut que les clients situés dans des pays soumis à des restrictions sur l'hébergement des données ne puissent pas tirer parti du service Cloud.

La console Web Wyse Management Suite prend en charge l'internationalisation. Dans le coin inférieur droit de la page, dans le menu déroulant, sélectionnez l'une des langues suivantes :

- Anglais
- Français
- Italien
- Allemand
- Espagnol
- Chinois
- Japonais

Matrice des fonctions Wyse Management Suite

Le tableau suivant fournit des informations sur les fonctionnalités prises en charge pour chaque type d'abonnement.

Tableau 1. Matrice des fonctionnalités pour chaque type d'abonnement

Fonctionnalités	Wyse Management Suite Standard	Wyse Management Suite Pro (Cloud privé)	Wyse Management Suite Pro (édition Cloud)
Solution hautement évolutive pour gérer les Thin Clients	Libérez jusqu'à 10 000 appareils	Jusqu'à 120 000 appareils	Jusqu'à 1 million de périphériques
Terme du contrat de licence	Téléchargement gratuit	Abonnement par poste	Abonnement par poste
Clé de licence	Non requis	Requis	Requis
Architecture	Cloud privé	Cloud privé	Cloud public
Déploiement flexible ou Cloud hybride	X	√	√
Programme d'installation avancée	X	√	√
Multitenancy	X	√	√
Administration déléguée pour la granularité des autorisations	X	√	√
Plusieurs référentiels pour prendre en charge votre architecture distribuée	X	√	√
Possibilité de configurer l'alias du serveur Wyse Management Suite	X	√	√
Architecture de référence haute disponibilité	X	√	X
Prise en charge du proxy : SOCKS5 et HTTPS	√	√	√
Prise en charge de l'API	X	√	X
Dell ProSupport pour les logiciels inclus	X	√	√
Points de terminaison Dell			
OptiPlex 7070 Ultra avec Dell Hybrid Client	X	√	√
OptiPlex 3090 Ultra et 7090 Ultra avec Dell Hybrid Client	X	√	√
Latitude 3320 avec Dell Hybrid Client	X	√	√
Wyse 5070 avec Dell Hybrid Client	X	√	√
Clients légers Wyse avec ThinOS	√	√	√
Clients légers Wyse avec ThinLinux	√	√	√
Clients légers Wyse avec Windows 10 IoT Enterprise	√	√	√
Wyse PCoIP zero clients (firmware Teradici)	X	√	√
Software thin clients avec Wyse Converter for PCs	X	√	√
Création de rapport et surveillance			
Console de gestion localisée	X	√	√
Journaux d'alertes, d'événements et d'audit par e-mail et application mobile	X	√	√

Tableau 1. Matrice des fonctionnalités pour chaque type d'abonnement

Fonctionnalités	Wyse Management Suite Standard	Wyse Management Suite Pro (Cloud privé)	Wyse Management Suite Pro (édition Cloud)
Création de rapports de niveau entreprise	X	√	√

Le tableau suivant fournit des informations sur les fonctionnalités de gestion de Dell Hybrid Client prises en charge pour chaque type d'abonnement.

Tableau 2. Matrice des fonctionnalités de gestion de Dell Hybrid Client

Fonctionnalités de gestion de Dell Hybrid Client	Wyse Management Suite Standard	Wyse Management Suite Pro (Cloud privé)	Wyse Management Suite Pro (édition Cloud)
Visibilité complète des actifs			
Découverte automatique des périphériques	X	√	√
Gestion des actifs, de l'inventaire et des systèmes	X	√	√
Affichage d'une configuration efficace au niveau des périphériques Wyse Management Suite après l'héritage	X	√	√
Sécurité			
Communication sécurisée (HTTPS)	X	√	√
MQTT sécurisé	X	√	√
L'authentication multifacteur ;	X	√	√
Authentification Active Directory pour l'administration basée sur les rôles	X	√	√
Mappage AD à l'aide de LDAPS	X	√	√
Authentification unique	X	√	√
Paramètres de verrouillage (activation/désactivation des ports des points de terminaison pris en charge)	X	√	√
Fonctionnalités complètes de gestion			
Gestion des correctifs et des images du système d'exploitation	X	√	√ *
Planification intelligente	X	√	√
Déploiement en mode silencieux	X	√	√
Regroupement des applications pour simplifier le déploiement et réduire les redémarrages	X	√	√
Création de groupes dynamiques et attribution en fonction des attributs des périphériques	X	√	√

Tableau 2. Matrice des fonctionnalités de gestion de Dell Hybrid Client

Fonctionnalités de gestion de Dell Hybrid Client	Wyse Management Suite Standard	Wyse Management Suite Pro (Cloud privé)	Wyse Management Suite Pro (édition Cloud)
Affectation du référentiel à la politique d'application et au mappage des sous-réseaux	X	√	√
Gestion avancée des applications et politique en matière d'applications	X	√	√
Héritage du groupe d'utilisateurs	X	√	√
Exception de l'utilisateur final	X	√	√
Annulation automatique de l'enregistrement des appareils	X	√	√
Configuration			
Configuration de l'Assistant Dell Hybrid Client	X	√	√
Prise en charge multi-écrans	X	√	√
Profil de suivi	X	√	√
Affiliation de fichiers pour prioriser le mode de livraison des applications	X	√	√
Paramètres du BIOS et support de configuration	X	√	√
Exportation ou importation des configurations de politique	X	√	√
Politique de groupe d'utilisateurs par défaut	X	√	√
Configuration du navigateur	X	√	√
Configurer le fournisseur de Cloud	X	√	√
Mise à jour automatique des applications signées par Dell	X	√	√
Itinérance des données de personnalisation des utilisateurs	X	√	√
Configurer VNC	X	√	√
Configurer SSH	X	√	√

REMARQUE : *L'astérisque indique que pour Dell Hybrid Client, un référentiel sur site est nécessaire lorsque vous utilisez l'environnement Cloud public Wyse Management Suite.

Le tableau suivant fournit des informations sur les fonctionnalités de gestion des clients légers et des clients zéro Wyse prises en charge pour chaque abonnement.

Tableau 3. Matrice des fonctionnalités de gestion des clients légers et des clients zéro Wyse

Tableau 3. Matrice des fonctionnalités de gestion des clients légers et des clients zéro Wyse

Fonctionnalités de gestion des clients légers et des clients zéro Wyse	Wyse Management Suite Standard	Wyse Management Suite Pro (Cloud privé)	Wyse Management Suite Pro (édition Cloud)
Visibilité complète des actifs			
Découverte automatique des périphériques	√	√	√
Gestion des actifs, de l'inventaire et des systèmes	√	√	√
Affichage d'une configuration efficace au niveau des périphériques après l'héritage	√	√	√
Création de rapport et surveillance			
Prise de contrôle à distance avec VNC	√	√	
Intervalle de pulsation et de vérification configurable	√	√	√
Sécurité			
Communication sécurisée (HTTPS)	√	√	√
Déploiement du certificat 802.1x	√	√	√
MQTT sécurisé	√	√	√
Authentification à deux facteurs	X	√	√
Authentification Active Directory pour l'administration basée sur les rôles	X	√	√
Fonctionnalité de jonction de domaine (Windows 10 IoT Enterprise)	X	√	√
Mappage AD à l'aide de LDAPS	X	√	√
Paramètres de verrouillage (activation ou désactivation des ports des points de terminaison pris en charge)	X	√	√
Fonctionnalités complètes de gestion			
Gestion des correctifs et des images du système d'exploitation	√	√	√ **
Planification intelligente	√	√	√
Déploiement en mode silencieux	√	√	√
Regroupement des applications pour simplifier le déploiement et réduire les redémarrages	X	√	√
Création de groupes dynamiques et attribution en fonction des attributs des périphériques	X	√	√

Tableau 3. Matrice des fonctionnalités de gestion des clients légers et des clients zéro Wyse

Fonctionnalités de gestion des clients légers et des clients zéro Wyse	Wyse Management Suite Standard	Wyse Management Suite Pro (Cloud privé)	Wyse Management Suite Pro (édition Cloud)
Affectation du référentiel à la politique d'application et au mappage des sous-réseaux	X	√	√
Annulation automatique de l'enregistrement des appareils	√	√	√
Politique d'application avancée	X	√	√
Configuration			
Configuration de l'Assistant Wyse ThinOS 8.x et 9.x	√	√	√
Prise en charge multi-écrans	√	√	√
Wyse Easy Setup et Wyse Overlay Optimizer	√	√	√
Prise en charge de la rédaction de scripts de personnalisation de l'installation d'applications	X	√	√
Paramètres du BIOS et support de configuration	X	√	√
Exportation ou importation de la configuration de politique	X	√	√
Prise en charge du progiciel RSP	X	√	√
Outil d'importation de WDM	X	√	X
Exception d'appareil en bloc	X	√	√

REMARQUE : **Le double astérisque indique que pour les systèmes d'exploitation ThinLinux et Windows 10 IoT Enterprise, un référentiel sur site est nécessaire lorsque vous utilisez l'environnement Cloud public Wyse Management Suite.

2

Mise en route avec Wyse Management Suite

Cette section fournit des informations sur les fonctionnalités générales qui vous permettront d'effectuer vos premiers pas en tant qu'administrateur et de gérer les clients légers à l'aide de Wyse Management Suite.

Sujets :

Connexion à Wyse Management Suite sur le Cloud public

Pour vous connecter à la console Wyse Management Suite, un navigateur Web pris en charge doit être installé sur votre système. Procédez comme suit pour vous connecter à la console Wyse Management Suite :

1. Accédez à l'édition cloud public (SaaS) de Wyse Management Suite en utilisant l'un des liens suivants :
   - **Datacenter pour les États-Unis** : us1.wysemanagementsuite.com/ccm-web
   - **Datacenter pour l'Europe** : eu1.wysemanagementsuite.com/ccm-web
2. Saisissez votre nom d'utilisateur et votre mot de passe.
3. Cliquez sur **Connexion**

   Si vous vous connectez à la console Wyse Management Suite pour la première fois, si un nouvel utilisateur est ajouté, ou si une licence d'utilisateur est renouvelée, la page des **conditions générales** s'affiche. Lisez les conditions générales, cochez les cases voulues, puis cliquez sur **Accepter**.

REMARQUE : Vous recevez vos informations d'identification de connexion lorsque vous vous inscrivez à l'évaluation de Wyse Management Suite sur www.wysemanagementsuite.com ou lorsque vous achetez votre abonnement. Vous pouvez acheter l'abonnement à Wyse Management Suite auprès de l'équipe des ventes Dell ou de votre partenaire Dell local. Pour plus de détails, voir www.wysemanagementsuite.com.

REMARQUE : Un référentiel accessible en externe doit être installé sur un serveur doté d'une zone DMZ lors de l'utilisation de l'édition Pro de Wyse Management Suite sur le cloud public. En outre, le nom de domaine complet (FQDN) du serveur doit être enregistré sur un serveur de noms de domaine (DNS) public.

Modification de votre mot de passe

Pour modifier le mot de passe de connexion, procédez comme suit :

1. Cliquez sur le lien du compte dans le coin supérieur droit de la console de gestion.
2. Cliquez sur **Modifier le mot de passe**.

REMARQUE : Nous vous recommandons de modifier votre mot de passe après la première ouverture de session. Le nom d'utilisateur et le mot de passe par défaut pour les administrateurs supplémentaires sont créés par le propriétaire du compte Wyse Management Suite.

Fermeture de session

Pour vous déconnecter de la console de gestion, procédez comme suit :

1. Cliquez sur le lien du compte dans le coin supérieur droit de la console de gestion.
2. Cliquez sur **Déconnexion**.

Conditions préalables pour déployer Wyse Management Suite sur le Cloud privé

Tableau 4. Conditions préalables

Description	10 000 appareils ou moins	50 000 appareils ou moins	120 000 appareils ou moins	Logithèque de logiciels Wyse Management Suite
Système d'exploitation	Windows Server 2012 R2, Windows Server 2016 ou Windows Server 2019 Standard. Le serveur Web Wyse Management Suite dispose d'un serveur Web Apache Tomcat intégré. Assurez-vous de ne pas installer Microsoft IIS et les serveurs Web Apache Tomcat séparément. Module linguistique pris en charge : anglais, français, italien, allemand, espagnol, japonais et chinois traditionnel			
Espace disque minimum	40 Go	120 Mo	200 Go	120 Mo
Mémoire minimale (RAM)	8 Go	16 Go	32 Go	16 Go
Configuration minimale de l'UC	4	4	16	4
Ports de communication réseau	Le programme d'installation de Wyse Management Suite ajoute les ports TCP (Transmission Control Protocol) 443, 8080 et 1883 à la liste d'exceptions de pare-feu. Les ports sont ajoutés pour accéder à la console Wyse Management Suite et pour envoyer les notifications push aux clients légers. ● TCP 443 : communication HTTPS ● TCP 1883 : communication MQTT ● TCP 3306 : MariaDB (facultatif si distant) ● TCP 27017 : MongoDB (facultatif si distant) ● TCP 11211 : Memcached ● TCP 5172, 49159 : kit de développement logiciel de gestion de l'utilisateur final (EMSDK) (facultatif et requis uniquement pour la gestion des périphériques Teradici) ● TLS 443 : communication sécurisée MQTT Les ports par défaut utilisés par le programme d'installation peuvent être remplacés par un autre port au cours de l'installation.			Le programme d'installation de Wyse Management Suite Repository ajoute les ports TCP 443 et 8080 à la liste d'exceptions de pare-feu. Les ports sont ajoutés pour accéder aux images de système d'exploitation et d'application gérées par Wyse Management Suite.
Navigateurs pris en charge	Internet Explorer version 11 Google Chrome version 58.0 et versions supérieures Mozilla Firefox version 52.0 et versions supérieures Navigateur Edge sur Windows : anglais uniquement			

- Les scripts d'installation Overlay Optimizer version 1.0 sont fournis avec le programme d'installation de Wyse Management Suite. L'administrateur doit exécuter les scripts pour activer Overlay Optimizer afin qu'il soit disponible dans Wyse Management Suite.
- Les scripts d'installation Dell Secure Client version 1.0 sont fournis avec le programme d'installation de Wyse Management Suite. L'administrateur doit exécuter les scripts pour activer Dell Secure Client afin qu'il soit disponible dans Wyse Management Suite.

REMARQUE : `WMS.exe` WMS_Repo.exe doit être installé sur deux serveurs différents. Pour les Clouds publics, vous devez installer le référentiel distant Wyse Management Suite. Pour les Clouds privés, vous devez installer le référentiel distant et le référentiel local Wyse Management Suite. Le logiciel peut être installé sur une machine physique ou virtuelle. De même, il n'est pas nécessaire que la logithèque de logiciels et le serveur Wyse Management Suite aient le même système d'exploitation.

REMARQUE : Pour une configuration de 10 000 appareils, la mémoire (RAM) minimale doit être de 12 Go pour des communications sécurisées MQTT.

REMARQUE : Il est recommandé d'utiliser MongoDB version 4.2.12 pour les configurations distribuées à partir de Wyse Management Suite 3.2

Zones fonctionnelles de la console de gestion

L'organisation de la console Wyse Management Suite comprend les zones fonctionnelles suivantes :

- La page **Tableau de bord** fournit des informations sur l'état actuel de chaque zone fonctionnelle du système.
- La page **Groupes et configurations** utilise un groupe hiérarchique de gestion des règles pour la configuration des périphériques. Il est possible de créer des sous-groupes de la politique globale de groupes pour classer les appareils en fonction des normes de l'entreprise. Par exemple, les appareils peuvent être regroupés selon la fonction professionnelle, le type d'appareils et ainsi de suite.
- La page **Utilisateurs** permet d'attribuer les rôles d'administrateur global, d'administrateur de groupe et d'observateur aux utilisateurs locaux et aux utilisateurs importés à partir d'Active Directory, afin qu'ils puissent se connecter à Wyse Management Suite. Les autorisations attribuées aux utilisateurs leur permettent d'effectuer des opérations en fonction des rôles qui leur ont été affectés. De plus, l'onglet **Utilisateur final** est ajouté pour la gestion des utilisateurs finaux.
- La page **Appareils** vous permet d'afficher et de gérer les appareils, les types d'appareils et les configurations propres aux appareils.
- La page **Applications et données** permet de gérer les applications de périphériques, l'inventaire des applications et le référentiel des fichiers.
- La page **Règles** vous permet d'ajouter, de modifier et d'activer ou désactiver des règles telles que le regroupement automatique et les notifications d'alertes.
- La page **Tâches** vous permet de créer des tâches pour des opérations telles que le redémarrage, l'éveil par appel réseau (Wakeup On LAN) et la politique d'image ou d'application qui doit être déployée sur les périphériques enregistrés.
- La page **Événements** vous permet d'afficher et de vérifier les événements système et les alertes.
- La page **Administration de portail** vous permet de configurer divers paramètres du système tels que la configuration du référentiel local, l'abonnement de licence Dell Hybrid Client, la configuration du répertoire actif et l'authentification à deux facteurs.

Configuration et gestion des clients légers

- **Gestion de la configuration** : Wyse Management Suite prend en charge une hiérarchie de groupes et de sous-groupes. Les groupes peuvent être créés manuellement ou automatiquement en fonction des règles définies par l'administrateur système. Vous pouvez organiser les groupes en fonction de la hiérarchie fonctionnelle, par exemple marketing, ventes et ingénierie, ou en fonction de la hiérarchie de localisation, par exemple le pays/la région, l'état et la ville.

  REMARQUE : Dans l'édition Pro, vous pouvez ajouter des règles pour créer des groupes. Vous pouvez également affecter des périphériques à un groupe existant en fonction des attributs de périphérique tels que le sous-réseau, le fuseau horaire et la localisation.

  Vous pouvez aussi configurer ce qui suit :

  - Les paramètres qui s'appliquent à tous les appareils du compte du locataire et qui sont définis au niveau du groupe de politiques par défaut. Ces paramètres sont l'ensemble de paramètres globaux dont héritent tous les groupes et sous-groupes. Les paramètres configurés pour des groupes de niveau inférieur sont prioritaires sur les paramètres qui ont été configurés pour les groupes parents ou de niveau supérieur.

    Par exemple :

    - Configurez les politiques pour le groupe de politiques par défaut (groupe parent). Après avoir configuré les politiques, vérifiez les politiques de groupe personnalisé (groupe enfant). Les mêmes ensembles de politiques sont également appliqués au groupe enfant. Les configurations des paramètres de groupe de politiques par défaut désignent un ensemble global de paramètres hérités de tous les groupes et sous-groupes du groupe parent.

- Configurez différents paramètres pour le groupe personnalisé. Le groupe personnalisé reçoit les deux charges utiles, mais les appareils du groupe de politiques par défaut ne reçoivent pas les charges utiles configurées pour le groupe de politiques personnalisé.
- Configurez différents paramètres pour le groupe personnalisé. Les paramètres configurés pour des groupes de niveau inférieur sont prioritaires sur les paramètres qui ont été configurés pour les groupes parents ou de niveau supérieur.

○ Les paramètres spécifiques à un périphérique particulier qui peuvent être configurés à partir de la page **Détails du périphérique**. Ces paramètres, tels que ceux des groupes de niveau inférieur, sont prioritaires sur les paramètres configurés pour les groupes de niveau supérieur.

Lorsque vous créez et publiez la politique, les paramètres de configuration sont appliqués à tous les appareils de ce groupe y compris à ceux des sous-groupes.

Une fois la politique publiée et propagée à tous les appareils, les paramètres ne sont pas renvoyés aux appareils tant que vous n'apportez pas de modification. Les nouveaux appareils enregistrés reçoivent la politique de configuration qui s'applique à tout le groupe pour lequel elle a été enregistrée. Cela inclut les paramètres hérités du groupe global et des groupes de niveau intermédiaire.

Les politiques de configuration sont publiées immédiatement et ne peuvent pas être planifiées à un moment ultérieur. Quelques modifications de politique, par exemple l'affichage des paramètres, peuvent forcer un redémarrage.

- **Déploiement de l'image de l'application et du système d'exploitation** : les mises à jour de l'image de l'application et du système d'exploitation peuvent être déployées à partir de l'onglet **Applications et données**. Les applications sont déployées en fonction des groupes de politiques.

  REMARQUE : la politique d'application avancée vous permet de déployer une application pour le groupe actuel et tous les sous-groupes en fonction de vos besoins. Les images de système d'exploitation peuvent être déployées sur le groupe actuel uniquement.

  Wyse Management Suite prend en charge les politiques d'application standard et avancées. Une politique d'application standard vous permet d'installer un seul progiciel d'application. Le périphérique redémarre lors de l'installation d'une application. Redémarrez le périphérique avant et après chaque installation d'application. Avec une politique d'application avancée, plusieurs progiciels d'application peuvent être installés avec seulement deux redémarrages. Cette fonction est disponible uniquement pour l'édition Pro. Les politiques d'application avancées prennent également en charge l'exécution de scripts de pré et post installation qui peuvent être nécessaires pour installer une application particulière.

  Vous pouvez configurer les politiques d'application standard et avancées pour les appliquer automatiquement lorsqu'un périphérique est enregistré avec Wyse Management Suite ou lorsqu'un périphérique est déplacé vers un nouveau groupe.

  Le déploiement des politiques d'application et des images de système d'exploitation sur les Thin Clients peut être planifié immédiatement ou plus tard en fonction du fuseau horaire du périphérique ou de tout autre fuseau horaire.

- **Inventaire des périphériques** : cette option se trouve sous l'onglet **Appareils**. Par défaut, cette option affiche une liste paginée de tous les appareils du système. Vous pouvez choisir d'afficher un sous-ensemble d'appareils à l'aide de différents filtres, par exemple par groupe ou sous-groupe, type de périphérique, type de système d'exploitation, état, sous-réseau et plate-forme ou fuseau horaire.

  Pour accéder à la page **Détails sur le périphérique** pour ce périphérique, cliquez sur l'entrée de périphérique répertoriée sur cette page. Tous les détails du périphérique s'affichent.

  La page **Détails du périphérique** affiche également tous les paramètres de configuration applicables à sur le périphérique et le niveau de groupe auquel chaque paramètre est appliqué.

  Cette page permet également de définir les paramètres de configuration qui sont spécifiques à ce périphérique en cliquant sur le bouton **Exceptions du périphérique**. Les paramètres configurés dans cette section remplacent tous les paramètres qui ont été configurés au niveau des groupes et/ou au niveau global.

- **Rapports** : vous pouvez générer et afficher des rapports en fonction des filtres prédéfinis. Pour générer des rapports, cliquez sur l'onglet **Rapports** de la page **Administration de portail**.
- **Application mobile** : vous pouvez recevoir des notifications d'alertes et gérer les appareils à l'aide de l'application mobile **Dell Mobile Agent** disponible pour les appareils Android. Pour télécharger l'application mobile et le **Dell Mobile Agent Getting Started Guide** (Guide de mise en route de Dell Mobile Agent), cliquez sur l'onglet **Alertes et classification** de la page **Administration de portail**.

Wyse Device Agent

La solution Wyse Device Agent (WDA) est un agent unifié pour toutes les solutions de gestion de clients légers. Si vous installez WDA, vous pouvez gérer les clients légers à l'aide de Wyse Management Suite.

Les trois types d'environnements de sécurité client suivants sont pris en charge par la solution Wyse Device Agent :

- **Environnements hautement sécurisés** : pour réduire le risque par rapport au serveur étranger DHCP ou DNS pour la détection de nouveaux appareils, les administrateurs doivent se connecter à chaque appareil individuellement et configurer l'URL du serveur Wyse Management Suite. Vous pouvez utiliser un certificat signé par une autorité de certification ou un certificat auto-signé. Cependant, Dell vous recommande d'utiliser un certificat signé par une autorité de certification. Dans la solution de cloud privé Wyse Management Suite avec certificat auto-signé, le certificat doit être configuré manuellement dans tous les appareils. En outre, le certificat doit être copié vers le dossier `Configuration de l'agent` pour préserver le certificat et réduire le risque par rapport au serveur étranger DHCP ou DNS, même après avoir recréé une image de l'appareil.

  Le dossier `Configuration de l'agent` est disponible à l'emplacement suivant :
  - Appareils Windows Embedded Standard : `%SYSTEMDRIVE% \\Wyse\\WCM\\ConfigMgmt\\Certificates`
  - Appareils ThinLinux : `/etc/addons.d/WDA/certs`
  - Appareils ThinOS : `wnos/cacerts/`

  REMARQUE : Vous devez importer le certificat vers un client léger exécutant le système d'exploitation ThinOS à l'aide d'un lecteur USB ou de chemins d'accès FTP.
- **Environnements sécurisés** : pour réduire le risque par rapport au serveur étranger DHCP ou DNS pour la détection de nouveaux appareils, les administrateurs doivent configurer le serveur Wyse Management Suite à l'aide de certificats signés par une autorité de certification. L'appareil peut chercher l'URL du serveur Wyse Management Suite à partir des enregistrements DHCP/DNS et effectuer la validation de l'autorité de certification. La solution de cloud privé Wyse Management Suite avec certificat auto-signé exige que le certificat soit envoyé vers l'appareil après le premier enregistrement si l'appareil ne dispose pas du certificat avant l'enregistrement. Ce certificat est conservé, même après que vous ayez recréé une image ou redémarré l'appareil pour réduire le risque par rapport au serveur étranger DHCP ou DNS.
- **Environnements normaux** : l'appareil obtient l'URL du serveur Wyse Management Suite à partir des enregistrements DHCP/DNS pour la solution de cloud privé Wyse Management Suite qui est configurée avec un certificat signé par une autorité de certification ou un certificat auto-signé. Si l'option de validation de l'autorité de certification est désactivée sur l'appareil, l'administrateur de Wyse Management Suite est averti une fois que l'appareil est enregistré pour la première fois. Dans ce scénario, Dell recommande que les administrateurs exécutent un envoi de certificat vers l'appareil sur lequel le serveur est configuré avec un certificat auto-signé. Cet environnement n'est pas disponible pour le cloud public.

Dell Client Agent

Dell Client Agent (DCA) est un agent unifié pour toutes les solutions de gestion Dell Hybrid Client. Si vous installez DCA, vous pouvez gérer Dell Hybrid Clients à l'aide de Wyse Management Suite.

Pour installer Dell Hybrid Client sur le périphérique OptiPlex 7070 Ultra :

1. Enregistrez le périphérique dans Wyse Management Suite en utilisant la méthode de découverte (DNS ou DHCP) ou la méthode manuelle **reg.json** : consultez la section Méthodes d'enregistrement de périphériques dans Wyse Management Suite.
2. Réinitialisez votre périphérique OptiPlex 7070 Ultra : consultez la section Réinitialiser Dell Hybrid Client.

Dell Client Agent-Enabler

Dell Client Agent-Enabler (DCA-Enabler) est un agent client pour la gestion des versions Ubuntu 18.04 et 20.04 LTS 64 bits sur les appareils Dell Ubuntu. Le logiciel Dell Hybrid Client est préchargé avec Dell Client Agent-Enabler (DCA-Enabler). DCA-Enabler prend en charge et vous permet d'effectuer les actions suivantes qui sont gérées par Wyse Management Suite :

- Enregistrement des appareils Ubuntu
- Déploiement de commandes en temps réel telles que Requête, Redémarrer, Arrêter, et Wake-on-LAN.
- Commande Device Pull Log.
- Annulation de l'enregistrement sur le serveur
- Conversion en commande Hybrid Client à l'aide de la page Tâches, Appareils ou Détails de l'appareil.
- Déploiement d'une politique d'application standard.
- Déploiement d'une politique d'application avancée.
- Déploiement d'une politique de conversion Generic Client en Dell Hybrid Client
- Déploiement d'une politique de certificats

DCA-Enabler est préchargé sur la plupart des plateformes Dell Ubuntu. Les dossiers DCA-Enabler et les fichiers correspondants se trouvent aux emplacements suivants :

- `/etc/dcae/config/`

- `/etc/dcae/certificates/`
- `/var/log/dcae/dcae.log`
- `/usr/sbin/dcae`

Vous pouvez vérifier le service et le package DCA-Enabler dans la plateforme Dell Ubuntu à l'aide des commandes suivantes :

- `systemctl status dcae.service-` La version active en cours d'exécution est affichée.
- `dpkg -l | grep dca-enabler-` La version de DCA-ENabler est affichée au format **dca-enabler 1.x.0-xx**.

3

Installation ou mise à niveau de Wyse Device Agent

Cette section fournit des informations sur la façon d'installer ou de mettre à niveau Wyse Device Agent sur vos clients légers, tels que les appareils Windows Embedded Standard, Linux et ThinLinux, à l'aide de Wyse Management Suite.

- **Appareils Windows Embedded Standard** : Wyse Device Agent 1.4.x peut être téléchargé à partir de support.dell.com. Vous pouvez installer ou mettre à niveau Wyse Device Agent sur des appareils Windows Embedded Standard à l'aide de l'une des méthodes suivantes :
  - Installation manuelle de Wyse Device Agent
  - Mise à niveau de Wyse Device Agent à l'aide de la politique de l'application Wyse Management Suite

  REMARQUE : Vous pouvez également mettre à niveau Wyse Device Agent manuellement en double-cliquant sur la dernière version du fichier .exe de Wyse Device Agent.

  REMARQUE : Wyse Device Agent peut être installé sur le système d'exploitation Windows Embedded Standard 7 uniquement si KB3033929 est disponible.
- **Appareils Linux et ThinLinux** : Wyse Device Agent peut être installé ou mis à niveau sur les appareils Linux et ThinLinux à l'aide de Wyse Management Suite. Pour plus d'informations, reportez-vous à la section d'installation ou mise à niveau de Wyse Device Agent sur les clients ThinLinux et Linux.

Sujets :

Installation manuelle de Wyse Device Agent sur un appareil Windows Embedded

Étapes

1. Copiez le fichier `WDA.exe` sur le Thin Client.
2. Double-cliquez sur le fichier `WDA.exe`.
3. Cliquez sur **Oui**.

   REMARQUE : Un message d'avertissement s'affiche lorsqu'une version plus ancienne de Wyse Device Agent ou HAgent est installée sur l'appareil.

4. Dans le champ **Jeton de groupe**, saisissez un jeton de groupe. Ce champ est facultatif.
   Pour ignorer cette étape, cliquez sur **Suivant**. Vous pourrez saisir les détails du jeton de groupe à un autre emplacement de l'interface utilisateur de Wyse Device Agent.
5. Dans la liste déroulante **Région**, sélectionnez la région du serveur de cloud public de Wyse Management Suite.
   Après avoir réussi l'installation, le serveur de cloud public de Wyse Management Suite enregistre automatiquement l'appareil dans la console Wyse Management Suite.

Mise à niveau de Wyse Device Agent à l'aide de la politique de l'application Wyse Management Suite

Prérequis

Nous vous recommandons d'utiliser l'application Wyse Management Suite pour mettre à niveau Wyse Device Agent. Dans la configuration du cloud privé Wyse Management Suite, les packages Wyse Device Agent les plus récents pour Windows Embedded Standard sont disponibles dans le référentiel local. Si vous utilisez un Cloud public ou un référentiel distant sur un Cloud privé, copiez le fichier `WDA.exe` dans le dossier `thinClientApps` du référentiel.

Étapes

1. Une fois le fichier `WDA.exe` copié dans le référentiel, accédez à **Applications et données**, puis créez une politique d'application standard avec ce package : voir Créer et déployer une politique d'application standard pour les clients légers.

   REMARQUE : la politique d'application avancée n'est prise en charge qu'à partir de la version Wyse Device Agent 14.x. Nous vous recommandons d'utiliser la politique d'application standard lors de la mise à niveau de Wyse Device Agent à partir de la version 14.x. Vous pouvez également utiliser la politique d'application avancée pour mettre à niveau Wyse Device Agent à partir de la version 14.x.

2. Accédez à la page **Tâches** et planifiez une tâche pour mettre à niveau Wyse Device Agent.

   REMARQUE : Pour mettre à niveau Windows Embedded Standard Wyse Device Agent de la version 13.x à la version 14.x, nous vous recommandons d'utiliser HTTP comme protocole de référentiel.

   Une fois l'installation terminée, l'état est envoyé au serveur.

Installation ou mise à niveau de Wyse Device Agent sur les clients ThinLinux et Linux

Prérequis

- Pour installer des Wyse Device Agents sur les Thin Clients Dell Wyse 3040 avec ThinLinux version 2.0, image version 2.0.14 et Wyse Device Agent version 3.0.7, vous devez installer le fichier `wda3040_3.0.10-01_amd64.deb`, puis le fichier `wda_3.2.12-01_amd64.tar`.
- Vous devez installer le module complémentaire de l'utilitaire de la plate-forme et le module complémentaire Wyse Device Agent pour les clients légers Linux. Vous pouvez installer le fichier `wda_x.x.x.tar` pour les Thin Clients ThinLinux.

À propos de cette tâche

Vous pouvez installer ou mettre à niveau des modules complémentaires en utilisant l'une des options suivantes :

- Utilisation de paramètres INI
- Gestionnaire de plug-ins
- Commandes RPM

Étapes

1. Si vous utilisez un cloud public ou un référentiel distant sur un cloud privé, copiez les fichiers RPM dans le dossier `thinClientApps` du référentiel. Par défaut, les fichiers RPM les plus récents pour Wyse Device Agent et pour les utilitaires de la plate-forme destinés aux clients ThinLinux et Linux sont disponibles dans un référentiel local.
2. Rendez-vous sur la page **Tâches** et planifiez une tâche pour mettre à niveau le module complémentaire de l'utilitaire de la plate-forme.

   Vous devez attendre l'installation complète de l'utilitaire de la plate-forme sur le Thin Client.

   REMARQUE : Installez tout d'abord le module complémentaire de l'utilitaire de la plate-forme, puis installez le module complémentaire Wyse Device Agent. Vous ne pouvez pas installer la dernière version de Wyse Device Agent avant d'avoir installé le module complémentaire de l'utilitaire de la plate-forme.

3. Sur la page **Tâches**, planifiez une tâche pour mettre à niveau Wyse Device Agent sur le client.

REMARQUE : Le client Linux redémarre après l'installation de la version 2.0.11 du module complémentaire Wyse Device Agent.

4

Installation ou mise à niveau de DCA-Enabler sur les appareils Ubuntu

Cette section fournit des informations sur la façon d'installer ou de mettre à niveau DCA-Enabler sur les appareils Ubuntu.

Sujets :

Installer DCA-Enabler sur les appareils Ubuntu

DCA-Enabler est préchargé sur la plupart des plateformes Dell Ubuntu. Si DCA-Enabler n'est pas préchargé, vous pouvez l'installer.

Étapes

1. Téléchargez les packages DCA-Enabler sur www.dell.com/support.
2. Extrayez le fichier téléchargé.
   Le fichier extrait contient des fichiers .deb.
3. Installez les packages DCA-Enabler à l'aide des commandes suivantes :
   - `"dpkg -i < dca-enabler-packages_1.x-x_amd64.deb >"`
   - `"dpkg -i < dca-enabler_1.x.x-x_amd64.deb >"`

Mise à niveau de DCA-Enabler sur les appareils Ubuntu

Vous pouvez mettre à jour DCA-Enabler sur les appareils Ubuntu en utilisant l'une des méthodes suivantes :

- Enregistrez l'appareil auprès de Wyse Management Suite et déployez le dernier package DCA-Enabler en utilisant la politique d'application.
- Téléchargez et extrayez manuellement le package, puis exécutez les commandes suivantes sur l'appareil :
  - `"dpkg -i < dca-enabler-packages_1.x-x_amd64.deb"`
  - `"dpkg -i < dca-enabler_1.x.x-x_amd64.deb"`

5

Enregistrement et configuration d'un nouvel appareil à l'aide de Wyse Management Suite

Sujets :

Enregistrer et configurer un nouveau périphérique Windows Embedded Standard à l'aide de Wyse Management Suite

Étapes

1. Installez Wyse Device Agent sur votre client léger : voir Installation ou mise à niveau de Wyse Device Agent.
2. Enregistrez votre client léger dans Wyse Management Suite : voir Enregistrement de Thin Clients Windows Embedded Standard dans Wyse Management Suite à l'aide de Wyse Device Agent.

   REMARQUE : Vous pouvez également enregistrer les appareils à l'aide de l'une des méthodes suivantes :
   - À l'aide des balises d'option DHCP : voir Enregistrement d'appareils à l'aide des balises d'option DHCP.
   - À l'aide d'un enregistrement SRV DNS : voir Enregistrement d'appareils à l'aide d'un enregistrement SRV DNS.

   REMARQUE : Lorsque l'option **Validation de l'inscription** est activée, les périphériques détectés, que ce soit manuellement ou automatiquement, se trouvent à l'état **En attente de validation de l'inscription** sur la page **Périphériques**. Le client peut sélectionner un ou plusieurs appareils sur la page **Appareils** et valider l'inscription. Une fois validés, les appareils sont déplacés vers le groupe prévu. Pour plus d'informations sur la validation des périphériques, voir Validation de l'inscription.
3. Ajoutez le périphérique au groupe de votre choix (facultatif) : voir Gestion des groupes et des configurations.
4. Configurez le client léger à l'aide de l'une des options suivantes :
   - À l'aide de la page **Groupes et configurations** : voir Modifier les paramètres de la politique Windows Embedded Standard.
   - À l'aide de la page **Appareils** : voir Gestion des périphériques.

Enregistrer et configurer un nouveau périphérique ThinOS 8.x à l'aide de Wyse Management Suite

Étapes

1. Dans le menu du bureau du client léger, sélectionnez **Configuration du système** > **Configuration centrale**.
   La fenêtre **Configuration centrale** s'affiche.
2. Saisissez la **Clé d'enregistrement de groupe** selon la configuration de votre administrateur pour le groupe de votre choix.
3. Cochez la case **Activer les paramètres avancés WMS**.
4. Dans le champ **Serveur WMS**, saisissez l'URL de Wyse Management Server.

5. Activez ou désactivez la validation CA selon votre type de licence. Pour le Cloud public, cochez la case **Activer la validation CA**. Pour le Cloud privé, cochez la case **Activer la validation de l'autorité de certification** si vous avez importé des certificats provenant d'une autorité de certification reconnue dans votre serveur Wyse Management Suite.

   Pour activer l'option Validation CA dans le Cloud privé, vous devez également installer le même certificat auto-signé sur sur le périphérique ThinOS. Si vous n'avez pas installé le certificat auto-signé sur le périphérique ThinOS, ne cochez pas la case **Activer la validation CA**. Vous pouvez installer le certificat sur sur le périphérique via Wyse Management Suite après l'enregistrement, puis activer l'option Validation CA.
6. Pour vérifier la configuration, cliquez sur **Valider la clé**.

   REMARQUE : Si la clé n'est pas validée, vérifiez la clé de groupe et l'URL de serveur WMS que vous avez fourni. Assurez-vous que les ports mentionnés ne sont pas bloqués par le réseau. Les ports par défaut sont les ports 443 et 1883.
7. Cliquez sur **OK**.

   REMARQUE : Lorsque l'option **Validation de l'inscription** est activée, les périphériques détectés, que ce soit manuellement ou automatiquement, se trouvent à l'état **En attente de validation de l'inscription** sur la page **Périphériques**. Le client peut sélectionner un ou plusieurs appareils sur la page **Appareils** et valider l'inscription. Une fois validés, les appareils sont déplacés vers le groupe prévu. Pour plus d'informations sur la validation des périphériques, voir Validation de l'inscription.

   Le périphérique est enregistré sur Wyse Management Suite.
8. Connectez-vous à Wyse Management Suite.
9. Ajoutez le périphérique au groupe de votre choix (facultatif) : voir Gestion des groupes et des configurations.
10. Configurez le client léger à l'aide de l'une des options suivantes :
    - À l'aide de la page **Groupes et configurations** : voir Modifier les paramètres de la politique ThinOS.
    - À l'aide de la page **Appareils** : voir Gestion des périphériques.

Enregistrer et configurer un nouveau périphérique ThinOS 9.x à l'aide de Wyse Management Suite

Étapes

1. Dans le menu du bureau du client léger, sélectionnez **Configuration du système** > **Configuration centrale**.
   La fenêtre **Configuration centrale** s'affiche.
2. Saisissez la **Clé d'inscription de groupe** selon la configuration de votre administrateur pour le groupe de votre choix.
3. Cochez la case **Activer les paramètres avancés WMS**.
4. Dans le champ **Serveur WMS**, saisissez l'URL de Wyse Management Server.
5. Activez ou désactivez la validation CA selon votre type de licence. Pour le Cloud public, sélectionnez la case à cocher **Activer la validation CA** et pour le Cloud privé, sélectionnez la case à cocher **Activer la validation CA** si vous avez importé des certificats provenant d'une autorité de certification reconnue dans votre serveur Wyse Management Suite.

   Pour activer l'option Validation CA dans le Cloud privé, vous devez également installer le même certificat auto-signé sur le périphérique ThinOS. Si vous n'avez pas installé le certificat auto-signé sur le périphérique ThinOS, ne cochez pas la case **Activer la validation CA**. Vous pouvez installer le certificat sur le périphérique via Wyse Management Suite après l'enregistrement, puis activer l'option Validation CA.
6. Pour vérifier la configuration, cliquez sur **Valider la clé**.

   REMARQUE : Si la clé n'est pas validée, vérifiez la clé de groupe et l'URL de serveur WMS que vous avez fourni. Assurez-vous que les ports mentionnés ne sont pas bloqués par le réseau. Les ports par défaut sont les ports 443 et 1883.

   Une fenêtre d'alerte s'affiche.
7. Cliquez sur **OK**.
8. Cliquez sur **OK** dans la fenêtre **Configuration centrale**.

   REMARQUE : Vous pouvez également enregistrer les périphériques à l'aide de l'une des méthodes suivantes :
   - À l'aide des balises d'option DHCP : voir Enregistrement des périphériques à l'aide des balises d'option DHCP.
   - À l'aide d'un enregistrement SRV DNS : voir Enregistrement des périphériques à l'aide d'un enregistrement SRV DNS.

   REMARQUE : Lorsque l'option **Validation de l'inscription** est activée, les périphériques détectés, que ce soit manuellement ou automatiquement, se trouvent à l'état **En attente de validation de l'inscription** sur la page **Périphériques**. Le client peut

sélectionner un ou plusieurs périphériques sur la page **Périphériques** et valider l'inscription. Une fois validés, les périphériques sont déplacés vers le groupe prévu. Pour plus d'informations sur la validation des périphériques, voir Validation de l'inscription.

Le périphérique est enregistré sur Wyse Management Suite.

9. Connectez-vous à Wyse Management Suite.
10. Ajoutez le périphérique au groupe de votre choix (en option) : voir Gestion des groupes et des configurations.
11. Configurez le client léger à l'aide de l'une des options suivantes :
    - À l'aide de la page **Groupes et configurations** : voir Modifier les paramètres de la politique ThinOS 9.x.
    - À l'aide de la page **Périphériques** : voir Gestion des périphériques.

Enregistrer et configurer un nouveau périphérique Linux ou ThinLinux à l'aide de Wyse Management Suite

Étapes

1. Installez Wyse Device Agent sur votre client léger : voir Installation ou mise à niveau de Wyse Device Agent.
2. Enregistrez votre client léger dans Wyse Management Suite : voir Enregistrer des clients légers Linux/ThinLinux dans Wyse Management Suite à l'aide de Wyse Device Agent.

   REMARQUE : Vous pouvez également enregistrer les appareils à l'aide de l'une des méthodes suivantes :
   - À l'aide des balises d'option DHCP : voir Enregistrement d'appareils à l'aide des balises d'option DHCP.
   - À l'aide d'un enregistrement SRV DNS : voir Enregistrement d'appareils à l'aide d'un enregistrement SRV DNS.

   REMARQUE : Lorsque l'option **Validation de l'inscription** est activée, les périphériques détectés, que ce soit manuellement ou automatiquement, se trouvent à l'état **En attente de validation de l'inscription** sur la page **Périphériques**. Le client peut sélectionner un ou plusieurs appareils sur la page **Appareils** et valider l'inscription. Une fois validés, les appareils sont déplacés vers le groupe prévu. Pour plus d'informations sur la validation des périphériques, voir Validation de l'inscription.

3. Ajoutez le périphérique au groupe de votre choix (facultatif) : voir Gestion des groupes et des configurations.
4. Configurez le client léger à l'aide de l'une des options suivantes :
   - À l'aide de la page **Groupes et configurations** : voir Modifier les paramètres de la politique ThinLinux ou Modifier les paramètres de la politique Linux.
   - À l'aide de la page **Appareils** : voir Gestion des périphériques.

Enregistrer et configurer un nouveau Thin Client Wyse Software à l'aide de Wyse Management Suite

Étapes

1. Installez Wyse Device Agent sur votre client léger : voir Installation ou mise à niveau de Wyse Device Agent.
2. Enregistrez votre client léger dans Wyse Management Suite : voir Enregistrer Thin Client Wyse Software dans Wyse Management Suite à l'aide de Wyse Device Agent.

   REMARQUE : Vous pouvez également enregistrer les appareils à l'aide de l'une des méthodes suivantes :
   - À l'aide des balises d'option DHCP : voir Enregistrement d'appareils à l'aide des balises d'option DHCP.
   - À l'aide d'un enregistrement SRV DNS : voir Enregistrement d'appareils à l'aide d'un enregistrement SRV DNS.

   REMARQUE : Lorsque l'option **Validation de l'inscription** est activée, les périphériques détectés, que ce soit manuellement ou automatiquement, se trouvent à l'état **En attente de validation de l'inscription** sur la page **Périphériques**. Le client peut sélectionner un ou plusieurs appareils sur la page **Appareils** et valider l'inscription. Une fois validés, les appareils sont déplacés vers le groupe prévu. Pour plus d'informations sur la validation des périphériques, voir Validation de l'inscription.

3. Ajoutez le périphérique au groupe de votre choix (en option) : voir Gestion des groupes et des configurations.
4. Configurez le client léger à l'aide de l'une des options suivantes :

- À l'aide de la page **Groupes et configurations** : voir Modifier les paramètres de la politique Thin Client Wyse Software.
- À l'aide de la page **Appareils** : voir Gestion des périphériques.

Enregistrement et configuration de Dell Hybrid Client à l'aide de Wyse Management Suite

Prérequis

Avant d'enregistrer l'appareil, assurez-vous que votre appareil dispose d'une connectivité réseau pour contacter le serveur Wyse Management Suite.

REMARQUE : vous pouvez enregistrer ou annuler l'enregistrement de l'appareil uniquement à partir du compte utilisateur invité.

Étapes

1. Connectez-vous à Dell Hybrid Client en tant qu'utilisateur invité.
2. Dans la barre supérieure, cliquez sur l'.

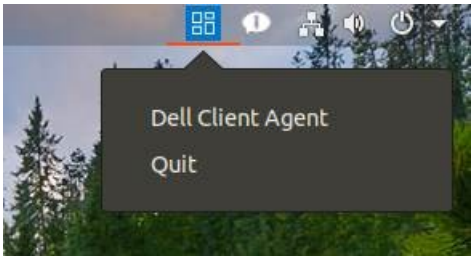


Figure 1. Icône Dell Client Agent

3. Cliquez sur **Dell Client Agent**.
   La boîte de dialogue **Dell Client Agent** s'affiche.
4. Cliquez sur **Inscription**.
   L'état par défaut s'affiche et indique **Découverte en cours**.
5. Pour enregistrer manuellement, cliquez sur le bouton **Annuler**.
6. Dans le champ **Serveur WMS**, saisissez l'URL du serveur Wyse Management Suite.
7. Dans le champ **Jeton de groupe**, saisissez la clé d'inscription de groupe. Le jeton de groupe est une clé unique permettant d'enregistrer directement vos appareils auprès de groupes.

   REMARQUE : si les champs client et groupe sont vides, l'appareil est enregistré auprès du groupe non géré. Toutefois, le jeton de groupe est obligatoire pour enregistrer l'appareil dans un Cloud public.

8. Cliquez sur le bouton **Marche/Arrêt** pour activer ou désactiver l'option **Valider l'autorité de certification du certificat de serveur**. Activez cette option pour effectuer la validation de certificat de serveur pour toutes les communications entre les appareils et les serveurs.

   L'option Validation de l'autorité de certification est activée automatiquement et ne peut pas être désactivée si une URL de Cloud public est saisie.
9. Cliquez sur **Enregistrer** pour enregistrer votre client hybride sur le serveur Wyse Management Suite.

   Vous pouvez également enregistrer les périphériques à l'aide de l'une des méthodes suivantes :
   - À l'aide des balises d'option DHCP : voir Enregistrement des périphériques à l'aide des balises d'option DHCP.
   - À l'aide d'un enregistrement SRV DNS : voir Enregistrement des périphériques à l'aide d'un enregistrement SRV DNS.

   REMARQUE : Lorsque l'option **Validation de l'inscription** est activée, les périphériques détectés, que ce soit manuellement ou automatiquement, se trouvent à l'état **En attente de validation de l'inscription** sur la page **Périphériques**. Le client peut sélectionner un ou plusieurs périphériques sur la page **Périphériques** et valider l'inscription. Une fois validés, les périphériques sont déplacés vers le groupe prévu. Pour plus d'informations sur la validation des périphériques, voir Validation de l'inscription.

   Lorsque votre client hybride est enregistré, l'état est affiché comme étant **Enregistré** avec une coche de couleur verte en regard de l'étiquette **État de l'enregistrement**. La légende du bouton **Enregistrer** devient **Annuler l'enregistrement**.

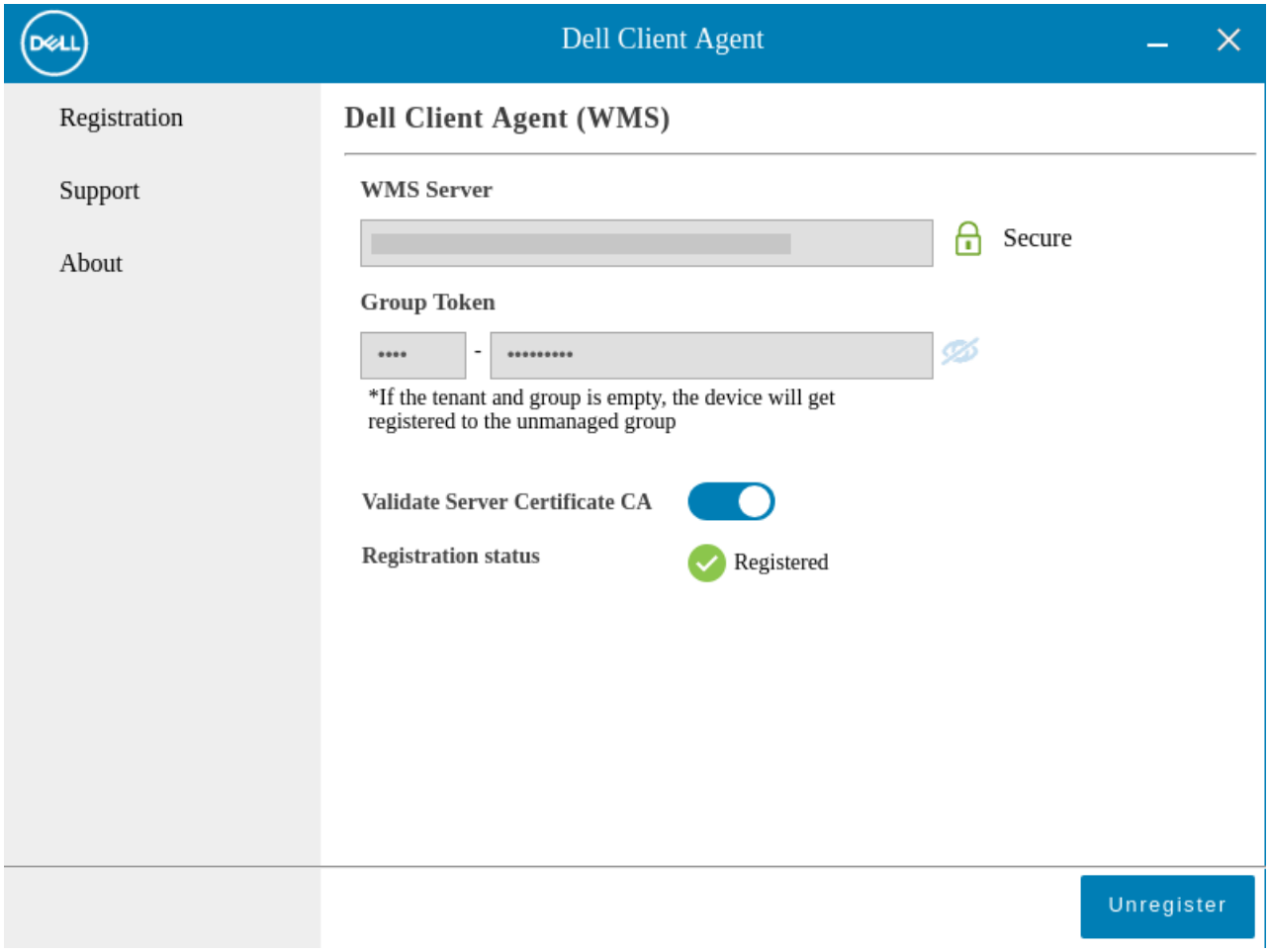


Figure 2. Dell Client Agent

10. Connectez-vous à Wyse Management Suite.
11. Ajoutez le périphérique au groupe de votre choix (facultatif) : voir Gestion des groupes et des configurations.
12. Configurez le client léger à l'aide de l'une des options suivantes :
    - À l'aide de la page **Groupes et configurations** : voir Modifier les paramètres de la politique Dell Hybrid Client.
    - À l'aide de la page **Périphériques** : voir Gestion des périphériques.

Enregistrement et configuration de Dell Generic Client à l'aide de Wyse Management Suite

Prérequis

- Avant d'enregistrer l'appareil, assurez-vous que votre appareil dispose d'une connectivité réseau pour contacter le serveur Wyse Management Suite.
- DCA-Enabler est installé sur l'appareil.

REMARQUE : Vous pouvez enregistrer ou annuler l'enregistrement de l'appareil uniquement à partir du compte utilisateur Ubuntu.

Étapes

1. Connectez-vous au Dell Generic Client exécutant le système d'exploitation Ubuntu.
2. Ouvrez le terminal.
3. Redémarrez le service dcae_service à l'aide de la commande `systemctl restart dcae.service`.

   Le service DCA-Enabler tente d'enregistrer manuellement l'appareil à l'aide du fichier reg.json présent dans le dossier `/etc/dcae/config`.

Vous pouvez également enregistrer les périphériques à l'aide de l'une des méthodes suivantes :

- À l'aide des balises d'option DHCP : voir Enregistrement des périphériques à l'aide des balises d'option DHCP.
- À l'aide d'un enregistrement SRV DNS : voir Enregistrement des périphériques à l'aide d'un enregistrement SRV DNS.

REMARQUE : Lorsque l'option **Validation de l'inscription** est activée, les périphériques détectés, que ce soit manuellement ou automatiquement, se trouvent à l'état **En attente de validation de l'inscription** sur la page **Périphériques**. Le client peut sélectionner un ou plusieurs périphériques sur la page **Périphériques** et valider l'inscription. Une fois validés, les périphériques sont déplacés vers le groupe prévu. Pour plus d'informations sur la validation des périphériques, voir Validation de l'inscription.

4. Connectez-vous à Wyse Management Suite.
5. Ajoutez ou déplacez l'appareil dans le groupe de votre choix (facultatif) : consultez Gestion des groupes et des configurations.
6. Configurez le Generic client à l'aide de l'une des options suivantes :
   - À l'aide de la page **Groupes et configurations** : consultez Modifier les paramètres du Dell Generic Client.
   - À l'aide de la page **Périphériques** : voir Gestion des périphériques.

6

Tableau de bord Wyse Management Suite

La page **Tableau de bord** vous permet d'afficher l'état d'un système et les tâches récentes qui sont effectuées au sein du système. Pour afficher une alerte particulière, cliquez sur le lien situé dans la section **Alertes**. La page **Tableau de bord** vous permet également d'afficher le résumé des appareils.

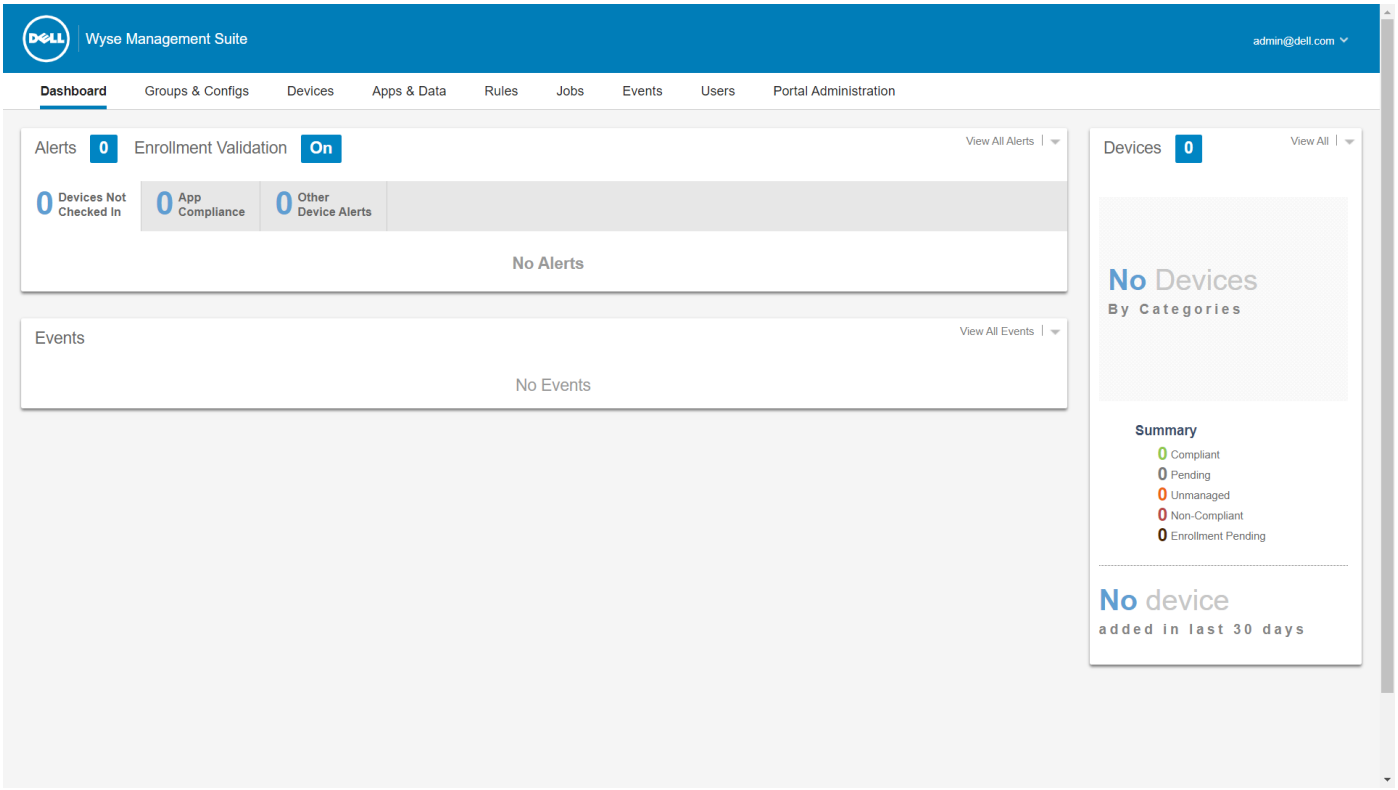


Figure 3. Tableau de bord

Sujets :

- Afficher les alertes
- Afficher la liste des événements
- Afficher l'état des appareils
- Activer la validation de l'inscription
- Modifier les préférences utilisateur
- Accéder à l'aide en ligne
- Changer votre mot de passe
- Déconnexion de la console de gestion

Afficher les alertes

La section **Alertes** affiche le récapitulatif de toutes les alertes.

Étapes

1. Cliquez sur **Tableau de bord**.
   Le récapitulatif des alertes s'affiche.

2. Cliquez sur **Afficher toutes les alertes**.
   La page **Événements** contient les attributs suivants :
   - **Appareils non vérifiés**
   - **Conformité d'application**
   - **Autres alertes d'appareil**

Afficher la liste des événements

La section **Événements** affiche le récapitulatif des événements qui se sont produits au cours des derniers jours.

Étapes

1. Cliquez sur **Tableau de bord**.
   Le récapitulatif des événements s'affiche.
2. Cliquez sur **Afficher tous les événements**.
   La page **Événements** s'affiche avec la liste de tous les événements.

Afficher l'état des appareils

La section **Afficher** fournit le récapitulatif des états des appareils.

Étapes

1. Cliquez sur **Tableau de bord**.
   Le récapitulatif des périphériques s'affiche.
2. Cliquez sur **Afficher tout**.
   La page **Périphériques** s'affiche avec la liste de tous les périphériques enregistrés. La section **Résumé** affiche le nombre d'appareils en fonction des catégories d'état suivantes :
   - **Conforme**
   - **En attente**
   - **Non géré**
   - **Non conforme**
   - **Inscription en attente**

Activer la validation de l'inscription

Vous pouvez activer l'option **Validation de l'inscription** pour permettre aux administrateurs de contrôler l'enregistrement manuel et automatique des clients légers sur un groupe.

Étapes

1. Cliquez sur **Tableau de bord**.
2. Cliquez sur le bouton **ON/OFF** en regard de l'option **Validation de l'inscription**.
   Vous êtes redirigé vers l'option **Autres paramètres** de la page **Administration de portail**.
3. Activez ou désactivez l'option **Validation de l'inscription**.

Modifier les préférences utilisateur

Vous pouvez modifier les préférences utilisateur, comme les notifications d'alertes, les paramètres de politique et le format de page.

Étapes

1. Dans le coin supérieur droit de la page **Tableau de bord**, cliquez sur le menu déroulant de connexion.
2. Cliquez sur **Préférences utilisateur**.
   La fenêtre **Préférences utilisateur** s'affiche.

3. Cliquez sur **Alertes** et cochez les cases appropriées pour attribuer un type d'alerte (Critique, Avertissement ou Informations) aux notifications envoyées par e-mail ou par les applications mobiles.
4. Cliquez sur **Politiques** et cochez la case **Me demander si je veux utiliser le mode Assistant ThinOS** pour afficher la fenêtre **Sélectionner le mode de configuration de ThinOS** à chaque fois que vous configurez les paramètres d'une politique ThinOS.
5. Cliquez sur **Taille de la page**, puis entrez un numéro compris entre 10 et 100 dans la zone de texte **Nombre d'éléments par page**. Cette option vous permet de définir le nombre d'éléments affichés sur chaque page.

Accéder à l'aide en ligne

Étapes

1. Dans le coin supérieur droit de la page **Tableau de bord**, cliquez sur le menu déroulant de connexion.
2. Cliquez sur **Aide WMS**.
   La page **Prise en charge de Wyse Management Suite** s'affiche.

Changer votre mot de passe

Étapes

1. Dans le coin supérieur droit de la page **Tableau de bord**, cliquez sur le menu déroulant de connexion.
2. Cliquez sur **Modifier le mot de passe**.
   La fenêtre **Modifier le mot de passe** s'affiche.
3. Saisissez le mot de passe actuel.
4. Saisissez le nouveau mot de passe.
5. Saisissez à nouveau le nouveau mot de passe pour confirmation.
6. Cliquez sur **Modifier le mot de passe**.

Déconnexion de la console de gestion

Étapes

1. Dans le coin supérieur droit de la page **Tableau de bord**, cliquez sur le menu déroulant de connexion.
2. Cliquez sur **Déconnexion**.

7

Gestion des groupes et des configurations

La page **Groupes et configurations** vous permet de définir les politiques requises pour configurer vos périphériques. Vous pouvez créer des sous-groupes des politiques de groupe globales et classer les périphériques en fonction de vos besoins. Par exemple, les périphériques peuvent être regroupés selon la fonction professionnelle, le type de périphériques et ainsi de suite.

Pour chaque groupe, vous pouvez définir des politiques pour les systèmes d'exploitation suivants :

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

Les périphériques héritent des politiques dans l'ordre dans lequel elles sont créées. Les paramètres configurés dans un groupe de politiques par défaut sont appliqués comme paramètres par défaut à toutes les politiques répertoriées dans le groupe de politiques par défaut. Dans un groupe, tous les périphériques appartenant à ce groupe se voient attribuer le groupe de politiques par défaut comme paramètre par défaut.

Sur la page **Détails du périphérique**, vous pouvez créer une exception pour un périphérique du groupe, de sorte que celui-ci ait un sous-ensemble de politiques différentes des politiques par défaut du groupe.

La configuration d'un actif particulier contenant des détails sur les configurations (niveaux global, groupe et périphérique) s'affiche sur la page. L'option permettant de créer des exceptions est disponible sur la page. Les paramètres **Exception** s'appliquent uniquement aux périphériques sélectionnés.

REMARQUE : Lorsque vous modifiez des politiques de niveau inférieur, une puce s'affiche en regard de la politique. Ce symbole indique que la politique déroge à une politique de niveau plus élevé. Par exemple, pour la personnalisation du système, le réseau, la sécurité et ainsi de suite. Lorsque vous modifiez des politiques, un astérisque (*) s'affiche en regard de la politique. Ce symbole indique que les modifications ne sont pas enregistrées ou qu'elles n'ont pas été publiées. Pour consulter ces modifications avant de les publier, cliquez sur le lien **Afficher les changements en attente**.

Si une configuration de politique doit avoir la priorité entre les différents niveaux, alors la politique ayant le niveau le plus bas aura la priorité.

Une fois que vous avez configuré les paramètres de la politique, les Thin Clients sont informés des changements. Les modifications prennent effet immédiatement après la configuration des Thin Clients.

REMARQUE : Certains paramètres, tels que la configuration du BIOS pour Windows Embedded Standard, nécessitent un redémarrage pour que les modifications prennent effet. Toutefois, pour la plupart des paramètres sur ThinOS, vous devez redémarrer le périphérique pour que les modifications prennent effet.

Les politiques sont appliquées avec la priorité indiquée ci-dessous :

- Politique de niveau global
- Politique de niveau groupe de périphériques
- Exceptions de périphériques
- Politique de niveau groupe d'utilisateurs
- Exceptions d'utilisateurs
- Personnalisation d'utilisateurs

Les configurations telles que le fond d'écran ou la politique de firmware appliquées au groupe de périphériques par défaut sont appliquées par défaut aux groupes enfants. Vous pouvez remplacer ces configurations pour les groupes enfants à partir de Wyse Management Suite 3.2.

Sujets :

Modifier un groupe non géré

Les appareils qui appartiennent au groupe non géré n'utilisent pas de licences ou ne reçoivent pas de configuration ni de politiques basées sur l'application. Pour ajouter des appareils à un groupe non géré, utilisez la clé d'enregistrement des appareils du groupe non géré pour l'enregistrement automatique ou l'enregistrement manuel des appareils.

Étapes

1. Sur la page **Groupes et configurations**, sélectionnez **Groupe non géré**.
2. Cliquez sur .
   La page **Modification d'un groupe non géré** s'affiche. Le champ **Nom du groupe** affiche le nom du groupe.
3. Modifiez les éléments suivants :
   - **Description** : fournit une brève description du groupe.
   - **Jeton de groupe** : sélectionnez cette option pour activer le jeton de groupe.
4. Cliquez sur **Enregistrer**.

   REMARQUE : Pour un cloud public, le jeton de groupe d'un groupe non géré doit être activé pour pouvoir y enregistrer les périphériques. Pour un cloud privé, le jeton de groupe d'un groupe non géré est automatiquement activé.

Créer un groupe de politiques de périphérique par défaut

Vous pouvez créer des groupes de politiques de groupe de périphériques globales et classer les appareils en fonction de vos besoins.

Étapes

1. Sur la page **Groupes et configurations**, cliquez sur l'option **Groupe de politiques de périphérique par défaut**.
2. Cliquez sur .
3. Dans la boîte de dialogue **Ajouter un groupe**, renseignez les champs **Nom du groupe** et **Description**.
4. Sélectionnez l'option **Il s'agit d'un groupe de sélections ThinOS parent** pour créer un groupe de sélections parent pour les appareils ThinOS. Cette étape est facultative.

   Pour plus d'informations, voir Créer un groupe de sélections ThinOS.
5. Dans l'onglet **Enregistrement**, cochez la case **Activé** sous Jeton de groupe.

6. Saisissez le jeton de groupe.
7. Dans l'onglet **Administration**, vous pouvez sélectionner le nom des administrateurs du groupe qui sont chargés de gérer ce groupe. Dans la zone **Administrateurs de groupe disponibles**, sélectionnez le groupe spécifique et cliquez sur la flèche droite pour le déplacer vers la zone **Administrateurs de groupe affectés**. Pour déplacer un groupe de la zone **Administrateurs de groupe affectés** vers la zone **Administrateurs de groupe disponibles**, faites l'inverse. Cette étape est facultative.
8. Cliquez sur **Enregistrer**.

   Le groupe est ajouté à la liste des groupes disponibles sur la page **Groupes et configurations**.

   REMARQUE : Pour enregistrer les appareils dans un groupe, saisissez le jeton de groupe qui est disponible sur la page **Groupes et configurations** pour le groupe correspondant.

Créer un groupe de sélections ThinOS

Étapes

1. Sur la page **Groupes et configurations**, cliquez sur l'option **Groupe de politiques de périphérique par défaut**.
2. Cliquez sur +.
3. Dans la boîte de dialogue **Ajouter un groupe**, renseignez les champs **Nom du groupe** et **Description**.
4. Sélectionnez l'option **Il s'agit d'un groupe de sélections ThinOS parent**.
5. Sélectionnez le nom des administrateurs de groupe qui sont chargés de la gestion de ce groupe. Dans la zone **Administrateurs de groupe disponibles**, sélectionnez le groupe spécifique et cliquez sur la flèche droite pour le déplacer vers la zone **Administrateurs de groupe affectés**. Pour déplacer un groupe de la zone **Administrateurs de groupe affectés** vers la zone **Administrateurs de groupe disponibles**, faites l'inverse. Cette étape est facultative.
6. Cliquez sur **Enregistrer**.

   Le groupe est ajouté à la liste des groupes disponibles sur la page **Groupes et configurations**.

   Pour ajouter des sous-groupes au groupe parent créé, cliquez sur le groupe parent sur la page **Groupes et configurations**, puis suivez les étapes décrites dans la section Créer un groupe de politiques d'appareil.

   REMARQUE : Le groupe de sélections parent peut avoir 10 groupes de sélections enfants et vous pouvez enregistrer les appareils dans un groupe de sélections enfant. Les profils peuvent être configurés pour d'autres systèmes d'exploitation. Les profils créés sont les mêmes que ceux des autres groupes personnalisés.

   REMARQUE : Certaines politiques qui sont modifiées dans les sous-groupes nécessitent un redémarrage du client pour que les changements prennent effet.

Modifier un groupe de politiques d'appareil par défaut

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez le **groupe de politiques d'appareil par défaut**.
2. Dans la boîte de dialogue **Modifier le groupe de politiques d'appareil par défaut**, modifiez les informations de groupe requises.
3. Cliquez sur **Enregistrer**.

Modifier un groupe de sélections ThinOS

Étapes

1. Accédez à la page **Groupes et configurations**, puis cliquez sur le groupe de sélections ThinOS que vous souhaitez modifier.
2. Cliquez sur .
3. Dans la boîte de dialogue **Modification d'un groupe de politiques par défaut**, modifiez les informations du groupe, telles que le **nom du groupe** et la **description**.
4. Dans l'onglet **Administration**, sélectionnez le nom des administrateurs de groupe qui sont chargés de gérer ce groupe. Dans la zone **Administrateurs de groupe disponibles**, sélectionnez le groupe spécifique et cliquez sur la flèche droite pour le déplacer vers la

zone **Administrateurs de groupe affectés**. Pour déplacer un groupe de la zone **Administrateurs de groupe affectés** vers la zone **Administrateurs de groupe disponibles**, cliquez sur la flèche de gauche. Cette étape est facultative.

5. Cliquez sur **Enregistrer**.

Supprimer un groupe de sélections ThinOS

En tant qu'administrateur, vous pouvez supprimer un groupe de la hiérarchie de groupes.

Étapes

1. Dans la page **Groupes et configurations**, sélectionnez le groupe de sélections ThinOS à supprimer.
2. Cliquez sur  .
   Un message d'avertissement indiquant que cette action supprime un ou plusieurs groupes de la hiérarchie d'arborescence de groupe s'affiche.
3. Dans la liste déroulante des groupes, sélectionnez un nouveau groupe cible pour les utilisateurs et les périphériques du groupe actuel.
4. Cliquez sur **Supprimer le groupe**.

   REMARQUE : Lorsque vous supprimez un groupe de la hiérarchie de groupes, tous les utilisateurs et périphériques qui appartiennent au groupe supprimé sont transférés vers le groupe personnalisé, par défaut ou non géré.

   REMARQUE : Lorsque vous supprimez le groupe de sélections, les périphériques du groupe supprimé ne peuvent pas être déplacés vers un autre groupe de sélections.

Créer un groupe de politiques d'utilisateur

Vous pouvez créer des groupes pour les groupes de politiques d'utilisateur globales et classer les utilisateurs et les appareils en fonction de leurs groupes d'utilisateurs.

Étapes

1. Sur la page **Groupes et configurations**, cliquez sur l'option **Groupe de politiques d'utilisateur par défaut**.
2. Cliquez sur  .
3. Dans la boîte de dialogue **Ajouter un nouveau groupe**, saisissez le **nom du groupe**, la **Description**, le **Domaine**, l'**attribut AD** (groupe AD ou groupe OU) et le **Nom de l'attribut AD** qui est le nom présent dans le domaine AD. Vous devez utiliser le **Nom du groupe** comme **Nom d'attribut AD**.

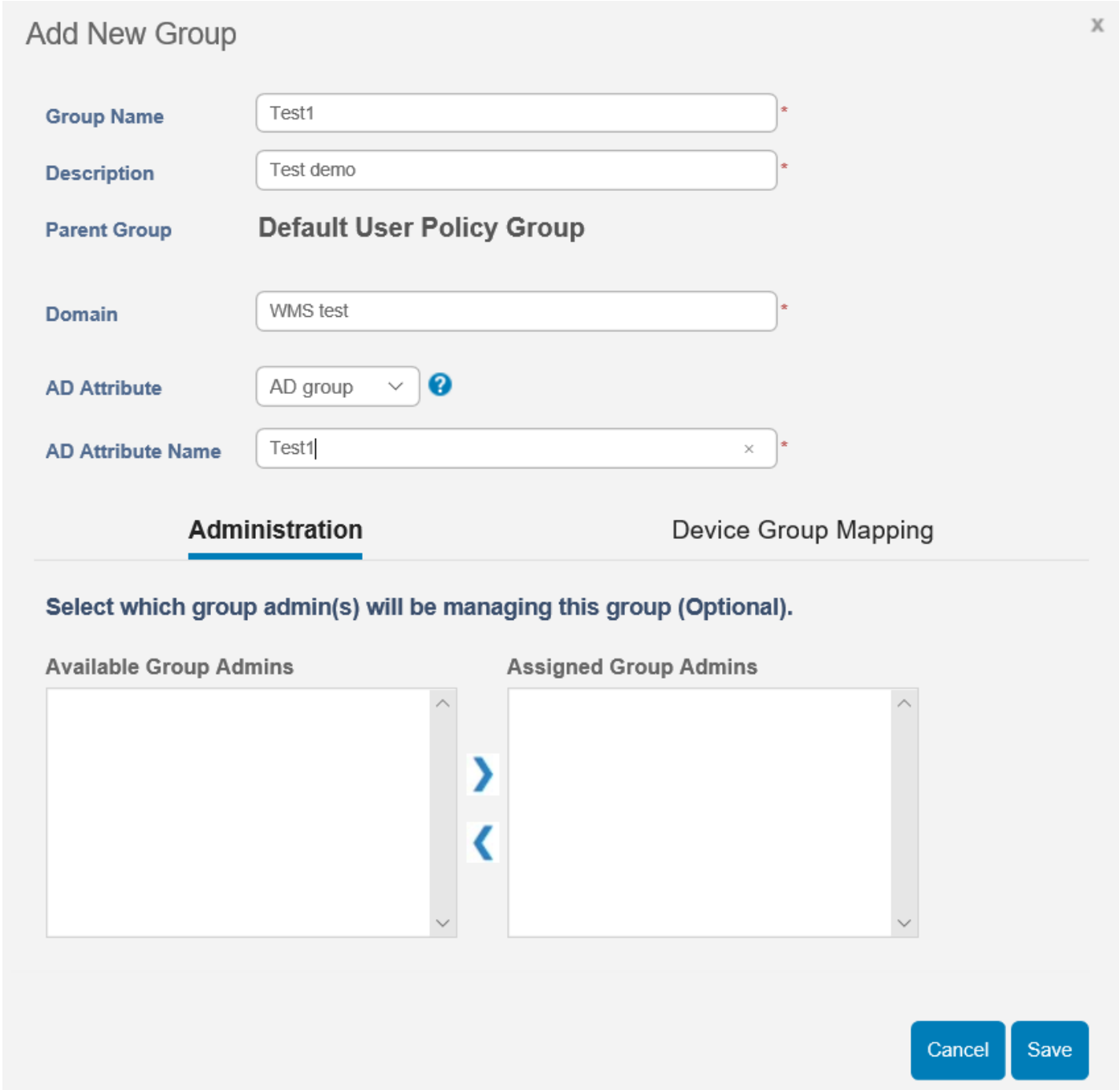


Figure 4. Ajouter un nouveau groupe

REMARQUE : Si le groupe AD est à l'intérieur d'un groupe OU dans le domaine, il vous faut alors sélectionner le groupe OU comme attribut AD.

4. Sélectionnez le nom des administrateurs de groupe qui sont chargés de la gestion de ce groupe.
5. Dans la zone **Administrateurs de groupe disponibles**, sélectionnez le groupe spécifique et cliquez sur la flèche droite pour le déplacer vers la zone **Administrateurs de groupe affectés**.

   Pour déplacer un groupe de la zone **Administrateurs de groupe affectés** vers la zone **Administrateurs de groupe disponibles**, faites l'inverse.
6. Cliquez sur **Enregistrer**.

   Le groupe est ajouté à la liste des groupes disponibles sur la page **Groupes et configurations**.

REMARQUE : Un groupe de politiques d'utilisateur doit être mappé à un groupe AD ou une unité d'organisation, mais pas aux deux.

7. Sélectionnez l'option **Mappage de groupe de périphériques** pour importer des groupes d'utilisateurs avec le mappage de périphérique afin de contrôler les configurations appliquées à tous les groupes de périphériques par défaut.

   Les groupes d'utilisateurs AD qui sont importés dans Wyse Management Suite peuvent être mappés au groupe de périphériques correspondant. En mappant les périphériques, ils ne reçoivent pas de politiques de groupes d'utilisateurs indésirables.

   REMARQUE : Par défaut, les groupes d'utilisateurs ne sont pas mappés à un groupe de périphériques. Si vous sélectionnez la politique **Groupe de périphériques par défaut**, tous les groupes de sous-périphériques sont sélectionnés. Cette fonctionnalité n'est disponible que sur la licence Pro de Wyse Management Suite. Vous pouvez importer 100 groupes d'utilisateurs vers Wyse Management Suite.

Modifier un groupe de politiques d'utilisateur

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez le groupe de politiques d'utilisateur par défaut.
2. Cliquez sur .
3. Dans la boîte de dialogue **Modifier le groupe de politiques d'utilisateur par défaut**, modifiez les informations de groupe requises.
4. Cliquez sur **Enregistrer**.

Configurer une politique de niveau global

Étapes

1. Sur la page **Groupes et configurations**, dans le menu déroulant **Modifier les politiques**, sélectionnez un type de périphérique.

   Les paramètres de politique de chaque type de périphérique sont affichés.
2. Sélectionnez le paramètre de politique à configurer, puis cliquez sur **Configurer cet élément**.
3. Après avoir configuré les options, cliquez sur **Enregistrer et Publier**.

Importer un groupe de politiques d'utilisateur

Étapes

1. Sur la page **Groupes et configurations**, cliquez sur l'option **Groupe de politiques d'utilisateur par défaut**.
2. Cliquez sur .
3. Dans la boîte de dialogue **Importation en bloc**, cliquez sur **Parcourir** et sélectionnez le fichier .csv.

   Le fichier.csv doit contenir les informations dans l'ordre indiqué ci-dessous :
   - Nom du groupe : nom d'affichage
   - Description
   - Domaine : nom du domaine
   - Attribut AD : groupe AD ou groupe OU
   - Nom d'attribut AD : nom de groupe présent dans le domaine AD

   REMARQUE : Vous devez utiliser le nom du groupe comme nom d'attribut AD. De plus, si le groupe AD est à l'intérieur d'un **groupe OU** dans le domaine, il vous faut alors sélectionner le **groupe OU** comme **attribut AD**.
4. Cochez la case **Le fichier CSV a une ligne d'en-tête** si le fichier .csv contient une ligne d'en-tête.
5. Cliquez sur **Importer**.

Supprimer un groupe

En tant qu'administrateur, vous pouvez supprimer un groupe de la hiérarchie de groupes.

Étapes

1. Dans la page **Groupes et configurations**, sélectionnez le groupe à supprimer.
2. Cliquez sur  .
   Un message d'avertissement indiquant que cette action supprime un ou plusieurs groupes de la hiérarchie d'arborescence de groupe s'affiche.
3. Dans la liste déroulante, sélectionnez un nouveau groupe pour déplacer les utilisateurs et les périphériques du groupe actuel.
4. Cliquez sur **Supprimer le groupe**.

   REMARQUE : Lorsqu'un groupe de périphériques est supprimé, tous les périphériques du groupe sont déplacés vers un groupe de périphériques sélectionné. Lorsqu'un groupe d'utilisateurs est supprimé, aucun périphérique ou utilisateur n'est associé à celui-ci.

Configurer la politique de niveau appareil

Étapes

1. Dans la page **Appareils**, cliquez sur l'appareil que vous souhaitez configurer.
   La page **Détails de l'appareil** s'affiche.
2. Dans la section **Configuration de l'appareil**, cliquez sur **Créer/modifier des exceptions**.

Exportation des politiques de groupe

L'option **Exporter les politiques** vous permet d'exporter les politiques du groupe actuel. Cette option est disponible pour les utilisateurs de licences Pro de Wyse Management Suite.

Étapes

1. Dans la page **Groupes et configurations**, sélectionnez le groupe à partir duquel vous souhaitez exporter des politiques. Le groupe doit avoir des politiques configurées.
2. Cliquez sur **Exporter les politiques**.
   L'écran **Exporter les politiques** s'affiche.
3. Sélectionnez les politiques de type de périphérique à exporter.
   Les options disponibles sont les suivantes :
   - Toutes les politiques de type de périphérique : toutes les politiques de type de périphérique sont exportées.
   - Politiques de type de périphérique spécifiques : sélectionnez un ou plusieurs types de périphériques dans la liste déroulante. Seules les politiques de type de périphérique sélectionnées sont exportées.
4. Cliquez sur le bouton **Oui** pour exporter les politiques de type de périphérique sélectionnées.
   Les politiques de groupe parent ne sont pas exportées. Seules les politiques qui sont configurées au niveau du groupe cible ou sélectionné sont exportées.
5. Cliquez sur le lien de téléchargement ou cliquez avec le bouton droit de la souris sur le fichier, puis cliquez sur **Enregistrer sous** pour enregistrer le fichier `JSON` .

   REMARQUE : Les mots de passe sont chiffrés dans le fichier exporté. Le nom de fichier est au format `[Group Name]-[ALL]-[Exported Date & Time]UTC.json`.

   REMARQUE : Pour éviter l'échec des politiques d'importation, assurez-vous de supprimer les mots de passe et toute référence à des fichiers tels que le certificat, le fond d'écran, le firmware, le logo, etc. avant de procéder à l'exportation vers un fichier.

Importation des politiques de groupe

L'option **Importer les politiques** vous permet d'importer les politiques. Cette option est disponible pour les utilisateurs de licences PRO de Wyse Management Suite. Vous pouvez importer des politiques de groupe à partir de la page **Groupes et configurations** ou de la page **Modifier les politiques**.

Importer des politiques de groupe à partir de la page Groupes et configurations

Étapes

1. Dans la page **Groupes et configurations**, sélectionnez le groupe de votre choix.

   Si le groupe de destination contient les mêmes politiques de type De périphériques que celles importées, les politiques sont supprimées et les nouvelles politiques sont ajoutées.
2. Cliquez sur **Importer les politiques**.
   L'écran **Assistant d'importation de politiques** s'affiche.
3. Sélectionnez le mode d'importation des politiques de groupe à partir du groupe sélectionné.
   Les options disponibles sont les suivantes :
   - À partir d'un groupe existant : sélectionnez un groupe dans la liste déroulante. Les politiques de ce groupe sont copiées vers le groupe actuel.
   - Depuis un fichier d'exportation : accédez au fichier `.json`. Les politiques de ce fichier sont copiées vers le groupe actuel.
4. Cliquez sur **Suivant**.
5. Sélectionnez les configurations de type de périphérique à importer.
   Les options disponibles sont les suivantes :
   - Toutes les politiques de type de périphérique : toutes les politiques de type de périphérique configuré sont importées vers le groupe actuel.
   - Politiques de type de périphérique spécifiques : sélectionnez un ou plusieurs types de périphériques dans la liste déroulante. Seules les politiques de type de périphérique sélectionnées sont importées vers le groupe actuel.
6. Cliquez sur **Suivant**.
   Un aperçu des politiques du groupe sélectionné s'affiche.
7. Cliquez sur **Suivant**.

   Le résumé du processus d'importation s'affiche. Les types d'avertissement suivants peuvent s'afficher :
   - **Les politiques de <type de système d'exploitation> importées sont appliquées au groupe <nom du groupe>** : cet avertissement s'affiche lorsque vous importez les configurations du système d'exploitation vers un groupe qui ne contient aucune des configurations.
   - **Les politiques de <type de système d'exploitation> existent déjà pour le groupe <nom du groupe>. Les politiques existantes de <type de système d'exploitation> sont supprimées et les nouvelles politiques sont appliquées** : cet avertissement s'affiche lorsque vous importez les nouvelles configurations du type de système d'exploitation vers un groupe qui contient les configurations du type de système d'exploitation.
   - **L'importation des politiques depuis un fichier qui contient les dépendances vers les fichiers d'inventaire a échoué. Pour que cette importation réussisse, utilisez l'option Importer dans la fenêtre « Modifier les politiques »** : cet avertissement s'affiche lorsque vous importez les configurations de type de périphériques à partir d'un fichier qui contient des références vers des fichiers d'inventaire.
8. Cliquez sur **Importer**.

   REMARQUE : Seules les configurations de type de périphérique sélectionnées peuvent être importées. Les politiques qui sont définies dans le groupe cible pour le type de périphériques sélectionné sont supprimées avant d'appliquer les nouvelles politiques du même type de périphériques.

   REMARQUE : Lors de l'importation des polices de groupe, les mots de passe et les fichiers de référence ne sont pas importés. L'administrateur doit les sélectionner avant de publier la politique.

Importer des politiques de groupe à partir de la page Modifier les politiques

Étapes

1. Dans la page **Groupes et configurations**, sélectionnez le groupe de votre choix.
2. Cliquez sur **Modifier les politiques**, puis sélectionnez l'option de votre choix.
3. Cliquez sur **Importer**.
   L'écran **Assistant d'importation de politiques** s'affiche.
4. Sélectionnez le mode d'importation des politiques de groupe à partir du groupe sélectionné. Les options disponibles sont les suivantes :
   - À partir d'un groupe existant : sélectionnez un groupe dans la liste déroulante. Les politiques de ce groupe sont copiées vers le groupe actuel.
   - À partir d'un fichier exporté : cliquez sur **Parcourir** et sélectionnez le fichier `.JSON`. Les politiques de ce fichier sont copiées vers le groupe actuel.
5. Cliquez sur **Suivant**.
   Un aperçu des politiques du groupe sélectionné s'affiche.
6. Cliquez sur **Suivant**. Le résumé du processus d'importation s'affiche. Les types d'avertissement suivants peuvent s'afficher :
   - **Les politiques de <type de périphérique> importées sont appliquées au groupe <nom du groupe>** : cet avertissement s'affiche lorsque vous importez les configurations de type de périphérique vers un groupe qui ne contient aucune de ces configurations de type de périphérique.
   - **Les politiques de <type de périphérique> existent déjà pour le groupe <nom du groupe>. Les politiques existantes de <type de périphérique> sont supprimées et les politiques importées sont appliquées** : cet avertissement s'affiche lorsque vous importez les configurations de type de périphérique vers un groupe qui contient les mêmes configurations de type de périphérique.
   - **L'importation des politiques depuis un fichier qui contient les dépendances vers les fichiers d'inventaire a échoué. Pour que cette importation réussisse, utilisez l'option Importer dans la fenêtre « Modifier les politiques »** : cet avertissement s'affiche lorsque vous importez les configurations de type de périphérique à partir d'un fichier qui contient des références vers des fichiers d'inventaire.
7. Cliquez sur **Importer**.

   REMARQUE : Lorsque vous importez une politique depuis un fichier, et s'il existe des références ou des dépendances non valides, l'importation échoue et un message d'erreur s'affiche. En outre, si le fichier à importer possède un fichier de référence ou de dépendance, accédez à la page **Modifier la politique** du type de périphérique respectif, puis importez les politiques de groupe.

   REMARQUE : Vous pouvez importer ou exporter des politiques de groupe d'un périphérique à un groupe d'utilisateurs et vice versa en utilisant un fichier ou d'un groupe à un autre. Les configurations non prises en charge telles que BIOS, Jonction de domaine, etc. sont ignorées lorsque vous importez des configurations dans un groupe d'utilisateurs.

Résultats

Si le groupe de destination contient les mêmes politiques de type de périphérique que celles importées, les politiques sont supprimées et les nouvelles politiques sont ajoutées.

REMARQUE : Lors de l'importation des politiques de groupe, les mots de passe ne sont pas importés. L'administrateur doit saisir à nouveau le mot de passe dans tous les champs de mot de passe.

Modifier les paramètres de la politique ThinOS

Étapes

1. Cliquez sur **Groupes & configurations**.
   La page **Groupes et configurations** s'affiche.
2. Cliquez sur le menu déroulant **Modifier les politiques**.
3. Cliquez sur **ThinOS**.
   La fenêtre **Sélectionner le mode de configuration de ThinOS** s'affiche.
4. Sélectionnez votre mode préféré pour configurer les paramètres de politique. Les modes disponibles sont les suivants :
   - Mode Assistant

- Mode Configuration avancée

REMARQUE : pour définir la configuration avancée ThinOS comme mode par défaut, cochez la case correspondante.

5. Après avoir configuré les paramètres de politique, cliquez sur **Enregistrer et Publier**.

REMARQUE : Le client léger redémarre si vous effectuez des modifications avec les paramètres suivants :

- Paramètres du BIOS
- DP audio
- Fenêtre contextuelle de la prise
- Nom de terminal
- Vitesse Ethernet
- Modification de l'affichage : résolution, pivoter, actualiser, double affichage et multi-écrans
- Mode du système : VDI, StoreFront, et Classic
- Liaison du port LPT

ThinOS : Mode Assistant

Utilisez cette page pour configurer les paramètres les plus fréquemment utilisés sur les appareils ThinOS.

Étapes

1. Sélectionnez **Assistant** comme mode de configuration.
2. Configurez les options selon vos besoins.
3. Cliquez sur **Suivant** pour accéder au prochain paramètre de politique.
4. Cliquez sur **Enregistrer et publier** après avoir configuré les options.

REMARQUE : Pour passer au mode de configuration avancée ThinOS, cliquez sur **Continuer**.

ThinOS : Mode avancé

Utilisez cette page pour configurer les paramètres de politique avancés des appareils ThinOS.

Étapes

1. Sélectionnez **Configuration avancée** comme mode de configuration.
2. Configurez les options selon vos besoins.
3. Cliquez sur **Enregistrer et publier** pour enregistrer et publier votre configuration.

REMARQUE : Pour revenir à la page **ThinOS**, cliquez sur **Supprimer la politique**.

Modifier les paramètres de la politique ThinOS 9.x

Prérequis

- Créez un groupe avec un jeton de groupe pour les appareils pour lesquels vous souhaitez transmettre le package d'application.
- Enregistrez le client léger dans Wyse Management Suite.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **ThinOS 9.x**.
   La fenêtre **Contrôle de configuration | ThinOS** s'affiche.

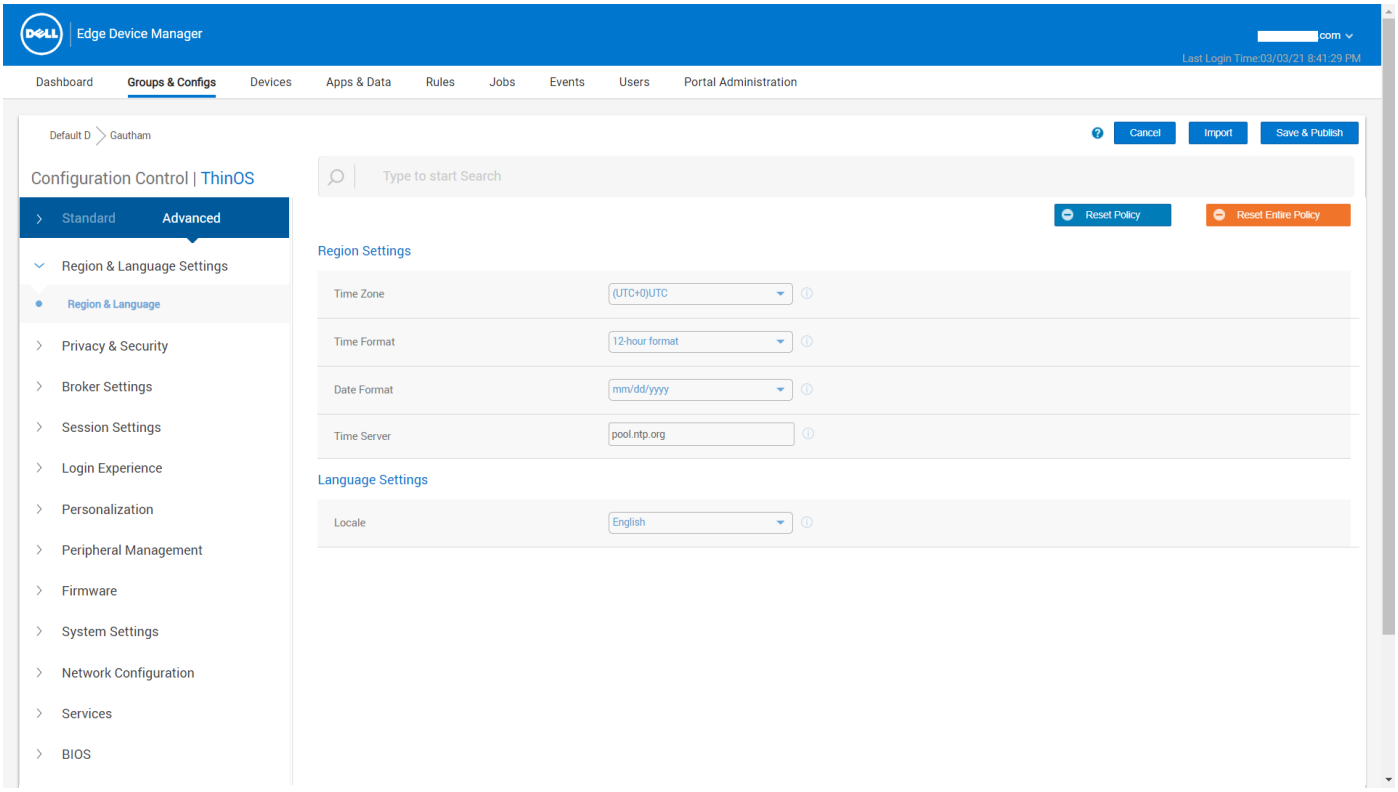


Figure 5. Contrôle de la configuration | ThinOS

3. Cliquez sur l'option **Avancé** ou **Standard**.
4. Sélectionnez les options à configurer.
5. Dans les champs correspondants, cliquez sur l'option que vous souhaitez configurer.

   Vous pouvez utiliser l'option de recherche globale pour trouver les paramètres pertinents disponibles dans les paramètres de la politique. Le résultat de la recherche affiche les paramètres dans l'ordre suivant :
   - Réglage
   - Groupe de paramètres
   - Sous-groupe de paramètres
   - Paramètre
6. Configurez les options selon vos besoins.

   REMARQUE : Vous pouvez cliquer sur l'option **Réinitialiser la politique** à partir de Wyse Management Suite 3.2 si vous souhaitez réinitialiser la politique sur les configurations par défaut. Vous pouvez également cliquer sur l'option **Réinitialiser la politique dans son intégralité** si vous souhaitez effacer toutes les configurations.
7. Cliquez sur **Enregistrer et publier**.

   REMARQUE : Une fois que vous avez cliqué sur **Enregistrer et publier**, les paramètres configurés s'affichent également dans l'onglet **Standard**.

   REMARQUE : Les configurations de la politique avec un fichier de référence tel que le firmware, le package, le fond d'écran, etc. appliquées au groupe parent, par exemple le groupe de périphériques par défaut, sont appliquées par défaut aux groupes enfants. Vous pouvez remplacer ces configurations et les supprimer des groupes enfants à partir de Wyse Management Suite 3.2.

   REMARQUE : Vous pouvez uniquement télécharger et déployer 10 certificats, fonds d'écran et fichiers de référence depuis la fenêtre **Contrôle de configuration | ThinOS**.

Configurations du BIOS pour ThinOS 9.x

À propos de cette tâche

Vous pouvez configurer les paramètres de configuration du BIOS sur des appareils ThinOS 9.x à l'aide de Wyse Management Suite 2.1. Vous pouvez déployer les packages du BIOS à l'aide de la page **Groupes et configurations** ou à l'aide de l'option de mappage de sous-réseau.

REMARQUE : Cette fonctionnalité n'est disponible qu'avec la licence Pro de Wyse Management Suite.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
   La fenêtre Contrôle de configuration | ThinOS s'affiche.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **ThinOS 9.x**.
3. Cliquez sur **Avancé**.
4. Dans le champ **BIOS**, cliquez sur **Sélectionner la plate-forme** pour choisir la plate-forme sur laquelle vous souhaitez configurer les paramètres du BIOS.

Mise à niveau de ThinOS 9.x vers des versions supérieures à l'aide de Wyse Management Suite

Prérequis

- Assurez-vous d'avoir créé un groupe à l'aide d'un jeton de groupe. Utilisez ce jeton de groupe pour enregistrer les appareils ThinOS 9.x.
- Assurez-vous que le client léger est enregistré auprès de Wyse Management Suite.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **ThinOS 9.x**.
   La fenêtre **Contrôle de configuration | ThinOS** s'affiche.
3. Cliquez sur **Avancé**.
4. Dans le champ **Firmware**, sélectionnez **Mises à jour du firmware du OS**.
5. Cliquez sur **Parcourir** pour localiser et télécharger le firmware.
   Les détails du contrat EULA du package et le nom des fournisseurs s'affichent.
6. Pour sélectionner un fichier, cliquez sur **Parcourir** et accédez à l'emplacement où se trouve votre firmware.
   - Si le contrat EULA est intégré dans le package, les détails du contrat EULA du package et le nom des fournisseurs s'affichent. Vous pouvez cliquer sur les noms des fournisseurs pour lire le contrat de licence de chaque fournisseur. Cliquez sur **Accepter** pour charger le package. Si vous chargez plusieurs packages, les détails du contrat EULA de chaque package s'affichent. Vous devez accepter le contrat de licence des packages individuellement.
   - Si vous n'acceptez pas le contrat EULA, le firmware n'est pas installé.

   REMARQUE : Vous pouvez télécharger et déployer plusieurs packages de firmware à partir du référentiel distant, du référentiel Cloud du client ou du référentiel Cloud de l'opérateur.
7. Dans le menu déroulant **Sélectionner le firmware ThinOS à déployer**, sélectionnez le firmware téléchargé.

   REMARQUE : Vous pouvez télécharger et déployer plusieurs packages de firmware à partir du référentiel distant, du référentiel Cloud du client ou du référentiel Cloud de l'opérateur.
8. Cliquez sur **Enregistrer et publier**.
   Le client léger télécharge le firmware et redémarre. La version du firmware est mise à niveau.

Télécharger et envoyer des packages du BIOS

Prérequis

- Créez un groupe dans Wyse Management Suite à l'aide d'un jeton de groupe. Utilisez ce jeton de groupe pour enregistrer les appareils ThinOS 9.x.
- Enregistrez le client léger dans Wyse Management Suite.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **ThinOS 9.x**.
   La fenêtre Contrôle de configuration | ThinOS s'affiche.
3. Cliquez sur **Avancé**.
4. Dans le champ **Firmware**, sélectionnez **Mises à jour du firmware du BIOS**.
5. Dans le menu déroulant **Sélectionner le BIOS ThinOS à déployer**, sélectionnez le package.

   REMARQUE : Vous pouvez télécharger et déployer plusieurs packages de firmware à partir du référentiel distant, du référentiel Cloud du locataire ou du référentiel Cloud de l'opérateur. Vous pouvez télécharger 10 packages à partir du référentiel Cloud du locataire.

6. Cliquez sur **Enregistrer et publier**.
   Le client léger redémarre et le package d'application est installé.

   Vous pouvez également télécharger le firmware du BIOS à partir des **Applications et données** sur Wyse Management Suite 2.1 comme indiqué dans les étapes suivantes :
   a. Accédez à la page **Applications et données**.
   b. Cliquez sur **Référentiel d'images SE** et sélectionnez **ThinOS 9.x**.
   c. Cliquez sur **Ajouter un fichier de BIOS** pour parcourir et ajouter le fichier que vous souhaitez ajouter au référentiel.

   REMARQUE : Cette fonctionnalité n'est disponible que sur la licence Pro de Wyse Management Suite.

Téléchargement et envoi des packages d'application ThinOS 9.x à l'aide des groupes et configurations

Prérequis

- Assurez-vous d'avoir créé un groupe à l'aide d'un jeton de groupe. Utilisez ce jeton de groupe pour enregistrer les appareils ThinOS 9.x.
- Enregistrez le client léger dans Wyse Management Suite.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **ThinOS 9.x**.
   La fenêtre **Contrôle de configuration | ThinOS** s'affiche.
3. Cliquez sur **Avancé**.
4. Dans le champ **Firmware**, cliquez sur **Mises à jour du package d'application**.
5. Pour sélectionner un fichier, cliquez sur **Parcourir** et accédez à l'emplacement où se trouve votre fichier.
   - Si le contrat EULA est intégré dans le package, les détails du contrat EULA du package et le nom des fournisseurs s'affichent. Vous pouvez cliquer sur les noms des fournisseurs pour lire le contrat de licence de chaque fournisseur. Cliquez sur **Accepter** pour charger le package. Si vous chargez plusieurs packages, les détails du contrat EULA de chaque package s'affichent. Vous devez accepter le contrat de licence des packages individuellement.
   - Si le contrat EULA n'est pas intégré dans le package, passez à l'étape 6.

   REMARQUE : Vous pouvez télécharger et déployer plusieurs packages de firmware à partir du référentiel distant, du référentiel Cloud du client ou du référentiel Cloud de l'opérateur.

6. Dans le menu déroulant **Sélectionner le(s) package(s) ThinOS à déployer**, sélectionnez le package.
7. Cliquez sur **Enregistrer et publier**.
   Le client léger redémarre et le package d'application est installé.

Modifier les paramètres d'une politique Windows Embedded Standard

Étapes

1. Cliquez sur **Groupes & configurations**.
   La page **Groupes et configurations** s'affiche.
2. Cliquez sur le menu déroulant **Modifier les politiques**.
3. Cliquez sur **WES**.
   La page **WES** s'affiche.
4. Après avoir configuré les paramètres de politique, cliquez sur **Enregistrer et Publier**.

Configuration des paramètres de déploiement d'appareils Windows Embedded

À partir de Wyse Management Suite 3.1, vous pouvez configurer les paramètres de déploiement pour des appareils Windows Embedded. Vous pouvez configurer les paramètres pour déployer en mode silencieux les configurations sur les appareils.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **WES** ou **ThinLinux**.
3. Cliquez sur **Paramètres de déploiement**.
4. Cliquez sur **Configurer cet élément**.
5. Configurez les options ci-dessous :
   - **Activer/désactiver toutes les notifications** : si vous désactivez cette option, toutes les options et notifications sont désactivées.
   - **Configurer la notification de mise à jour** : si vous désactivez cette option, la boîte de dialogue de mise à jour de la configuration ne s'affiche pas sur l'appareil.
   - **Notification de mise à jour de l'application** : si vous désactivez cette option, la notification de l'utilisateur ne s'affiche pas lorsque vous déployez une politique d'application.
   - **Notification de mise à jour d'image** : si vous désactivez cette option, la notification de l'utilisateur ne s'affiche pas lorsque vous déployez une politique d'image.
   - **Notification de déconnexion** : si vous désactivez cette option, la notification de l'utilisateur ne s'affiche pas lorsqu'un utilisateur se déconnecte de l'appareil.
   - **Notification de redémarrage** : si vous désactivez cette option, la notification de l'utilisateur ne s'affiche pas lorsque la configuration de redémarrage de l'appareil est déployée.
   - **Afficher l'écran de verrouillage** : si vous désactivez cette option, l'écran de verrouillage ne s'affiche pas pendant les mises à jour de l'application et de l'image.

   REMARQUE : Toutes les options sont activées par défaut.
6. Cliquez sur **Enregistrer et publier**.

Modifier les paramètres de la politique Linux

Étapes

1. Cliquez sur **Groupes & configurations**.
   La page **Groupes et configurations** s'affiche.
2. Cliquez sur le menu déroulant **Modifier les politiques**.
3. Cliquez sur **Linux**.
4. Après avoir configuré les paramètres de politique, cliquez sur **Enregistrer et Publier**.

Modifier les paramètres de la politique ThinLinux

Étapes

1. Cliquez sur **Groupes & configurations**.
   La page **Groupes et configurations** s'affiche.
2. Cliquez sur le menu déroulant **Modifier les politiques**.
3. Cliquez sur **ThinLinux**.
4. Après avoir configuré les paramètres de politique, cliquez sur **Enregistrer et Publier**.

Configuration des paramètres de déploiement pour les appareils ThinLinux

À partir de Wyse Management Suite 3.1, vous pouvez configurer les paramètres de déploiement pour des appareils ThinLinux. Vous pouvez configurer les paramètres pour déployer en mode silencieux les configurations sur les appareils.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **ThinLinux**.
3. Cliquez sur **Paramètres de déploiement**.
4. Cliquez sur **Configurer cet élément**.
5. Configurez l'une des options suivantes :
   - **Activer/désactiver toutes les notifications** : si vous désactivez cette option, toutes les options et notifications sont désactivées.
   - **Configurer la notification de mise à jour** : si vous désactivez cette option, la boîte de dialogue de mise à jour de la configuration ne s'affiche pas sur l'appareil.
   - **Notification de mise à jour de l'application** : si vous désactivez cette option, la notification de l'utilisateur ne s'affiche pas lorsque vous déployez une politique d'application.
   - **Notification de mise à jour d'image** : si vous désactivez cette option, la notification de l'utilisateur ne s'affiche pas lorsque vous déployez une politique d'image.
   - **Notification de déconnexion** : si vous désactivez cette option, la notification de l'utilisateur ne s'affiche pas lorsqu'un utilisateur se déconnecte de l'appareil.
   - **Notification de redémarrage** : si vous désactivez cette option, la notification de l'utilisateur ne s'affiche pas lorsque la configuration de redémarrage de l'appareil est déployée.
   - **Afficher l'écran de verrouillage** : si vous désactivez cette option, l'écran de verrouillage ne s'affiche pas pendant les mises à jour de l'application et de l'image.

   REMARQUE : Toutes les options sont activées par défaut.
6. Cliquez sur **Enregistrer et publier**.

Modifier les paramètres de la politique Thin Client Wyse Software

Étapes

1. Cliquez sur **Groupes & configurations**.
   La page **Groupes et configurations** s'affiche.
2. Cliquez sur le menu déroulant **Modifier les politiques**.
3. Cliquez sur **Thin Client Wyse Software**.
   La page **Thin Client Wyse Software** s'affiche.
4. Après avoir configuré les paramètres de politique, cliquez sur **Enregistrer et Publier**.

Modifier les paramètres de la politique Cloud Connect

Étapes

1. Cliquez sur **Groupes & configurations**.
   La page **Groupes et configurations** s'affiche.
2. Cliquez sur le menu déroulant **Modifier les politiques**.
3. Cliquez sur **Cloud Connect**.
4. Après avoir configuré les paramètres de politique, cliquez sur **Enregistrer et Publier**.

Modifier les paramètres de la politique de Dell Hybrid Client

Prérequis

- Créez un groupe avec un jeton de groupe pour les appareils pour lesquels vous souhaitez transmettre le package d'application.
- Enregistrez Dell Hybrid Client dans Wyse Management Suite.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **Client hybride**.
   La fenêtre **Contrôle de configuration | Client hybride** s'affiche.
3. Cliquez sur l'option **Avancé**.
4. Sélectionnez les options à configurer.
5. Dans les champs respectifs, cliquez sur le paramètre et configurez les options selon vos besoins.

   REMARQUE : Vous pouvez cliquer sur l'option **Réinitialiser la politique** si vous souhaitez réinitialiser la politique sur les configurations par défaut à partir de Wyse Management Suite 3.2. Vous pouvez également cliquer sur l'option **Réinitialiser la politique dans son intégralité** si vous souhaitez effacer toutes les configurations.

6. Cliquez sur **Enregistrer et publier**.

   REMARQUE : Une fois que vous avez cliqué sur **Enregistrer et publier**, les paramètres configurés s'affichent également dans l'onglet **Standard**.

   Le tableau suivant énumère l'ensemble des fonctionnalités que vous pouvez configurer dans la fenêtre **Contrôle de configuration | Client hybride**.

Tableau 5. Paramètres de la politique des clients hybrides

Fonctionnalité	Sous-fonctionnalité : groupe de politique des utilisateurs	Sous-fonctionnalité : groupe de politique des périphériques
Gestion périphérique	Paramètres d'affichage	Paramètres d'affichage
	Imprimantes	Imprimantes
	Audio	Audio
	Souris	Souris
	Clavier	Clavier
Configuration du réseau	Sans fil	Sans fil
		Proxy
		Bluetooth
Paramètres du navigateur	Paramètres de Google Chrome	Raccourcis du navigateur
	Paramètres de Firefox	

Tableau 5. Paramètres de la politique des clients hybrides

Fonctionnalité	Sous-fonctionnalité : groupe de politique des utilisateurs	Sous-fonctionnalité : groupe de politique des périphériques
	Raccourcis du navigateur	
	Navigateur par défaut	
Paramètres régionaux et linguistiques	Région	Région
		Serveurs de temps
		Langue
Personnalisation	Bureau	Bureau
		Informations sur le périphérique
SignOn	Non applicable	Jonction de domaine
		Liste d'utilisateurs précédemment connectés
Confidentialité et sécurité	Non applicable	Certificat
		Propriétés du compte utilisateur invité
		Verrouillage USB
		Mot de passe GRUB
		Mot de passe Bremen
		Serveur VNC
		Serveur SSH
Paramètres d'alimentation	Source d'économie d'énergie	Source d'économie d'énergie
	Bouton de suspension et d'alimentation	Bouton de suspension et d'alimentation
Espace de travail Citrix	Session broker Citrix	Session broker Citrix
	Paramètres globaux Citrix	Paramètres globaux Citrix
VMware ViewClient	Session broker VMware ViewClient	Session broker VMware ViewClient
	Paramètres globaux VMware	Paramètres globaux VMware
RDP	Session broker RDP	Session broker RDP
Mode Dell Hybrid Client	Mode Dell Hybrid Client	Mode Dell Hybrid Client
Paramètres WMS	Non applicable	Paramètres du client WMS
		Paramètres de déploiement
Sécurité des applications	VLC Media Player	VLC Media Player
	Visionneuse d'images	Visionneuse d'images
	Libre Office	Libre Office
Lecteurs réseau	Liste des lecteurs réseau	Liste des lecteurs réseau
BIOS	Non applicable	Sélectionnez votre plateforme : • DHC 3090 • DHC 3320 • DHC 5070 • DHC 7070 • DHC 7090

REMARQUE : N'utilisez pas de caractères spéciaux ou n'ajoutez pas d'espaces dans le nom du fichier de ressources, tels que les fichiers de fonds d'écran, de certificats, et de logos publicitaires.

Pour plus d'informations sur la manière de configurer Dell Hybrid Client, consultez le *guide de l'administrateur Dell Hybrid Client* à l'adresse www.dell.com/support.

Configurer les paramètres du client Wyse Management Suite pour Dell Hybrid Client

En tant qu'administrateur, vous pouvez configurer le comportement de l'agent Wyse Management Suite en fonction des configurations de Dell Hybrid Client. Les administrateurs peuvent également configurer les appareils pour appliquer des configurations en dehors des heures de bureau.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **Client hybride**.
   La fenêtre **Contrôle de configuration | Client hybride** s'affiche.
3. Cliquez sur l'option **Standard**.
4. Accédez à **Paramètres WMS** > **Paramètres client WMS**.
5. Pour configurer les heures et les jours ouvrables pour le groupe de périphériques, cliquez sur **Ajouter une ligne** dans le champ **Heures de bureau** et dans le menu déroulant **Jours ouvrés**.
6. Pour permettre à l'agent de rapporter les sessions d'utilisateurs, activez l'option **Activer la création de rapport de session** et sélectionnez le moment dans le menu déroulant **Session de rapport**. Les options disponibles sont les suivantes :
   - **Envoyer la session utilisateur au moment de l'exécution** : Dell Client Agent envoie le rapport de session utilisateur chaque fois qu'un utilisateur se déconnecte du périphérique.
   - **Envoyer la session utilisateur au moment de la vérification** : Dell Client Agent envoie le rapport de session utilisateur toutes les 8 heures.
   - **Envoyer la session utilisateur en dehors des heures de bureau** : Dell Client Agent envoie le rapport de session utilisateur en dehors des heures de bureau configurées à l'étape 5.
7. Pour déployer les configurations sur n'importe quel périphérique en fonction des configurations de niveau utilisateur, activez l'option **Activer l'itinérance de personnalisation de l'utilisateur**. Si cette option est activée, les paramètres configurés par un utilisateur sur un appareil tels que les données du navigateur Google Chrome, les données du navigateur Firefox, la personnalisation du bureau, le fond d'écran personnalisé, l'état de l'application du navigateur, les données du cloud et les détails de la session VDI sont enregistrés dans le serveur de Wyse Management Suite. Ces configurations sont appliquées automatiquement lorsqu'un utilisateur se connecte à un autre appareil. Les paramètres configurés sont prioritaires par rapport à toutes les autres configurations. De plus, les paramètres peuvent être configurés à partir du groupe des politiques utilisateur.
8. Pour activer les notifications sur le périphérique, activez l'option **Activer la notification push**. Si cette option est activée, les paramètres configurés sont appliqués immédiatement après avoir cliqué sur **Enregistrer et publier**. Si vous désactivez cette option, les configurations sont appliquées lorsque l'appareil envoie un signal de pulsation.

   REMARQUE : Si vous désactivez cette option, le déploiement d'applications peut indiquer un état d'erreur car Wyse Management Suite n'envoie pas la notification push à Dell Hybrid Client.

9. Pour appliquer la configuration en dehors des heures de bureau spécifiées, sélectionnez l'option dans le menu déroulant. Les options disponibles sont les suivantes :
   - **Immédiatement** : si vous sélectionnez cette option, les configurations sont appliquées immédiatement après avoir cliqué sur **Enregistrer et publier**.
   - **En dehors des heures de bureau spécifiées** : si vous sélectionnez cette option, les configurations sont appliquées en dehors des heures de bureau configurées à l'étape 5.
   - **Lorsqu'aucun utilisateur ne s'est connecté au périphérique pendant un certain temps** si vous sélectionnez cette option, la configuration est appliquée lorsqu'aucun utilisateur ne s'est connecté au périphérique pendant un certain temps. Vous pouvez spécifier le délai d'inactivité au-delà duquel les configurations sont appliquées au périphérique.

   REMARQUE : Vous pouvez également configurer ces paramètres pour un périphérique particulier à partir de la page **Périphériques**. Pour plus d'informations, consultez la section Configurer la politique de niveau périphérique.

10. Pour sauvegarder les configurations de l'utilisateur et les déployer sur plusieurs appareils, activez l'option **Itinérance des données utilisateur**. Vous pouvez configurer l'enregistrement des paramètres après une fonction spécifiée, dans un référentiel de votre choix, ou les configurations qui doivent être enregistrées dans le référentiel. Cette configuration est prise en charge à partir de la version 1.5 de Dell Hybrid Client ou version supérieure.
11. Pour activer la mise à jour automatique des applications signées par Dell après l'enregistrement de l'appareil Dell Hybrid Client dans Wyse Management Suite, activez l'option **Mise à jour automatique**. L'application est automatiquement mise à jour si la version du

package de l'application dans le référentiel de Wyse Management Suite est supérieure à la version installée sur l'appareil Dell Hybrid Client. Vous pouvez également sélectionner l'application et configurer la fréquence à laquelle la mise à jour automatique doit être effectuée.

REMARQUE : L'appareil Dell Hybrid Client doit être allumé pour que la configuration soit appliquée à l'appareil.

12. Pour activer le mode de débogage du journal Dell Client Agent, activez l'option **Mode Assistance**.

Configuration des paramètres de déploiement pour des appareils Dell Hybrid Client

À partir de Wyse Management Suite 3.1, vous pouvez configurer les paramètres de déploiement pour des appareils Dell Hybrid Client. Vous pouvez configurer les paramètres pour déployer en mode silencieux les configurations sur les appareils.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **Client hybride**.
3. Accédez à **Paramètres WMS** > **Paramètre de déploiement**.
4. Configurez une ou plusieurs des options ci-dessous :
   - **Configurer la notification de mise à jour** : si vous désactivez cette option, la boîte de dialogue de mise à jour de la configuration ne s'affiche pas sur l'appareil.
   - **Notification de mise à jour de l'application** : si vous désactivez cette option, la notification de l'utilisateur ne s'affiche pas lorsque vous déployez une politique d'application.
   - **Notification de mise à jour d'image** : si vous désactivez cette option, la notification de l'utilisateur ne s'affiche pas lorsque vous déployez une politique d'image.
   - **Notification de déconnexion** : si vous désactivez cette option, la notification de l'utilisateur ne s'affiche pas lorsqu'un utilisateur se déconnecte de l'appareil.
   - **Notification de redémarrage** : si vous désactivez cette option, la notification de l'utilisateur ne s'affiche pas lorsque la configuration de redémarrage de l'appareil est déployée.
   - **Afficher l'écran de verrouillage** : si vous désactivez cette option, l'écran de verrouillage ne s'affiche pas pendant les mises à jour de l'application et de l'image.

   REMARQUE : Vous pouvez activer l'option **Activer/désactiver toutes les notifications** si vous souhaitez activer toutes les options et notifications.

   REMARQUE : Les options **Configurer la notification de mise à jour** et **Afficher l'écran de verrouillage** sont désactivés par défaut.
5. Cliquez sur **Enregistrer et publier**.

Modifier les paramètres de la politique Dell Generic Client

Prérequis

- Créez un groupe avec un jeton de groupe pour les appareils.
- Enregistrez Dell Generic Client dans Wyse Management Suite.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **Generic Client**.
   La fenêtre **Contrôle de configuration | Generic Client** s'affiche.
3. Cliquez sur l'option **Avancé**.
4. Sélectionnez les options à configurer.
5. Dans les champs respectifs, cliquez sur le paramètre et configurez les options selon vos besoins.

REMARQUE : Vous pouvez cliquer sur l'option **Réinitialiser la politique** si vous souhaitez réinitialiser la politique sur les configurations par défaut à partir de Wyse Management Suite 3.2.

6. Cliquez sur **Enregistrer et publier**.

   REMARQUE : Une fois que vous avez cliqué sur **Enregistrer et publier**, les paramètres configurés s'affichent également dans l'onglet **Standard**.

   Le tableau suivant énumère l'ensemble des fonctionnalités que vous pouvez configurer dans la fenêtre **Contrôle de configuration | Generic Client**.

Tableau 6. Paramètres de la politique Generic Client

Fonctionnalité	Sous-fonctionnalité : groupe de politique des utilisateurs	Sous-fonctionnalité : groupe de politique des périphériques
Confidentialité et sécurité	Certificat	Certificat
Niveau de consignation de l'agent	Niveau de consignation	Niveau de consignation

Création et importation d'un fichier d'exception d'appareil en bloc

À partir de Wyse Management Suite 3.1, vous pouvez déployer des configurations d'exception d'appareil sur plusieurs appareils ThinOS 9.x.

Étapes

1. Créez un fichier d'exception d'appareil en bloc. Pour créer un fichier, effectuez l'une des opérations suivantes :
   - Créez une politique de groupe pour un groupe de test, puis exportez cette politique vers un fichier. Si la configuration contient des mots de passe, ils sont remplacés par des caractères * dans le fichier exporté. Par exemple :


```
{
    "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"
                    }
                }
            }
        }
    ]
}
```

- Créez un fichier .json qui respecte le format suivant :

```
{

"devices": {

<serialnumber>: {

"parameters": {

"<parametername>": {

       "value": <value>

},

"<parametername>": {

       "value": <value>

}

},

configurations: [<configuration name>]

}

}

"configurations": {

<configurationName>: {

"<parametername>": {

       "value": <value>

},

"<parametername>": {

       "value": <value>

}

  }

}

}
```

Par exemple :

```
{
    "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. Compressez et chiffrez le fichier.

   REMARQUE : Vous pouvez utiliser le logiciel 7-zip pour compresser et chiffrer le fichier.

   REMARQUE : La taille du fichier ne doit pas dépasser 1 Mo.

3. Accédez à **Groupes et configurations**, puis cliquez sur **Importer les politiques**.
   L'écran **Assistant d'importation de politiques** s'affiche.
4. Sélectionnez **Exceptions d'appareil en bloc**.
5. Cliquez sur **Parcourir** et sélectionnez le fichier .zip chiffré par mot de passe.
6. Cliquez sur **Suivant**.
   La page **Sélectionner les configurations de type d'appareil à importer** s'affiche.
7. Cliquez sur **Suivant**.

   REMARQUE : Puisque vous pouvez importer en bloc un fichier d'exception d'appareil pour les modèles ThinOS 9.x, vous ne pouvez pas configurer les options dans la page.

8. Saisissez le mot de passe du fichier .zip qui a été utilisé pour compresser le fichier .json.
9. Cliquez sur **Suivant**.
   Un récapitulatif de l'importation des exceptions d'appareil en bloc s'affiche.
10. Cliquez sur **Importer**.

Une fois les configurations importées, un lien de génération de rapport est créé dans la page **Groupe et configurations** et permet de télécharger le rapport. Un message de réussite s'affiche sur la page **Groupe et configurations**.

REMARQUE : Si un appareil n'est pas enregistré et que les configurations sont importées, les exceptions sont appliquées à cet appareil uniquement si l'appareil est enregistré dans les 30 jours suivants avec l'un des numéros de série préchargés.

REMARQUE : Si un appareil est déjà enregistré et que les configurations sont importées avec le numéro de série de l'appareil, les exceptions d'appareil sont appliquées à l'appareil.

REMARQUE : Le fichier importé est protégé par mot de passe. Le chiffrement AES-256 et ZipCrypto est pris en charge.

REMARQUE : Les configurations telles que les certificats, le fond d'écran, le logo, etc., ainsi que les ressources qui leur sont associées, ne sont pas importées.

8

Gestion des périphériques

Cette section décrit la procédure à suivre pour exécuter une tâche d'administration de routine des périphériques en utilisant la console de gestion. Pour localiser l'inventaire des périphériques, cliquez sur l'onglet **Appareils**. Vous pouvez afficher un sous-ensemble des périphériques à l'aide de différents critères de filtre, par exemple les groupes ou les sous-groupes, le type de périphérique, le type de système d'exploitation, l'état, le sous-réseau, la plate-forme ou le fuseau horaire.

Vous pouvez trier la liste des périphériques selon les éléments suivants :

- Type
- Plateforme
- Version du système d'exploitation
- Numéro de série
- Adresse IP
- Détails du dernier utilisateur
- Détails du groupe
- Heure du dernier enregistrement
- État de l'enregistrement
- Écrire l'état du filtre

Pour afficher la page **Détails du périphérique** d'un périphérique particulier, cliquez sur l'entrée du périphérique répertorié sur cette page. Tous les paramètres de configuration du périphérique et le niveau de groupe auquel chaque paramètre est appliqué s'affichent sur la page **Détails du périphérique**.

Vous pouvez définir le paramètre de configuration propre au périphérique. Les paramètres configurés dans cette section remplacent tous les paramètres qui ont été configurés au niveau des groupes et/ou au niveau global.

REMARQUE : Vous ne pouvez pas exporter les détails des appareils vers un fichier CSV depuis la page **Appareils** de Wyse Management Suite 3.2. Vous devez aller dans **Administration du portail** > **Rapports** > **Générer un rapport** et sélectionner une option sous la catégorie **Appareils** dans la liste déroulante **Type** pour exporter les détails.

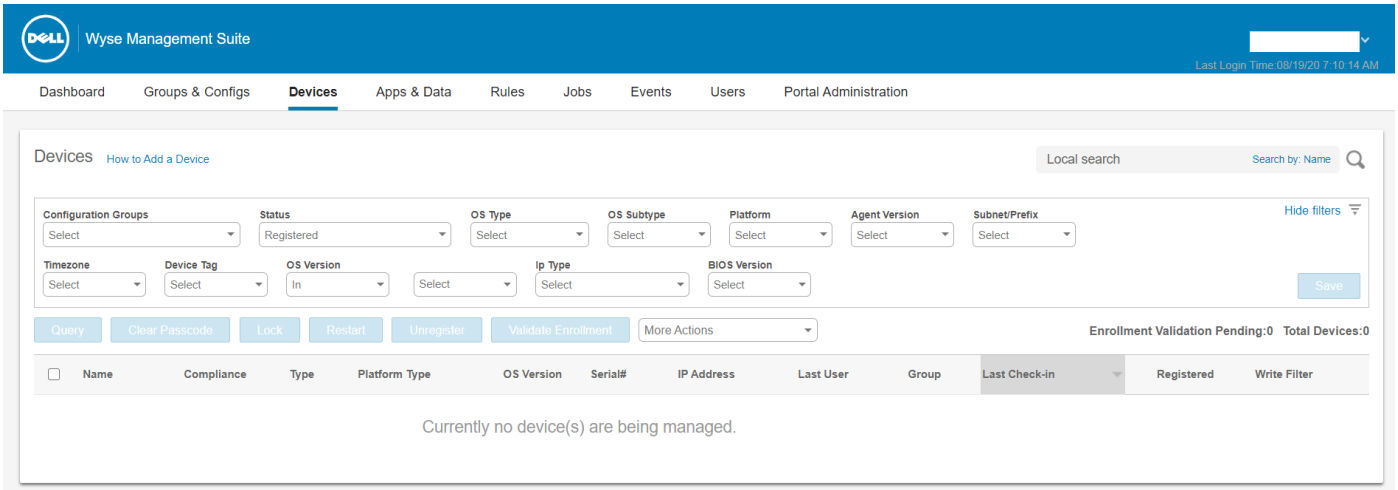


Figure 6. Page Périphériques

Sujets :

- Méthodes d'enregistrement de périphériques dans Wyse Management Suite
- Rechercher un périphérique à l'aide de filtres
- Enregistrer le filtre sur la page Appareils
- Interroger l'état de l'appareil
- Verrouiller les appareils
- Redémarrer les appareils

- Annuler l'enregistrement de l'appareil
- Validation de l'inscription
- Réinitialiser l'appareil aux valeurs d'usine par défaut
- Modifier une attribution de groupe sur la page Appareils
- Envoyer des messages à un appareil
- Commande Wake on LAN
- Afficher les détails des appareils
- Affichage des paramètres d'affichage
- Affichage des détails des cartes NIC virtuelles
- Affichage des informations du BIOS
- Gérer le résumé des appareils
- Afficher les informations sur le système
- Afficher les événements d'appareil
- Afficher les applications installées
- Renommer le Thin Client
- Activation d'une connexion de prise de contrôle à distance
- Configuration d'une connexion de prise de contrôle à distance pour des appareils Dell Hybrid Client
- Arrêt des appareils
- Numéroter un appareil
- État de conformité du périphérique
- Extraction d'une image Windows Embedded Standard ou ThinLinux
- Demander un fichier journal
- Troubleshooting your device
- Réinitialiser Dell Hybrid Client
- Convertir votre Dell Generic Client en Hybrid Client
- Extraire le package d'interface utilisateur de configuration pour Dell Hybrid Client
- Réinitialiser Dell Hybrid Client aux paramètres d'usine
- Modifier des groupes d'appareils en bloc

Méthodes d'enregistrement de périphériques dans Wyse Management Suite

Vous pouvez enregistrer un Thin Client avec Wyse Management Suite à l'aide de l'une des méthodes suivantes :

- Effectuez un enregistrement manuel via l'interface utilisateur fournie par Wyse Device Agent (WDA) sur l'appareil.
- Enregistrez automatiquement en configurant les balises d'option appropriées sur le serveur DHCP.
- Enregistrez automatiquement en configurant les enregistrements SRV DNS appropriés sur le serveur DNS.

REMARQUE :

- Pour un cloud public, enregistrez un Thin Client en indiquant l'URL Wyse Management Suite et le jeton de groupe pour le groupe sur lequel vous souhaitez enregistrer l'appareil.
- Pour un Cloud privé, enregistrez un client léger en indiquant l'URL de Wyse Management Suite et le jeton de groupe (facultatif) pour le groupe sur lequel vous souhaitez enregistrer l'appareil. Les appareils sont enregistrés auprès du groupe non géré, si le jeton de groupe n'est pas fourni.

Enregistrement manuel Dell Hybrid Client

Prérequis

Avant d'enregistrer l'appareil, assurez-vous que votre appareil dispose d'une connectivité réseau pour contacter le serveur Wyse Management Suite.

REMARQUE : Vous pouvez enregistrer l'appareil uniquement à partir du compte utilisateur invité. En tant qu'utilisateur invité, vous pouvez annuler l'enregistrement de l'appareil à partir de Wyse Management Suite uniquement en mode dev. Les utilisateurs du domaine ne peuvent pas annuler l'enregistrement de l'appareil à partir de Wyse Management Suite.

Étapes

1. Connectez-vous à Dell Hybrid Client en tant qu'utilisateur invité. Par défaut, le nom d'utilisateur administrateur est **guest**.
2. Dans la barre supérieure, cliquez sur l'  .
3. Cliquez sur **Dell Client Agent**.
   La fenêtre **Dell Client Agent** s'affiche.
4. Cliquez sur **Inscription**.
   L'état par défaut s'affiche et indique **Découverte en cours**.
5. Pour enregistrer manuellement, cliquez sur le bouton **Annuler**.
6. Dans le champ **Serveur WMS**, saisissez l'URL du serveur Wyse Management Suite.
7. Dans le champ **Jeton de groupe**, saisissez la clé d'inscription de groupe. Le jeton de groupe est une clé unique permettant d'enregistrer directement vos appareils auprès de groupes.

   REMARQUE : si les champs client et groupe sont vides, l'appareil est enregistré auprès du groupe non géré. Toutefois, le jeton de groupe est obligatoire pour enregistrer l'appareil dans un Cloud public.

8. Cliquez sur le bouton **Marche/Arrêt** pour activer ou désactiver l'option **Valider l'autorité de certification du certificat de serveur**. Activez cette option pour effectuer la validation de certificat de serveur pour toutes les communications entre les appareils et les serveurs.

   L'option Validation de l'autorité de certification est activée automatiquement et ne peut pas être désactivée si une URL de Cloud public est saisie.
9. Cliquez sur **Enregistrer** pour enregistrer votre périphérique sur le serveur Wyse Management Suite.

   Lorsque votre périphérique est enregistré, l'état est affiché comme étant **Enregistré** avec une coche de couleur verte en regard de l'étiquette **État de l'enregistrement**. La légende du bouton **Enregistrer** devient **Annuler l'enregistrement**.

   REMARQUE : Les administrateurs ou les utilisateurs invités ne peuvent pas annuler l'enregistrement de l'appareil directement à partir de la fenêtre **Dell Client Agent**. Pour annuler l'enregistrement de l'appareil, vous devez soit passer en mode dev, soit utiliser la console de Wyse Management Suite.

Enregistrer Dell Generic Client en utilisant la méthode de recherche manuelle

Vous pouvez utiliser la méthode de recherche manuelle pour enregistrer les appareils Dell Ubuntu tels que OptiPlex 3090 Ultra, OptiPlex 7090 Ultra, OptiPlex 7070 Ultra, et Latitude 3320 fonctionnant sous Ubuntu version 18.04 ou 20.04 LTS 64-bit vers Wyse Management Suite en utilisant l'agent Dell Client Agent-Enabler.

Étapes

1. Créez un fichier reg.json en utilisant le modèle suivant :

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

2. Copiez le fichier reg.json dans `/etc/dcae/config`.
3. Redémarrez le périphérique.

   REMARQUE : Les appareils Dell Ubuntu sont enregistrés dans Wyse Management Suite en tant que Dell Hybrid Client si la version de DCA-Enabler est 1.1.0-17 ou inférieure. Si la version de DCA-Enabler est 1.2.0-xx ou supérieure, les appareils sont enregistrés en tant que Dell Generic Client.

Enregistrer Dell Hybrid Client en utilisant la méthode de découverte manuelle

Vous pouvez utiliser la méthode de découverte manuelle pour enregistrer les périphériques OptiPlex 7070 Ultra exécutant la version 18.04 LTS 64 bits d'Ubuntu dans Wyse Management Suite à l'aide de l'agent Dell Client Agent Enabler.

Étapes

1. Créez un fichier reg.json en utilisant le modèle suivant :

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

2. Copiez le fichier reg.json dans `/etc/dcae/config`.
3. Redémarrez le périphérique.

Enregistrer des appareils ThinOS à l'aide de Wyse Device Agent

Pour enregistrer les appareils ThinOS manuellement, procédez comme suit :

Étapes

1. Dans le menu du bureau du client léger, sélectionnez **Configuration du système** > **Configuration centrale**.
   La fenêtre **Configuration centrale** s'affiche.
2. Cliquez sur l'onglet **WDA**. Le service WDA s'exécute automatiquement une fois que le processus d'amorçage du client est terminé.

   WMS est sélectionné par défaut.
3. Cochez la case **Activer Wyse Management Suite** pour activer Wyse Management Suite.
4. Saisissez la **Clé d'inscription de groupe** selon la configuration de votre administrateur pour le groupe de votre choix.
5. Sélectionnez l'option **Activer les paramètres avancés WMS** et saisissez les informations du serveur WMS ou du serveur MQTT.
6. Activez ou désactivez la validation CA selon votre type de licence. Pour le Cloud public, sélectionnez la case à cocher **Activer la validation CA** et pour le Cloud privé, sélectionnez la case à cocher **Activer la validation CA** si vous avez importé des certificats provenant d'une autorité de certification reconnue dans votre serveur Wyse Management Suite.

   Pour activer l'option Validation CA dans le Cloud privé, vous devez également installer le même certificat auto-signé sur le périphérique ThinOS. Si vous n'avez pas installé le certificat auto-signé sur l'appareil ThinOS, ne cochez pas la case **Activer la validation CA**. Vous pouvez installer le certificat sur le périphérique via Wyse Management Suite après l'enregistrement, puis activer l'option Validation CA.

   REMARQUE :
   - Un message d'avertissement s'affiche si vous désactivez la validation de l'autorité de certification. Vous devez cliquer sur OK pour confirmer.
   - Pour la version cloud public de Wyse Management Suite du centre de données américain, ne modifiez pas les informations par défaut du serveur WMS et du serveur MQTT. Pour la version cloud public de Wyse Management Suite du centre de données européen, utilisez les informations suivantes :
     - Serveur CCM : eu1.wysemanagementsuite.com
     - Serveur MQTT : eu1-pns.wysemanagementsuite.com:1883
   - Un message d'avertissement s'affiche si l'adresse du serveur contient http. Vous devez cliquer sur OK pour confirmer.
7. Pour vérifier la configuration, cliquez sur **Valider la clé**. L'appareil redémarre automatiquement après la validation de la clé.

   REMARQUE : Si la clé n'est pas validée, vérifiez la clé de groupe et l'URL de serveur WMS que vous avez fourni. Assurez-vous que les ports 443 et 1883 ne sont pas bloqués par le réseau.
8. Cliquez sur **OK**.
   Le périphérique est enregistré sur Wyse Management Suite.

Enregistrement de Thin Clients Windows Embedded Standard dans Wyse Management Suite à l'aide de Wyse Device Agent

Prérequis

Créez un groupe dans Wyse Management Suite pour enregistrer un appareil.

Étapes

1. Ouvrez l'application Wyse Device Agent.
   L'écran Wyse Device Agent s'affiche.
2. Dans la liste déroulante **Serveur de gestion**, sélectionnez **Wyse Management Suite**.
3. Saisissez l'adresse du serveur et le numéro de port dans les champs correspondants.

   REMARQUE : Si l'adresse du serveur contient **http**, un message d'avertissement s'affiche. Cliquez sur **OK** pour confirmer.

4. Saisissez le jeton de groupe. Pour un locataire unique, le jeton de groupe est une étape facultative.

   REMARQUE : Le jeton de groupe saisi dans le champ **Jeton de groupe** n'est pas affiché en texte clair.

5. Activez ou désactivez la validation CA qui correspond à votre type de licence.

   REMARQUE : Si vous désactivez la validation CA, un message d'avertissement s'affiche. Cliquez sur **OK** pour confirmer.

6. Cliquez sur **Enregistrer**.

Enregistrer Thin Client Wyse Software dans Wyse Management Suite à l'aide de Wyse Device Agent

Prérequis

Créez un groupe pour enregistrer un périphérique dans Wyse Management Suite.

Étapes

1. Ouvrez l'application **Wyse Device Agent**.
   La fenêtre **Wyse Device Agent** s'affiche.
2. Saisissez les détails de l'appareil pour l'enregistrement.
3. Dans la liste déroulante **Serveur de gestion**, sélectionnez **Wyse Management Suite**.
4. Saisissez l'adresse du serveur et le numéro de port dans les champs correspondants.

   REMARQUE : Si l'adresse du serveur contient **http**, un message d'avertissement s'affiche. Cliquez sur **OK** pour confirmer.

5. Saisissez le jeton de groupe. Pour un locataire unique, le jeton de groupe est une étape facultative.
6. Activez ou désactivez la validation CA qui correspond à votre type de licence.

   REMARQUE : Si vous désactivez la validation CA, un message d'avertissement s'affiche. Cliquez sur **OK** pour confirmer.

7. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement terminé, le message **Enregistré à Wyse Management Suite** s'affiche.

Enregistrer des clients légers ThinLinux via Wyse Device Agent

Prérequis

Créez un groupe dans Wyse Management Suite pour enregistrer un appareil.

Étapes

1. Ouvrez l'application Wyse Device Agent.
   L'écran Wyse Device Agent s'affiche.
2. Saisissez les détails de l'appareil pour l'enregistrement.
3. Dans l'onglet Wyse Management Suite, saisissez les détails du serveur Wyse Management Suite.
4. Saisissez le jeton de groupe.
   Pour un locataire unique, le jeton de groupe est une étape facultative.
5. Cliquez sur **Enregistrer**.

Une fois l'enregistrement terminé, un message de confirmation s'affiche.

Enregistrer les appareils ThinOS à l'aide de la méthode FTP INI

Prérequis

Créez un groupe à enregistrer dans Wyse Management Suite.

Étapes

1. Créez un fichier `wnos.ini`. Saisissez les paramètres suivants :

   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`

   Par exemple, pour enregistrer l'appareil ThinOS dans Wyse Management Suite (le FQDN du serveur est ServerFQDN.domain.com) avec le jeton de groupe defa-defadefa et l'option de validation CA, saisissez le paramètre INI suivant :

   CCMEnable=`yes` **CCMServer**= `is ServerFQDN.domain.com` **GroupPrefix**=`defa` **GroupKey**=`defadefa` **CAVAlidation**=`yes` **Discover**=`yes`

2. Placez le fichier `wnos.ini` dans le dossier wnos de n'importe quel chemin FTP.
3. Accédez à **Configuration centrale** dans l'appareil ThinOS.
4. Dans l'onglet **Général**, indiquez le chemin FTP dans les serveurs de fichiers ou le chemin vers le dossier parent.
5. Saisissez les informations d'identification si nécessaire. Si le FTP n'a pas besoin d'informations d'identification, le nom d'utilisateur et le mot de passe peuvent être anonymes.
6. Cliquez sur **OK**, puis redémarrez le client léger.
7. Accédez à **Configuration centrale** dans l'appareil ThinOS.
   Dans l'onglet **Wyse Device Agent**, observez que les détails du serveur de gestion Wyse sont disponibles dans le champ correspondant et que l'entrée du client est visible sur la page Serveur Wyse Management > Appareils.

Enregistrer des appareils ThinLinux version 2.0 à l'aide de la méthode FTP INI

Prérequis

Créez un groupe à enregistrer dans Wyse Management Suite.

Étapes

1. Créez un fichier `wlx.ini`. Saisissez les paramètres suivants :

   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`

   Par exemple, pour enregistrer l'appareil ThinLinux version 2.0 dans Wyse Management Suite (le FQDN du serveur est ServerFQDN.domain.com) avec le jeton de groupe defa-defadefa et l'option de validation CA, saisissez le paramètre INI suivant :

   WMSEnable=`yes`

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

   GroupRegistrationKey=`defa-defadefa`

   CAValidation=`True`

2. Placez le fichier wlx ini dans le dossier wyse\wlx2.
3. Accédez à **Paramètres** et passez en administrateur sur le client léger ThinLinux.
4. Accédez à **Gestion** > **INI**.
5. Saisissez l'URL du serveur FTP.

6. Cliquez sur **Enregistrer**, puis redémarrez le client léger.
7. Accédez à **Gestion** > **Wyse Device Agent**.
   Dans l'onglet Wyse Device Agent, observez que les détails du serveur de gestion Wyse sont disponibles dans le champ correspondant et que l'entrée du client est visible sur la page Serveur Wyse Management > Appareils.

Enregistrer des appareils ThinLinux version 1.0 à l'aide de la méthode FTP INI

Prérequis

Créez un groupe à enregistrer dans Wyse Management Suite.

Étapes

1. Créez un fichier `wlx.ini` et saisissez le paramètre suivant :

   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`

   Par exemple, pour enregistrer l'appareil ThinLinux version 1.0 dans Wyse Management Suite (le FQDN du serveur est ServerFQDN.domain.com) avec le jeton de groupe defa-defadefa et l'option de validation CA, saisissez le paramètre INI suivant :

   WMSEnable=`yes`

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

   GroupRegistrationKey=`defa-defadefa`

   CAValidation=`True`

2. Placez le fichier wlx ini dans le dossier `wyse\wlx`.
3. Accédez à **Paramètres** et passez en administrateur sur le client léger ThinLinux.
4. Accédez à **Gestion** > **INI**.
5. Saisissez l'URL du serveur FTP.
6. Cliquez sur **Enregistrer**, puis redémarrez le client léger.
7. Accédez à **Gestion** > **Wyse Device Agent**.
   Dans l'onglet Wyse Device Agent, observez que les détails du serveur de gestion Wyse sont disponibles dans le champ correspondant et que l'entrée du client est visible sur la page Serveur Wyse Management > Appareils.

Enregistrement des périphériques à l'aide des balises d'option DHCP

Vous pouvez enregistrer les périphériques à l'aide des balises d'option DHCP.

Tableau 7. Enregistrement du périphérique à l'aide des balises d'option DHCP (suite)

Balise d'option	Description
Nom : WMS **Type de données** : chaîne **Code** : 165 **Description** : FQDN du serveur WMS	Cette balise pointe vers l'URL du serveur Wyse Management Suite. Par exemple, `wmsserver.acme.com`, où wmsserver.acme.com est le nom du domaine complet du serveur où Wyse Management Suite est installé. **REMARQUE :** N'utilisez pas https://FQDN ou FQDN:443 dans l'URL de serveur, ou le client léger ne sera pas enregistré sous Wyse Management Suite.
Nom : MQTT **Type de données** : chaîne **Code** : 166	Cette balise dirige le périphérique vers le serveur Push Notification server (PNS) de Wyse Management Suite. Pour l'installation d'un Cloud privé, le périphérique est dirigé vers le service MQTT du serveur Management Suite Wyse. Par exemple, `wmsservername.domain.com:1883`.

Tableau 7. Enregistrement du périphérique à l'aide des balises d'option DHCP

Balise d'option	Description
Description : Serveur MQTT	Pour enregistrer vos périphériques dans le Cloud public Wyse Management Suite, le périphérique doit pointer vers les serveurs (MQTT) PNS du Cloud public. Par exemple : US1 : us1-pns.wysemanagementsuite.com EU1 : eu1-pns.wysemanagementsuite.com Vous devez saisir les détails du serveur MQTT lorsque vous configurez les détails de Wyse Device Agent dans l'ancienne version de ThinOS et des périphériques Windows Embedded. MQTT est un composant de WMS qui est nécessaire pour informer les clients légers. Les URL (avec et sans détails MQTT) doivent être ajoutées à la liste verte dans l'environnement Cloud public Wyse Management Suite. **REMARQUE :** vous ne pouvez pas utiliser les URL MQTT pour vous connecter à Wyse Management Suite.
Nom : validation CA **Type de données** : chaîne **Code** : 167 **Description** : validation de l'autorité de certification	Vous pouvez activer ou désactiver l'option de validation CA si vous enregistrez vos périphériques avec Wyse Management Suite en Cloud privé. Par défaut, la validation CA est activée dans le Cloud public. Vous pouvez aussi désactiver la validation CA dans le Cloud public. Saisissez **Vrai**, si vous avez importé les certificats SSL à partir d'une autorité connue pour la communication https entre le client et le serveur Wyse Management Suite. Saisissez **Faux**, si vous n'avez pas importé les certificats SSL à partir d'une autorité connue pour la communication https entre le client et le serveur Wyse Management Suite.
Nom : jeton de groupe **Type de données** : chaîne **Code** : 199 **Description** : jeton de groupe	Cette balise est requise pour enregistrer les périphériques ThinOS avec Wyse Management Suite sur le Cloud public ou privé. Cette balise est facultative pour enregistrer les périphériques Windows Embedded Standard ou ThinLinux avec Wyse Management Suite sur le Cloud privé. Si la balise n'est pas disponible, les périphériques sont automatiquement enregistrés pour le groupe non géré lors de l'installation sur site.

REMARQUE : Pour obtenir des instructions détaillées sur l'ajout de balises d'option DHCP sur le serveur Windows, voir Créer et configurer des balises d'option DHCP.

Enregistrement d'appareils à l'aide d'un enregistrement SRV DNS

L'enregistrement du périphérique basé sur DNS est pris en charge par les versions suivantes de Wyse Device Agent :

- Systèmes intégrés Windows : version 13.0 ou ultérieure
- Thin Linux : version 2.0.24 ou ultérieure
- ThinOS : firmware 8.4 ou versions ultérieures

Vous pouvez enregistrer les périphériques avec le serveur Wyse Management Suite si les champs d'enregistrement SRV DNS sont définis avec des valeurs valides.

REMARQUE : Pour obtenir des instructions détaillées sur l'ajout d'enregistrements SRV DNS sur le serveur Windows, voir Créer et configurer des enregistrements SRV DNS.

Le tableau suivant répertorie les valeurs valides pour les enregistrements SRV DNS :

Tableau 8. Configuration du périphérique à l'aide de l'enregistrement SRV DNS

URL/Balise	Description
Nom d'enregistrement : _WMS_MGMT **Enregistrement FQDN** : _WMS_MGMT._tcp.<Domainname>	Cet enregistrement pointe vers l'URL de serveur Wyse Management Suite. Par exemple, `wmsserver.acme.com` est le

Tableau 8. Configuration du périphérique à l'aide de l'enregistrement SRV DNS (suite)

URL/Balise	Description
Type d'enregistrement : SRV	nom du domaine complet du serveur où Wyse Management Suite est installé. **REMARQUE :** N'utilisez pas https://FQDN ou FQDN:443 dans l'URL de serveur, ou le client léger ne sera pas enregistré sous Wyse Management Suite.
Nom d'enregistrement : _WMS_MQTT **Enregistrement FQDN** : _WMS_MQTT._tcp.<Domainname> **Type d'enregistrement** : SRV	Cet enregistrement dirige l'e périphérique vers le serveur Push Notification server (PNS) de Wyse Management Suite. Pour l'installation d'un Cloud privé, le périphérique est dirigé vers le service MQTT du serveur Management Suite Wyse. Par exemple, `wmsservername.domain.com:1883`. **REMARQUE :** MQTT est facultatif pour la version la plus récente de Wyse Management Suite. Pour enregistrer vos périphériques dans le Cloud public Wyse Management Suite, le périphérique doit pointer vers les serveurs (MQTT) PNS du Cloud public. Par exemple : US1 :us1-pns.wysemanagementsuite.com UE1 :eu1-pns.wysemanagementsuite.com Vous devez saisir les détails du serveur MQTT lorsque vous configurez les détails de Wyse Device Agent dans l'ancienne version de ThinOS et des périphériques Windows Embedded. MQTT est un composant de WMS qui est nécessaire pour informer les clients légers. Les URL (avec et sans détails MQTT) doivent être ajoutées à la liste verte dans l'environnement Cloud public Wyse Management Suite. **REMARQUE :** vous ne pouvez pas utiliser les URL MQTT pour vous connecter à Wyse Management Suite.
Nom d'enregistrement : _WMS_GROUPTOKEN **FQDN d'enregistrement** : _WMS_GROUPTOKEN._tcp.<Domainname> **Type d'enregistrement** : TEXTE	Cet enregistrement est requis pour enregistrer les périphériques ThinOS avec Wyse Management Suite sur le Cloud public ou privé. Cet enregistrement est facultatif pour enregistrer les périphériques Windows Embedded Standard ou ThinLinux avec Wyse Management Suite sur le Cloud privé. Si l'enregistrement n'est pas disponible, les périphériques sont automatiquement enregistrés pour le groupe non géré lors de l'installation sur site. **REMARQUE :** le jeton de groupe est facultatif pour la dernière version de Wyse Management Suite sur le Cloud privé.
Nom d'enregistrement : _WMS_CAVALIDATION **FQDN d'enregistrement** : _WMS_CAVALIDATION._tcp.<Domainname> **Type d'enregistrement** : TEXTE	Vous pouvez activer ou désactiver l'option de validation CA si vous enregistrez vos périphériques avec Wyse Management Suite en Cloud privé. Par défaut, la validation CA est activée dans le Cloud public. Vous pouvez aussi désactiver la validation CA dans le Cloud public. Saisissez **Vrai**, si vous avez importé les certificats SSL à partir d'une autorité connue pour la communication https entre le client et le serveur Wyse Management Suite. Saisissez **Faux**, si vous n'avez pas importé les certificats SSL à partir d'une autorité connue pour la communication https entre le client et le serveur Wyse Management Suite. **REMARQUE :** la validation CA est facultative pour la version la plus récente de Wyse Management Suite.

Rechercher un périphérique à l'aide de filtres

Étapes

1. Dans la liste déroulante **Groupes de configuration**, sélectionnez soit le groupe de politiques par défaut, soit les groupes ajoutés par un administrateur.
2. Dans la liste déroulante **État**, sélectionnez l'une des options suivantes :
   - **Enregistrement**
     - Inscrit
     - Pré-enregistré
     - Pas inscrit
     - Conforme
     - Validation de l'inscription en attente
     - En attente
     - Non conforme
   - **L'état de la connexion**
     - En ligne
     - Hors ligne
     - Inconnu
   - **Autres**
     - Ajouté(s) récemment
3. Dans la liste déroulante **Type de système d'exploitation**, sélectionnez l'un des systèmes d'exploitation suivants :
   - **Thin Client**
     - Linux
     - ThinLinux
     - ThinOS
     - WES
     - Teradici (Cloud privé)
     - Thin Client Wyse Software
   - **Client hybride**
     - Client hybride
4. Dans la liste déroulante **Sous-type de SE**, sélectionnez un sous-type pour votre système d'exploitation.
5. Dans le menu déroulant **Plate-forme**, sélectionnez une plate-forme.
6. Dans le menu déroulant **Version du système d'exploitation**, sélectionnez une version de système d'exploitation.
7. Dans la liste déroulante **Version de l'agent**, sélectionnez une version de l'agent.
8. Dans la liste déroulante **Sous-réseau/Préfixe**, sélectionnez un sous-réseau.
9. Dans la liste déroulante **Fuseau horaire**, sélectionnez le fuseau horaire.
10. Dans la liste déroulante **Numéro de périphérique**, sélectionnez un numéro de périphérique.
11. Dans la liste déroulante **Type d'IP**, sélectionnez le type d'IP.
12. Dans le menu déroulant **Version du BIOS**, sélectionnez la version du BIOS.

Enregistrer le filtre sur la page Appareils

Vous pouvez enregistrer le filtre actuel en tant que groupe en configurant les options de filtre requises.

Étapes

1. Saisissez le **nom** du filtre.
2. Décrivez le filtre dans la zone **Description**.
3. Cochez cette case pour définir le filtre actuel en tant qu'option par défaut.
4. Cliquez sur **Enregistrer le filtre**.

Interroger l'état de l'appareil

Vous pouvez envoyer une commande de mise à jour de l'état et des informations sur l'appareil dans le système.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
3. Cochez la case du périphérique.
4. Cliquez sur **Requête**.
   Une fenêtre **Alerte** s'affiche.
5. Cliquez sur **Envoyer la commande** pour envoyer la commande de requête.

Verrouiller les appareils

Vous pouvez envoyer une commande pour verrouiller l'appareil enregistré pour un groupe d'appareils qui sont connectés à une session VDI. Cette option s'applique aux clients légers utilisant le système d'exploitation ThinOS.

Prérequis

Le périphérique doit être connecté à une connexion VDI, et un utilisateur doit être connecté au périphérique.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
3. Cochez la case du périphérique.
4. Cliquez sur **Verrouiller**.
   Une fenêtre **Alerte** s'affiche.
5. Cliquez sur **Envoyer la commande** pour envoyer la commande de verrouillage.

   Depuis Wyse Management Suite 3.2, vous pouvez également envoyer une commande pour verrouiller l'appareil depuis la page **Tâches**. Pour plus d'informations, consultez la section Planifier une tâche de commande d'appareil.

Redémarrer les appareils

Vous pouvez envoyer une commande pour redémarrer un appareil enregistré.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
3. Cochez la case du périphérique.
4. Cliquez sur **Redémarrer**.
   Une fenêtre **Alerte** s'affiche.
5. Cliquez sur **Envoyer la commande** pour envoyer la commande de redémarrage.

Annuler l'enregistrement de l'appareil

Vous pouvez envoyer une commande pour annuler l'enregistrement d'un appareil dans Wyse Management Suite.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
3. Cochez la case du périphérique.
4. Cliquez sur **Annuler l'enregistrement**.
   Une fenêtre **Alerte** s'affiche.
5. Cochez la case **Forcer l'annulation de l'enregistrement**.
6. Cliquez sur **Envoyer la commande** pour envoyer la commande d'annulation de l'enregistrement.

   REMARQUE : L'option Forcer l'annulation de l'enregistrement peut être utilisée pour supprimer l'appareil en l'absence de communication entre le serveur et le client. L'appareil est déplacé vers un état non géré et peut être supprimé de l'entrée du serveur. Les actions Annuler l'enregistrement et Forcer l'annulation de l'enregistrement peuvent également être effectuées par l'interface utilisateur WES WDA.

Validation de l'inscription

Lorsque vous enregistrez un appareil manuellement ou à l'aide de la méthode de détection automatique DHCP/DNS, l'appareil est enregistré dans un groupe particulier si le jeton de groupe est défini. Si le jeton de groupe n'est pas défini, l'appareil est enregistré dans le groupe non géré.

Dans Wyse Management Suite, l'option **Validation de l'inscription** est disponible là où le client doit procéder à une approbation manuelle avant que l'appareil ne soit enregistré dans un groupe.

Lorsque l'option **Validation de l'inscription** est activée, les appareils détectés automatiquement présentent l'état **Validation en attente** sur la page **Appareils**. Le client peut sélectionner un ou plusieurs appareils sur la page **Appareils** et valider l'inscription. Une fois validés, les appareils sont déplacés vers le groupe prévu. Pour plus d'informations sur la validation des appareils, voir Validation de l'inscription.

REMARQUE : L'option **Validation de l'inscription** est désactivée pour les clients existants dans le Cloud public ou lors de la mise à niveau des clients sur site.

L'état de validation des appareils s'affiche également dans la section **Appareils** de la page **Tableau de bord**.

Valider l'enregistrement d'un appareil

Vous pouvez activer l'option **Validation de l'inscription** pour permettre aux administrateurs de contrôler l'enregistrement manuel et automatique des clients légers sur un groupe. Vous pouvez filtrer les appareils présentant l'état **Validation en attente** en cliquant sur le nombre **En attente** sur la page **Tableau de bord** ou en sélectionnant l'option **Validation de l'inscription en attente** dans la liste déroulante **État** de la page **Appareils**.

Prérequis

- Vous devez activer l'option **Validation de l'inscription** lors de l'installation de Wyse Management Suite ou sur la page **Administration de portail**.
- L'appareil doit présenter l'état Inscription en attente.

Étapes

1. Cochez la case située en regard de l'appareil que vous souhaitez valider.
2. Cliquez sur l'option **Valider l'inscription**.
   Une fenêtre **Alerte** s'affiche.
3. Cliquez sur **Envoyer la commande**.
   L'appareil est déplacé dans le groupe souhaité, puis il est enregistré.

Réinitialiser l'appareil aux valeurs d'usine par défaut

Vous pouvez envoyer une commande pour rétablir votre appareil aux valeurs d'usine par défaut.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
3. Cochez la case du périphérique.
4. Dans le menu déroulant **Plus d'actions**, sélectionnez **Rétablissement des paramètres d'usine**.
   Une fenêtre **Alerte** s'affiche.
5. Indiquez la raison de la réinitialisation du client.
6. Cliquez sur **Envoyer la commande**.

   Depuis Wyse Management Suite 3.2, vous pouvez également envoyer une commande pour verrouiller l'appareil depuis la page **Tâches**. Pour plus d'informations, consultez la section Planifier une tâche de commande d'appareil.

Modifier une attribution de groupe sur la page Appareils

Vous pouvez modifier l'attribution de groupe d'un appareil à l'aide de la page **Appareils**.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
3. Cochez la case du périphérique.
4. Dans le menu déroulant **Plus d'actions**, cliquez sur **Modifier le groupe**.
   La fenêtre **Modifier l'attribution de groupe** s'affiche.
5. Dans le menu déroulant, sélectionnez un nouveau groupe pour le périphérique.
6. Cliquez sur **Enregistrer**.

Envoyer des messages à un appareil

Vous pouvez envoyer un message à un appareil enregistré à l'aide de la page **Appareils**.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphériques** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
3. Cochez la case du périphérique.
4. Dans le menu déroulant **Plus d'actions**, sélectionnez **Envoyer un message**.
   La fenêtre **Envoyer un message** s'affiche.
5. Saisissez le message.
6. Cliquez sur **Envoyer**.

   Vous pouvez également envoyer un message à l'appareil depuis la page **Tâches** de Wyse Management Suite 3.2. Pour plus d'informations, consultez la section Planifier une tâche de commande d'appareil.

Commande Wake on LAN

Vous pouvez envoyer une commande pour activer un périphérique si celui-ci est éteint ou en mode Veille.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
3. Cochez la case du périphérique.

4. Dans le menu déroulant **Plus d'actions**, cliquez sur **Wake On LAN**.
   Une fenêtre **Alerte** s'affiche.
5. Cliquez sur **Envoyer la commande**.

Afficher les détails des appareils

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
   La liste des périphériques souhaités s'affiche.
3. Cliquez sur l'un des appareils affichés.
   La page **Détails de l'appareil** s'affiche.

Affichage des paramètres d'affichage

À partir de Wyse Management Suite 3.1, vous pouvez afficher la configuration de l'affichage des appareils qui exécutent les systèmes d'exploitation Windows Embedded et ThinLinux. Vous pouvez afficher le nom du fournisseur, le numéro de modèle, le numéro de série, la résolution, les proportions, le mode, l'alignement et les informations de rotation de la configuration d'affichage.

Étapes

1. Accédez à la page **Périphériques**.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
   La liste des périphériques souhaités s'affiche.
3. Cliquez sur l'un des appareils affichés.

   La page **Détails du périphérique** s'affiche.

4. Accédez à **Infos système** > **Périphériques**.
   Vous pouvez afficher les informations de la configuration de l'affichage.

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

Figure 7. Paramètres d'affichage

Affichage des détails des cartes NIC virtuelles

À partir de Wyse Management Suite 3.1, vous pouvez afficher les détails de l'adaptateur réseau des appareils qui exécutent les systèmes d'exploitation Windows Embedded et ThinLinux. Vous pouvez afficher le nom de l'adaptateur, l'adresse MAC, l'adresse IP, l'adresse IP de la passerelle et les détails du serveur DNS de la carte réseau.

Étapes

1. Accédez à la page **Périphériques**.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
   La liste des périphériques souhaités s'affiche.
3. Cliquez sur l'un des appareils affichés.

   La page **Détails du périphérique** s'affiche.
4. Accédez à **Infos système** > **Détails du réseau – Cartes réseau**.
   Vous pouvez afficher les détails de la carte NIC virtuelle dans la section **Détails du réseau – Cartes réseau**.

Figure 8. Détails du réseau – Cartes réseau

Affichage des informations du BIOS

À partir de Wyse Management Suite 3.1, vous pouvez afficher la valeur du paramètre du BIOS sur la page **Détails de l'appareil**.

Étapes

1. Accédez à la page **Périphériques**.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
   La liste des périphériques souhaités s'affiche.
3. Cliquez sur l'un des appareils affichés.

   La page **Détails du périphérique** s'affiche. Vous pouvez afficher les détails du BIOS dans la section **Paramètres du BIOS** de l'onglet **Infos système**.

Gérer le résumé des appareils

Vous pouvez afficher et gérer les informations sur les remarques, les attributions de groupe, les alertes et la configuration des appareils à l'aide de la page **Appareils**.

Étapes

1. Cliquez sur **Périphériques**.
2. Sur la page **Détails sur le périphérique**, cliquez sur l'onglet **Récapitulatif**.
   Le récapitulatif de périphérique s'affiche.
3. Dans le volet de droite, cliquez sur **Ajouter une remarque**.
   La fenêtre **Ajouter une remarque** s'affiche.
4. Saisissez le message dans le champ correspondant et cliquez sur **Enregistrer**.
5. Dans le volet de droite, cliquez sur **Modifier l'attribution de groupe**.
   La fenêtre **Modifier l'attribution de groupe** s'affiche.
6. Dans le menu déroulant, sélectionnez un nouveau groupe pour le périphérique.
7. Cliquez sur **Enregistrer**.
8. Cliquez sur **Créer/Modifier des exceptions** pour créer ou modifier une exception au niveau du périphérique et configurez une politique de périphérique spécifique sur la page **Périphériques**.

Afficher les informations sur le système

Étapes

1. Cliquez sur **Périphériques**.

La page **Périphérique** s'affiche.

2. Appliquez les filtres pour rechercher le périphérique souhaité.
   La liste des périphériques souhaités s'affiche.
3. Cliquez sur l'un des appareils affichés.
   La page **Détails de l'appareil** s'affiche.
4. Cliquez sur **Informations système**.
   Les informations système s'affichent.

Afficher les événements d'appareil

Vous pouvez afficher et gérer les informations sur les événements système relatifs à un appareil.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
   La liste des périphériques souhaités s'affiche.
3. Cliquez sur l'un des appareils affichés.
   La page **Détails de l'appareil** s'affiche.
4. Sur la page **Détails sur le périphérique**, cliquez sur l'onglet **Événements**.
   Les événements liés à l'appareil s'affichent.

Afficher les applications installées

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
   La liste des périphériques souhaités s'affiche.
3. Cliquez sur l'un des appareils affichés.
   La page **Détails de l'appareil** s'affiche.
4. Cliquez sur l'onglet **Applications installées**.
   La liste des applications installées sur le périphérique s'affiche.

   Cette option est disponible pour les appareils Windows Embedded Standard, Linux et ThinLinux. Voici les attributs affichés sur la page :
   - Nom
   - Éditeur
   - Version
   - Installé sur

   REMARQUE :

   le nombre d'applications installées augmente ou diminue en fonction de l'installation ou de la désinstallation des applications. La liste est mise à jour lorsque l'appareil effectue une vérification ou est ensuite interrogé.

Renommer le Thin Client

Vous pouvez utiliser cette page pour modifier le nom d'hôte des clients légers exécutés sur les systèmes d'exploitation Windows Embedded Standard, ThinLinux et ThinOS.

Étapes

1. Sur la page **Appareils**, cliquez sur l'appareil.
2. Dans la liste déroulante **Plus d'options**, sélectionnez l'option **Modifier le nom d'hôte**.
3. Saisissez le nouveau nom d'hôte lorsque vous y êtes invité.

REMARQUE : Le nom d'hôte ne peut contenir que des caractères alphanumériques et un seul tiret.

4. Pour les appareils Windows Embedded Standard, la liste déroulante **Redémarrage** est incluse dans la fenêtre **Alerte**. Pour redémarrer le système, sélectionnez l'option **Redémarrer**. Si vous sélectionnez l'option **Réamorcer ultérieurement**, l'appareil redémarre à l'heure configurée, puis le nom d'hôte est mis à jour.

   REMARQUE : Pour les appareils ThinLinux, nul besoin de redémarrer pour mettre à jour le nom d'hôte.

5. Cliquez sur **Envoyer la commande**.
   Un message de confirmation s'affiche.

Activation d'une connexion de prise de contrôle à distance

Utilisez cette page pour permettre aux administrateurs globaux et de groupes d'accéder à distance aux sessions de clients légers Windows Embedded Standard, ThinLinux et ThinOS. Cette fonctionnalité ne concerne que le Cloud privé et est disponible pour les licences standard et Pro.

Étapes

1. Sur la page **Appareils**, cliquez sur l'appareil.
2. Dans la liste déroulante **Plus d'options**, sélectionnez l'option **Clichés instantanés distants (VNC)**.
   L'adresse IP et le numéro de port du client léger cible s'affichent dans la boîte de dialogue **Clichés instantanés distants (VNC)**.

   REMARQUE : le numéro de port par défaut est 5900.

3. Modifiez le numéro de port du client léger cible (facultatif).
4. Cliquez sur **Connexion** pour lancer une session à distance vers le client léger cible.

   REMARQUE : le portail Wyse Management Suite prend en charge un maximum de cinq sessions de mise en mémoire fantôme à distance par client.

Configuration d'une connexion de prise de contrôle à distance pour des appareils Dell Hybrid Client

Utilisez cette page pour autoriser les administrateurs globaux et de groupe à accéder à distance aux sessions de appareils Dell Hybrid Client. Cette fonction est disponible uniquement pour le cloud privé et les licences standard et Pro.

Étapes

1. Déployez le package du module complémentaire VNC à partir de Wyse Management Suite à l'aide de la politique d'application standard ou avancée (voir Politique d'application).
   Le module complémentaire est installé et l'appareil redémarre.
2. Configurez et déployez les options du serveur VNC à partir de Wyse Management Suite. Pour configurer les options du serveur VNC, procédez comme suit :
   a. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
   b. Dans le menu déroulant **Modifier les politiques**, cliquez sur **Client hybride**.
      La fenêtre **Contrôle de configuration | Client hybride** s'affiche.
   c. Cliquez sur l'option **Standard** ou **Advanced**.
   d. Accédez à **Confidentialité et sécurité** > **Serveur VNC** et configurez les options.
   e. Cliquez sur **Enregistrer et publier**.

Arrêt des appareils

Wyse Management Suite vous permet d'arrêter les appareils tels que Windows Embedded Standard, ThinLinux et les clients légers ThinOS.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour localiser le périphérique souhaité.
   La liste des périphériques souhaités s'affiche.
3. Dans la liste déroulante **Plus d'options**, cliquez sur **Arrêter maintenant**.
   La commande à distance pour arrêter l'appareil est envoyée vers l'appareil sélectionné. L'appareil répond au serveur et la commande est appliquée avec succès.
   REMARQUE : L'option **Arrêter maintenant** n'est pas activée pour les clients légers qui exécutent sur le système d'exploitation Linux.

Numéroter un appareil

Wyse Management Suite vous permet d'identifier un périphérique ou un groupe de périphériques à l'aide de l'option **Numéroter un périphérique**.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour localiser le périphérique souhaité.
   La liste des périphériques souhaités s'affiche.
3. Sélectionnez un ou plusieurs périphériques. Dans la liste déroulante **Plus d'options**, cliquez sur **Numéroter un périphérique**.
   La fenêtre **Définir un numéro de périphérique** s'affiche.
4. Saisissez le numéro souhaité.
5. Cliquez sur **Définir un numéro**.

État de conformité du périphérique

Par défaut, les couleurs suivantes s'affichent pour indiquer l'état du périphérique :

- Rouge : lorsque le périphérique enregistré n'a pas été vérifié pendant plus de sept jours.
- Gris : lorsque vous appliquez une règle de configuration sur le périphérique.
- Vert : lorsque vous appliquez toutes les politiques de configuration sur le périphérique.

La valeur par défaut peut être remplacée par une valeur comprise entre 1 et 99 jours.

L'option **État de la connexion** est située en regard du nom du périphérique. Les couleurs suivantes s'affichent pour indiquer l'état de la connexion :

- Rouge : lorsque l'appareil n'a pas émis de signal depuis plus de trois tentatives.
- Gris : lorsque l'appareil n'a pas émis de pulsation depuis plus de deux tentatives, mais moins de trois tentatives.
- Vert : lorsque le périphérique émet régulièrement un signal.

Extraction d'une image Windows Embedded Standard ou ThinLinux

Prérequis

- Si vous utilisez le référentiel distant Wyse Management Suite 1.3, le modèle d'extraction Récupération/Récupération+ SE n'est pas disponible dans le référentiel. Vous devez mettre à niveau Wyse Management Suite vers la version 1.4 ou une version ultérieure pour accéder aux modèles.
- Pour exécuter l'opération d'extraction d'image ThinLinux, vous devez fermer la fenêtre **Paramètres** dans l'appareil ThinLinux. Vous devez exécuter cette opération avant d'extraire une image SE/SE+Récupération de l'appareil ThinLinux.
- Pour mettre à niveau ThinLinux 1.x vers la version 2.x, l'administrateur doit mettre à jour l'appareil avec les dernières versions de WDA et Merlin, puis extraire l'image. L'image extraite doit être utilisée pour mettre à niveau ThinLinux 1.x vers la version 2.x.
- Assurez-vous que la machine virtuelle sur laquelle le serveur est exécuté dispose de suffisamment de mémoire pour effectuer l'extraction et exécuter les services requis pour Wyse Management Suite si vous utilisez un référentiel local.

Étapes

1. Accédez à la page de périphérique **Windows Embedded Standard** ou **ThinLinux**.
2. Sélectionnez l'option **Extraire l'image de SE** dans la liste déroulante **Plus d'actions**.
3. Saisissez ou sélectionnez les informations suivantes :
   - **Nom de l'image :** nommez l'image. Pour remplacer l'image avec un nom similaire et les fichiers image dont la création a échoué, cliquez sur **Remplacer le nom**.
   - **Logithèque de fichiers :** dans le menu déroulant, sélectionnez le référentiel de fichiers dans lequel l'image est chargée. Il existe deux types de référentiels de fichiers :
     - Référentiel local
     - Le référentiel Wyse Management Suite distant
   - **Type d'extraction :** sélectionnez **Par défaut** ou **Avancé** en fonction de vos besoins.
     - Lorsque le type d'extraction **Par défaut** est sélectionné, les options suivantes sont affichées :
       - Compresser
       - SE
       - BIOS
       - Récupération : pour ThinLinux 2.x
     - Lorsque le type d'extraction **Avancé** est sélectionné, une liste déroulante permettant de sélectionner les modèles s'affiche. Sélectionnez n'importe quel modèle disponible par défaut.

       REMARQUE : Vous pouvez utiliser les modèles personnalisés créés manuellement en modifiant les modèles existants ou par défaut.
4. Cliquez sur **Préparer l'extraction d'image**.

Résultats

Lorsque la commande **Extraire l'image de SE** est envoyée, le périphérique client reçoit une demande d'extraction d'image du serveur. Un message de demande d'extraction d'image s'affiche côté client. Cliquez sur l'une des options suivantes :

- **Extraire après Sysprep** : l'appareil redémarre et se connecte au système d'exploitation avec l'état désactivé. Exécutez une opération Sysprep personnalisée. Une fois l'opération sysprep personnalisée terminée, l'appareil démarre le système d'exploitation Merlin et extrait l'image.

  REMARQUE : Cette option s'applique aux appareils Windows Embedded Standard.
- **Extraire maintenant** : l'appareil démarre avec le système d'exploitation Merlin et l'extraction de l'image est exécutée.

Demander un fichier journal

Vous pouvez demander un fichier journal à partir d'appareils Windows Embedded Standard, ThinOS et ThinLinux. L'appareil ThinOS charge les journaux système. Windows Embedded Standard télécharge les journaux Wyse Device Agent et les journaux de l'observateur d'événements Windows. Linux ou ThinLinux télécharge les journaux Wyse Device Agent et les journaux système.

Prérequis

L'appareil doit être activé pour pouvoir extraire le fichier journal.

Étapes

1. Rendez-vous sur la page **Appareils**, puis cliquez sur un appareil particulier.
   Les détails de l'appareil s'affichent.
2. Cliquez sur l'onglet **Journal de l'appareil**.
3. Cliquez sur **Demander un fichier journal**.
4. Une fois les fichiers journaux chargés sur le serveur Wyse Management Suite, activez le lien **Cliquez ici**, puis téléchargez les journaux.

   REMARQUE : Les fichiers journaux de l'appareil sont au format `Hostname-timestamp`. Dell Hybrid Client, Linux ou ThinLinux chargent le fichier journal au format `.tar` ; les systèmes Windows ou ThinOS 9.x chargent le fichier journal au format `.zip`.

Troubleshooting your device

Vous pouvez afficher et gérer les informations de dépannage à l'aide de la page **Appareils**.

Étapes

1. Sur la page **Détails sur le périphérique**, cliquez sur l'onglet **Dépannage**.
2. Cliquez sur **Demander une capture d'écran**.
   Vous pouvez capturer l'écran du client léger avec ou sans l'autorisation du client. Si vous cochez la case **Exiger l'acceptation de l'utilisateur**, un message s'affiche sur le client. Cette option s'applique uniquement aux appareils Windows Embedded Standard, Linux et ThinLinux.
3. Cliquez sur **Demander la liste des processus** pour afficher la liste des processus en cours d'exécution sur le Thin Client.
4. Cliquez sur **Demander la liste des services** pour afficher la liste des services en cours d'exécution sur le Thin Client.
5. Cliquez sur **Lancer le suivi** pour accéder à la console Mesures de performance.
   Dans la console **Mesures de performance**, les détails suivants s'affichent :
   - Moyenne de la dernière minute du processeur
   - Utilisation moyenne de la mémoire de dernière minute

Réinitialiser Dell Hybrid Client

Vous pouvez envoyer une commande pour réinitialiser Dell Hybrid Client.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
3. Cochez la case du périphérique.
4. Dans le menu déroulant **Plus d'actions**, sélectionnez **Réinitialiser**.
   Une fenêtre **Alerte** s'affiche.
5. Cliquez sur **Envoyer la commande**.
   Cette action assure la fonction d'image de récupération pour le périphérique.

Convertir votre Dell Generic Client en Hybrid Client

Vous pouvez envoyer une commande pour convertir votre Dell Generic Client en Dell Hybrid Client.

Prérequis

L'appareil Dell Ubuntu (Generic Client) doit être préchargé avec le pack Dell Hybrid dans la partition de récupération.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour trouver l'appareil Generic Client privilégié.
3. Cochez la case du périphérique.
4. Dans le menu déroulant **Plus d'actions**, sélectionnez **Convertir en Hybrid**.
   Une fenêtre **Alerte** s'affiche.
5. Cliquez sur **Envoyer la commande**.

   REMARQUE : La commande **Convertir en Hybrid** est également disponible sur la page **Tâches**, **Appareils** et **Détails sur l'appareil**.

Extraire le package d'interface utilisateur de configuration pour Dell Hybrid Client

Lorsque Dell Hybrid Client possède une version du schéma de configuration supérieure à la version présente dans le serveur Wyse Management Suite, vous pouvez extraire le dernier package d'interface utilisateur de configuration.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
3. cliquez sur le périphérique que vous souhaitez configurer.
   La page **Détails du périphérique** s'affiche.
4. Dans le menu déroulant **Plus d'actions**, cliquez sur **Extraire le package d'interface utilisateur de configuration**.
   Une fenêtre **Alerte** s'affiche.
5. Cliquez sur **Envoyer la commande**.

Réinitialiser Dell Hybrid Client aux paramètres d'usine

Vous pouvez envoyer une commande pour réinitialiser Dell Hybrid Client aux paramètres d'usine.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphérique** s'affiche.
2. Appliquez les filtres pour rechercher le périphérique souhaité.
3. Cochez la case du périphérique.
4. Dans le menu déroulant **Plus d'actions**, sélectionnez **Rétablissement des paramètres d'usine**.
   Une fenêtre **Alerte** s'affiche.
5. Indiquez la raison du rétablissement des paramètres de Dell Hybrid Client
6. Cliquez sur **Envoyer la commande**.

Modifier des groupes d'appareils en bloc

Vous pouvez modifier le groupe de plusieurs appareils en utilisant le numéro de série, l'adresse MAC ou le nom d'hôte à partir de Wyse Management Suite 3.2. Cette option s'applique uniquement à la licence Pro de Wyse Management Suite.

Prérequis

Créez un fichier CSV avec le numéro de série, l'adresse MAC ou le nom de l'hôte des appareils.

Étapes

1. Cliquez sur **Périphériques**.
   La page **Périphériques** s'affiche.
2. Dans la liste déroulante **Plus d'actions**, sélectionnez **Modification de groupes en bloc**.
   La fenêtre **Modifier l'attribution de groupe en bloc** s'affiche.
3. Dans la liste déroulante **Sélectionner la propriété pour filtrer les appareils**, sélectionnez une propriété pour filtrer les appareils à déplacer dans un nouveau groupe en fonction de la propriété sélectionnée.
4. Pour sélectionner le fichier CSV, cliquez sur **Parcourir** et allez à l'emplacement où se trouve le fichier CSV.
5. Dans la liste déroulante **Sélectionner un nouveau groupe pour ces appareils**, sélectionnez le nouveau groupe pour les appareils.
6. Cliquez sur **Enregistrer**.

   REMARQUE : Vous pouvez modifier le groupe d'un maximum de 100 appareils à la fois.

9

Applications et données

Cette section décrit la procédure à suivre pour exécuter des tâches d'application de périphérique de routine, créer des images du système d'exploitation, gérer l'inventaire et définir des politiques à l'aide de la console Wyse Management. Les noms des référentiels sont codés par couleur pour indiquer l'état.

Vous pouvez configurer le type de politiques suivant à l'aide de la page **Applications et données** :

- Politique d'application standard : cette politique vous permet d'installer un seul package d'application.
- Politique d'application avancée : cette politique vous permet d'installer plusieurs packages d'application.
- Politique d'image : cette politique vous permet d'installer le système d'exploitation.

Le déploiement de politiques d'application et d'images de système d'exploitation sur les Thin Clients peut être planifié pour une exécution immédiate ou ultérieure, selon un fuseau horaire spécifique ou selon le fuseau horaire configuré sur votre périphérique.

Sujets :

Politiques d'application

Wyse Management Suite prend en charge les types suivants d'inventaire d'application et de politiques de déploiement d'applications :

- Configurer l'inventaire de l'application client léger
- Configurer l'inventaire de l'application Thin Client Wyse Software
- Créer et déployer une politique d'application standard pour les clients légers
- Créer et déployer une politique d'application avancée pour les clients légers
- Créer et déployer une politique d'application standard sur les Thin Clients Wyse Software
- Créer et déployer une politique d'application avancée pour les Thin Clients Wyse Software

Remarques importantes concernant les appareils Windows :

- Prend en charge l'installation pour les applications Windows avec les extensions .msi, .exe, .msu, .msp.

  Les applications avec toute autre extension sont téléchargées vers `%sytemdrive%\wyse\WDA" Ex: "C:\wyse\WDA`.

- Pour déployer des applications .exe à l'aide de Wyse Management Suite, suivez la méthode d'installation silencieuse. Vous devez saisir les paramètres silencieux appropriés si nécessaire. Par exemple, **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**

- Prend en charge les déploiements de scripts avec les extensions de fichier .bat, .cmd, .ps1, .vbs.

  Les scripts avec toute autre extension sont téléchargés vers `%sytemdrive%\wyse\WDA" Ex: "C:\wyse\WDA`.

- Tout script transmis à l'aide de Wyse Management Suite doit être non interactif, ce qui signifie qu'aucune interaction de l'utilisateur n'est requise lors de l'installation.
- Avec la politique d'application avancée, tout script/exe qui renvoie une valeur autre que 0 est considéré comme défaillant.
- Dans la politique d'application avancée, en cas d'échec de la préinstallation, l'installation de l'application ne se poursuit pas.
- Tout exe/script transmis à l'aide d'une application standard est signalé comme ayant abouti, le code d'erreur étant mis à jour dans l'état de la tâche.
- Pour les applications avec l'extension msi/msu/msp, les codes d'erreur standard sont signalés. Si l'application renvoie REBOOT_REQUIRED, l'appareil effectue un redémarrage supplémentaire.

Remarques importantes concernant les appareils Linux :

- Prend en charge l'installation pour les applications Linux avec l'extension .bin, .deb pour ThinLinux 2.0 et .RPM pour Thin Linux 1.0.
- Prend en charge les déploiements de scripts pour les appareils ThinLinux avec les extensions .sh.
- Dans la politique d'application standard ou avancée, tout script/deb/rpm qui renvoie une valeur autre que 0 est considéré comme défaillant.
- Dans la politique d'application avancée, en cas d'échec de la préinstallation, l'installation de l'application ne se poursuit pas.

Configurer l'inventaire de l'application client léger

Étapes

1. Cliquez sur l'onglet **Applications et données**.
2. Dans le volet de gauche, accédez à **Inventaire d'applications** > **Thin Client**.
   Les détails de l'application s'affichent dans la fenêtre **Inventaire Thin Client**.
3. Pour ajouter une application à l'inventaire, placez les fichiers de l'application du client léger dans le dossier `<repo-dir>\repository\thinClientApps`.
   Wyse Management Suite Repository envoie périodiquement des métadonnées pour tous les fichiers vers le serveur Wyse Management Suite.
4. Pour modifier l'application, procédez comme suit :
   a. Sélectionnez l'application téléchargée dans la liste.
   b. Cliquez sur **Modifier l'appli**.
      La fenêtre **Modifier l'application** s'affiche.
   c. Saisissez la note.
   d. Cliquez sur **Enregistrer**.

      REMARQUE : Un suffixe global est ajouté aux applications téléchargées par l'opérateur.

   Les applications qui sont présentes dans différents référentiels sont répertoriées une seule fois. La colonne **Nom du référentiel** affiche le nombre de référentiels dans lesquels l'application est présente. Vous pouvez pointer la souris sur la colonne pour afficher le nom des référentiels. En outre, le nom du référentiel est codé par couleur pour indiquer la disponibilité.

Configurer l'inventaire de l'application Thin Client Wyse Software

Étapes

1. Cliquez sur l'onglet **Applications et données**.
2. Dans le volet de gauche, accédez à **Inventaire d'applications** > **Wyse Software Thin Client**.
3. Pour ajouter une application à l'inventaire, placez les fichiers de l'application du client léger dans le dossier `<repo-dir>\repository\softwareTcApps`.
   Wyse Management Suite Repository envoie périodiquement des métadonnées pour tous les fichiers vers le serveur Wyse Management Suite.

Créer et déployer une politique d'application standard pour les clients légers

Étapes

1. Dans le référentiel local, accédez à **thinClientApps**, puis copiez l'application sur le dossier.
2. Accédez à **Applications et données** > **Inventaire d'applications** > **Thin Client**, puis vérifiez que l'application est enregistrée dans Wyse Management Suite.

   REMARQUE : l'interface de l'inventaire d'applications met environ deux minutes à remplir les programmes récemment ajoutés.

3. Accédez à **Applications et données** > **Politiques d'application** > **Thin Client**.
4. Cliquez sur **Ajouter une politique**.
   La fenêtre **Ajouter une politique d'application standard** s'affiche.
5. Saisissez un **nom de politique**.
6. Dans la liste déroulante **Groupe**, sélectionnez un groupe.
7. Dans la liste déroulante **Tâche**, sélectionnez la tâche.
8. Dans la liste déroulante **Type de système d'exploitation**, sélectionnez le système d'exploitation.
9. Cochez la case **Fichiers de filtre basés sur les extensions** pour filtrer les applications.
10. Dans la liste déroulante **Application**, sélectionnez l'application.
    Si les fichiers de l'application sont disponibles sur plusieurs référentiels, le nombre de référentiels s'affiche à côté du nom de fichier.

REMARQUE : À partir de Wyse Management Suite 3.1, vous pouvez ajouter un script pour installer l'application sur les appareils ThinLinux. Vous devez vérifier qu'un shebang valable est présent dans le script pour ThinLinux.

11. Pour déployer cette politique sur un système d'exploitation ou une plate-forme spécifiques, sélectionnez **Filtre de sous-type de SE** ou **Filtre de plate-forme**.
12. Dans la liste déroulante **Appliquer automatiquement la politique**, sélectionnez l'une des options suivantes :
    - **Ne pas appliquer automatiquement** : les politiques ne sont pas automatiquement appliquées aux périphériques.
    - **Appliquer la politique aux nouveaux appareils** : la politique est automatiquement appliquée à un appareil enregistré qui appartient à un groupe sélectionné ou à l'appareil qui est déplacé vers un groupe sélectionné. Lorsque cette option est sélectionnée, la politique est appliquée à tous les nouveaux appareils qui sont enregistrés dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe. L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés.
    - **Appliquer la politique aux périphériques lors de la vérification** : la politique est automatiquement appliquée au périphérique lors de la vérification. Lorsque cette option est sélectionnée, la politique est appliquée à tous les appareils présents dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe immédiatement ou à une heure planifiée avant l'enregistrement de l'appareil, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe.

    REMARQUE : L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés dans Wyse Management Suite.

    REMARQUE : Pour les appareils Windows, spécifiez les paramètres d'installation silencieuse pour les fichiers .exe afin d'exécuter l'application en mode silencieux. Par exemple, **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**

13. Pour arrêter le processus d'installation après une valeur définie, spécifiez le nombre de minutes dans le champ **Délai d'expiration de l'installation de l'application**. La valeur par défaut est 60 minutes.

    REMARQUE : L'option **Délai d'expiration de l'installation de l'application** ne s'applique qu'aux appareils Windows Embedded Standard, Thin Client Wyse Software, Linux et ThinLinux.

14. Cliquez sur **Enregistrer** pour créer une politique.
    Un message s'affiche pour permettre à l'administrateur de planifier cette politique sur les périphériques en fonction du groupe.
15. Sélectionnez **Oui** pour planifier une tâche sur la même page.
16. Sélectionnez l'une des options suivantes :
    - **Immédiatement** : le serveur exécute la tâche immédiatement.
    - **Sur le fuseau horaire du périphérique** : le serveur crée une tâche pour chaque fuseau horaire du périphérique et planifie la tâche à la date et à l'heure sélectionnées du fuseau horaire du périphérique.
    - **Sur le fuseau horaire sélectionné** : le serveur crée une tâche à exécuter à la date et à l'heure du fuseau horaire désigné.
17. Pour créer la tâche, cliquez sur **Aperçu**. Les planifications sont affichées sur la page suivante.
18. Vous pouvez consulter l'état de la tâche en accédant à la page **Tâches**.

Création et déploiement d'une politique d'application standard sur les clients légers Wyse Software

Étapes

1. Dans le référentiel local, accédez à **softwareTcApps**, puis copiez l'application dans le dossier.
2. Accédez à **Applications et données** > **Inventaire d'applications** > **Thin Client Wyse Software**, puis vérifiez que l'application est enregistrée dans Wyse Management Suite.

   REMARQUE : l'interface de l'inventaire d'applications met environ deux minutes à remplir les programmes récemment ajoutés.

3. Cliquez sur **Ajouter une politique**.
   La fenêtre **Ajouter une politique d'application standard** s'affiche.
4. Saisissez un **nom de politique**.
5. Dans la liste déroulante **Groupe**, sélectionnez un groupe.
6. Dans la liste déroulante **Tâche**, sélectionnez la tâche.
7. Dans la liste déroulante **Type de système d'exploitation**, sélectionnez le système d'exploitation.
8. Cochez la case **Fichiers de filtre basés sur les extensions** pour filtrer les applications.

9. Dans la liste déroulante **Application**, sélectionnez l'application.
   Si les fichiers de l'application sont disponibles sur plusieurs référentiels, le nombre de référentiels s'affiche à côté du nom de fichier.
10. Pour déployer cette politique sur un système d'exploitation ou une plate-forme spécifiques, sélectionnez **Filtre de sous-type de SE** ou **Filtre de plate-forme**.
11. Dans la liste déroulante **Appliquer automatiquement la politique**, sélectionnez l'une des options suivantes :
    - **Ne pas appliquer automatiquement** : les politiques ne sont pas automatiquement appliquées aux périphériques.
    - **Appliquer la politique aux nouveaux appareils** : la politique est automatiquement appliquée à un appareil enregistré qui appartient à un groupe sélectionné ou à l'appareil qui est déplacé vers un groupe sélectionné. Lorsque cette option est sélectionnée, la politique est appliquée à tous les nouveaux appareils qui sont enregistrés dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe. L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés.
    - **Appliquer la politique aux périphériques lors de la vérification** : la politique est automatiquement appliquée au périphérique lors de la vérification. Lorsque cette option est sélectionnée, la politique est appliquée à tous les appareils présents dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe immédiatement ou à une heure planifiée avant l'enregistrement de l'appareil, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe.

    REMARQUE : L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés dans Wyse Management Suite.

    REMARQUE : Pour les appareils Windows, spécifiez les paramètres d'installation silencieuse pour les fichiers .exe afin d'exécuter l'application en mode silencieux. Par exemple, **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**

12. Pour arrêter le processus d'installation après une valeur définie, spécifiez le nombre de minutes dans le champ **Délai d'expiration de l'installation de l'application**. La valeur par défaut est 60 minutes.

    REMARQUE : L'option **Délai d'expiration de l'installation de l'application** s'applique uniquement aux périphériques Windows Embedded Standard et aux clients légers Wyse Software.

13. Cliquez sur **Enregistrer** pour créer une politique.
    Un message s'affiche pour permettre à l'administrateur de planifier cette politique sur les périphériques en fonction du groupe.
14. Sélectionnez **Oui** pour planifier une tâche sur la même page.
15. Sélectionnez l'une des options suivantes :
    - **Immédiatement** : le serveur exécute la tâche immédiatement.
    - **Sur le fuseau horaire du périphérique** : le serveur crée une tâche pour chaque fuseau horaire du périphérique et planifie la tâche à la date et à l'heure sélectionnées du fuseau horaire du périphérique.
    - **Sur le fuseau horaire sélectionné** : le serveur crée une tâche à exécuter à la date et à l'heure du fuseau horaire désigné.
16. Pour créer la tâche, cliquez sur **Aperçu**. Les planifications sont affichées sur la page suivante.
17. Vous pouvez consulter l'état de la tâche en accédant à la page **Tâches**.

Activation de la connexion directe pour Citrix StoreFront à l'aide de la politique d'application standard

Pour activer la connexion directe pour Citrix StoreFront, effectuez les opérations suivantes :

- **Scénario 1** : si vous souhaitez activer la connexion directe pour StoreFront sur la version actuelle de Citrix Receiver, effectuez les opérations suivantes :
  1. Créez et déployez une politique d'application standard pour désinstaller Citrix Receiver à l'aide du paramètre **`/silent`**.
  2. Créez et déployez une politique d'application standard pour réinstaller Citrix Receiver à l'aide du paramètre **`/silent /includeSSON /AutoUpdateCheck = Disabled`**.
- **Scénario 2** : si vous souhaitez mettre à niveau Citrix Receiver et activer la connexion directe pour StoreFront, effectuez les opérations suivantes :
  1. Créez et déployez une politique d'application standard pour mettre à niveau Citrix Receiver à l'aide du paramètre **`/silent /includeSSON /AutoUpdateCheck = Disabled`**.
- **Scénario 3** : si vous souhaitez rétrograder Citrix Receiver et activer la connexion directe pour StoreFront, effectuez les opérations suivantes :
  1. Créez et déployez une politique d'application standard pour rétrograder Citrix Receiver à l'aide du paramètre **`/silent /includeSSON /AutoUpdateCheck = Disabled`**.

Créer et déployer une politique d'application avancée pour les clients légers

Étapes

1. Copiez l'application et les scripts de pré-/post-installation (si nécessaire) pour effectuer le déploiement sur les Thin Clients.
2. Enregistrez l'application et les scripts de pré-/post-installation dans le dossier thinClientApps de la logithèque locale ou de Wyse Management Suite Repository.
3. Accédez à **Applications et données** > **Inventaire d'applications** > **Thin Client** et vérifiez que l'application est enregistrée.
4. Accédez à **Applications et données** > **Politiques d'application** > **Thin Client**.
5. Cliquez sur **Ajouter une politique avancée**.
   La page **Ajouter une politique d'application avancée** s'affiche.
6. Saisissez un **nom de politique**.
7. Dans la liste déroulante **Groupe**, sélectionnez un groupe.
8. Cochez la case **Sous-groupes** pour appliquer la politique aux sous-groupes.
9. Dans la liste déroulante **Tâche**, sélectionnez la tâche.
10. Dans la liste déroulante **Type de système d'exploitation**, sélectionnez le système d'exploitation.
11. Cochez la case **Fichiers de filtre basés sur les extensions** pour filtrer les applications.
12. Cliquez sur **Ajouter une application**, et sélectionnez une ou plusieurs applications sous **Applications**. Pour chaque application, vous pouvez sélectionner un script de pré- et post-installation sous **Pré-installation**, **Post-installation** et **Paramètres d'installation**.

    REMARQUE : À partir de Wyse Management Suite 3.1, vous pouvez ajouter un script pour installer l'application sur les appareils ThinLinux. Vous devez vérifier qu'un shebang valable est présent dans le script pour ThinLinux.

13. Si vous souhaitez que le système redémarre une fois l'application installée, sélectionnez **Redémarrage**.
14. Cliquez sur **Ajouter une application** et répétez l'étape pour ajouter plusieurs applications.

    REMARQUE : Pour arrêter la politique d'application au premier échec, sélectionnez **Activer la dépendance d'application**. Si cette option n'est pas sélectionnée, l'échec d'une application n'affecte pas la mise en œuvre de la politique.

    Si les fichiers de l'application sont disponibles sur plusieurs référentiels, le nombre de référentiels s'affiche à côté du nom de fichier.
15. Pour déployer cette politique sur un système d'exploitation ou une plate-forme spécifiques, sélectionnez **Filtre de sous-type de SE** ou **Filtre de plate-forme**.
16. Indiquez la durée d'affichage en minutes de la boîte de dialogue de message sur le client.
    Un message s'affiche sur le client, ce qui vous laisse le temps de sauvegarder votre travail avant le début de l'installation.
17. Pour autoriser un retard dans la mise en œuvre de la politique, cochez la case **Autoriser le retard d'exécution de la politique**. Si cette option est sélectionnée, les menus déroulants suivants s'activent :
    - Dans la liste déroulante **Nombre max. d'heures par retard**, sélectionnez le nombre maximal d'heures (1 à 24 heures) pendant lesquelles vous pouvez retarder l'exécution de la politique.
    - Dans la liste déroulante **Retards max.**, sélectionnez le nombre de fois (de 1 à 3) que vous pouvez retarder l'exécution de la politique.
18. Dans la liste déroulante **Appliquer automatiquement la politique**, sélectionnez l'une des options suivantes :
    - **Ne pas appliquer automatiquement** : les politiques ne sont pas automatiquement appliquées aux périphériques.
    - **Appliquer la politique aux nouveaux appareils** : la politique est automatiquement appliquée à un appareil enregistré qui appartient à un groupe sélectionné ou à l'appareil qui est déplacé vers un groupe sélectionné. Lorsque cette option est sélectionnée, la politique est appliquée à tous les nouveaux appareils qui sont enregistrés dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe. L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés.
    - **Appliquer la politique aux périphériques lors de la vérification** : la politique est automatiquement appliquée au périphérique lors de la vérification. Lorsque cette option est sélectionnée, la politique est appliquée à tous les appareils présents dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe immédiatement ou à une heure planifiée avant l'enregistrement de l'appareil, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe.

    REMARQUE : L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés dans Wyse Management Suite.

REMARQUE : Pour les appareils Windows, spécifiez les paramètres d'installation silencieuse pour les fichiers .exe afin d'exécuter l'application en mode silencieux. Par exemple, **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**

19. Cochez la case **Ignorer la vérification du filtre d'écriture** pour ignorer les cycles du filtre d'écriture. Cette option s'applique aux périphériques des systèmes d'exploitation Windows Embedded Standard et aux périphériques Thin Client Wyse Software.
20. Pour arrêter le processus d'installation après une valeur définie, spécifiez le nombre de minutes dans le champ **Délai d'expiration de l'installation de l'application**. La valeur par défaut est 60 minutes.

    REMARQUE : L'option **Délai d'expiration de l'installation de l'application** s'applique uniquement aux périphériques Windows Embedded Standard et aux clients légers Wyse Software.

21. Cliquez sur **Enregistrer** pour créer une politique.
    Un message s'affiche pour permettre à l'administrateur de planifier cette politique sur les périphériques en fonction du groupe.
22. Sélectionnez **Oui** pour planifier une tâche sur la même page.
23. Sélectionnez l'une des options suivantes :
    - **Immédiatement** : le serveur exécute la tâche immédiatement.
    - **Sur le fuseau horaire du périphérique** : le serveur crée une tâche pour chaque fuseau horaire du périphérique et planifie la tâche à la date et à l'heure sélectionnées du fuseau horaire du périphérique.
    - **Sur le fuseau horaire sélectionné** : le serveur crée une tâche à exécuter à la date et à l'heure du fuseau horaire désigné.
24. Pour créer la tâche, cliquez sur **Aperçu**. Les planifications sont affichées sur la page suivante.
25. Vous pouvez consulter l'état de la tâche en accédant à la page **Tâches**.

Créer et déployer une politique d'application avancée pour les Thin Clients Wyse Software

Étapes

1. Copiez l'application et les scripts de pré-/post-installation (si nécessaire) pour effectuer le déploiement sur les Thin Clients.
2. Enregistrez l'application et les scripts de pré-/post-installation dans le dossier thinClientApps de la logithèque locale ou de Wyse Management Suite Repository.
3. Accédez à **Applications et données** > **Inventaire d'applications** > **Thin Client Wyse Software**, puis vérifiez que l'application est enregistrée.
4. Accédez à **Applications et données** > **Politiques d'application** > **Thin Client Wyse Software**.
5. Cliquez sur **Ajouter une politique avancée**.
   La page **Ajouter une politique d'application avancée** s'affiche.
6. Saisissez un **nom de politique**.
7. Dans la liste déroulante **Groupe**, sélectionnez un groupe.
8. Cochez la case **Sous-groupes** pour appliquer la politique aux sous-groupes.
9. Dans la liste déroulante **Tâche**, sélectionnez la tâche.
10. Dans la liste déroulante **Type de système d'exploitation**, sélectionnez le système d'exploitation.
11. Cochez la case **Fichiers de filtre basés sur les extensions** pour filtrer les applications.
12. Cliquez sur **Ajouter une application**, et sélectionnez une ou plusieurs applications sous **Applications**. Pour chaque application, vous pouvez sélectionner un script de pré- et post-installation sous **Pré-installation**, **Post-installation** et **Paramètres d'installation**.
13. Si vous souhaitez que le système redémarre une fois l'application installée, sélectionnez **Redémarrage**.
14. Cliquez sur **Ajouter une application** et répétez l'étape pour ajouter plusieurs applications.

    REMARQUE : Pour arrêter la politique d'application au premier échec, sélectionnez **Activer la dépendance d'application**. Si cette option n'est pas sélectionnée, l'échec d'une application n'affecte pas la mise en œuvre de la politique.

    Si les fichiers de l'application sont disponibles sur plusieurs référentiels, le nombre de référentiels s'affiche à côté du nom de fichier.
15. Pour déployer cette politique sur un système d'exploitation ou une plate-forme spécifiques, sélectionnez **Filtre de sous-type de SE** ou **Filtre de plate-forme**.
16. Indiquez la durée d'affichage en minutes de la boîte de dialogue de message sur le client.
    Un message s'affiche sur le client, ce qui vous laisse le temps de sauvegarder votre travail avant le début de l'installation.
17. Pour autoriser un retard dans la mise en œuvre de la politique, cochez la case **Autoriser le retard d'exécution de la politique**. Si cette option est sélectionnée, les menus déroulants suivants s'activent :

- Dans la liste déroulante **Nombre max. d'heures par retard**, sélectionnez le nombre maximal d'heures (1 à 24 heures) pendant lesquelles vous pouvez retarder l'exécution de la politique.
- Dans la liste déroulante **Retards max.**, sélectionnez le nombre de fois (de 1 à 3) que vous pouvez retarder l'exécution de la politique.

18. Dans la liste déroulante **Appliquer automatiquement la politique**, sélectionnez l'une des options suivantes :
    - **Ne pas appliquer automatiquement** : les politiques ne sont pas automatiquement appliquées aux périphériques.
    - **Appliquer la politique aux nouveaux appareils** : la politique est automatiquement appliquée à un appareil enregistré qui appartient à un groupe sélectionné ou à l'appareil qui est déplacé vers un groupe sélectionné. Lorsque cette option est sélectionnée, la politique est appliquée à tous les nouveaux appareils qui sont enregistrés dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe. L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés.
    - **Appliquer la politique aux périphériques lors de la vérification** : la politique est automatiquement appliquée au périphérique lors de la vérification. Lorsque cette option est sélectionnée, la politique est appliquée à tous les appareils présents dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe immédiatement ou à une heure planifiée avant l'enregistrement de l'appareil, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe.

    REMARQUE : L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés dans Wyse Management Suite.

    REMARQUE : Pour les appareils Windows, spécifiez les paramètres d'installation silencieuse pour les fichiers .exe afin d'exécuter l'application en mode silencieux. Par exemple, **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**

19. Cochez la case **Ignorer la vérification du filtre d'écriture** pour ignorer les cycles du filtre d'écriture. Cette option s'applique aux périphériques des systèmes d'exploitation Windows Embedded Standard et aux périphériques Thin Client Wyse Software.
20. Pour arrêter le processus d'installation après une valeur définie, spécifiez le nombre de minutes dans le champ **Délai d'expiration de l'installation de l'application**. La valeur par défaut est 60 minutes.

    REMARQUE : L'option **Délai d'expiration de l'installation de l'application** s'applique uniquement aux périphériques Windows Embedded Standard et aux clients légers Wyse Software.

21. Cliquez sur **Enregistrer** pour créer une politique.
    Un message s'affiche pour permettre à l'administrateur de planifier cette politique sur les périphériques en fonction du groupe.
22. Sélectionnez **Oui** pour planifier une tâche sur la même page.
23. Sélectionnez l'une des options suivantes :
    - **Immédiatement** : le serveur exécute la tâche immédiatement.
    - **Sur le fuseau horaire du périphérique** : le serveur crée une tâche pour chaque fuseau horaire du périphérique et planifie la tâche à la date et à l'heure sélectionnées du fuseau horaire du périphérique.
    - **Sur le fuseau horaire sélectionné** : le serveur crée une tâche à exécuter à la date et à l'heure du fuseau horaire désigné.
24. Pour créer la tâche, cliquez sur **Aperçu**. Les planifications sont affichées sur la page suivante.
25. Vous pouvez consulter l'état de la tâche en accédant à la page **Tâches**.

Créer et déployer une politique d'application standard pour Dell Hybrid Clients

Étapes

1. Dans le référentiel local, accédez à **hybridClientApps**, puis copiez l'application dans le dossier.

   REMARQUE : Vous ne pouvez déployer et installer que des applications signées par Dell sur Dell Hybrid Clients.

2. Accédez à **Applications et données** > **Inventaire d'applications** > **Client hybride**, puis vérifiez que l'application est enregistrée dans Wyse Management Suite.

   REMARQUE : L'interface de l'inventaire d'applications met environ deux minutes à remplir les programmes récemment ajoutés.

3. Accédez à **Applications et données** > **Politiques d'application** > **Client hybride**.
4. Cliquez sur **Ajouter une politique**.
   La fenêtre **Ajouter une politique d'application standard** s'affiche.

5. Saisissez un **nom de politique**.
6. Dans la liste déroulante **Groupe**, sélectionnez un groupe.
7. Dans la liste déroulante **Tâche**, sélectionnez la tâche.
8. Dans la liste déroulante **Type de système d'exploitation**, sélectionnez le système d'exploitation.
9. Dans la liste déroulante **Application**, sélectionnez l'application.
   Si les fichiers de l'application sont disponibles sur plusieurs référentiels, le nombre de référentiels s'affiche à côté du nom de fichier.
10. Pour déployer cette politique sur un système d'exploitation ou une plate-forme spécifiques, sélectionnez **Filtre de sous-type de SE** ou **Filtre de plate-forme**.
11. Dans le champ **Paramètres d'installation**, saisissez les paramètres d'installation pour l'application sélectionnée.
12. Dans la liste déroulante **Appliquer automatiquement la politique**, sélectionnez l'une des options suivantes :
    - **Ne pas appliquer automatiquement** : les politiques ne sont pas automatiquement appliquées aux périphériques.
    - **Appliquer la politique aux nouveaux appareils** : la politique est automatiquement appliquée à un appareil enregistré qui appartient à un groupe sélectionné ou à l'appareil qui est déplacé vers un groupe sélectionné. Lorsque cette option est sélectionnée, la politique est appliquée à tous les nouveaux appareils qui sont enregistrés dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe. L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés.
    - **Appliquer la politique aux périphériques lors de la vérification** : la politique est automatiquement appliquée au périphérique lors de la vérification. Lorsque cette option est sélectionnée, la politique est appliquée à tous les appareils présents dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe immédiatement ou à une heure planifiée avant l'enregistrement de l'appareil, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe.

    REMARQUE : L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés dans Wyse Management Suite.
13. Indiquez le nombre de minutes pendant lesquelles la boîte de dialogue du message doit être affichée sur le client dans la zone **Délai d'expiration (1-999 min)**. La fonctionnalité Délai d'expiration affiche un message sur le client, ce qui vous laisse le temps de sauvegarder votre travail avant le début de l'installation.
14. Pour arrêter le processus d'installation après une valeur définie, spécifiez le nombre de minutes dans le champ **Délai d'expiration de l'installation de l'application**. La valeur par défaut est 60 minutes.
15. Cliquez sur **Enregistrer** pour créer une politique.
    Un message s'affiche pour permettre à l'administrateur de planifier cette politique sur les périphériques en fonction du groupe.
16. Sélectionnez **Oui** pour planifier une tâche sur la même page.
17. Sélectionnez l'une des options suivantes :
    - **Immédiatement** : le serveur exécute la tâche immédiatement.
    - **Sur le fuseau horaire du périphérique** : le serveur crée une tâche pour chaque fuseau horaire du périphérique et planifie la tâche à la date et à l'heure sélectionnées du fuseau horaire du périphérique.
    - **Sur le fuseau horaire sélectionné** : le serveur crée une tâche à exécuter à la date et à l'heure du fuseau horaire désigné.
18. Pour créer la tâche, cliquez sur **Aperçu**. Les planifications sont affichées sur la page suivante.
19. Vous pouvez consulter l'état de la tâche en accédant à la page **Tâches**.

Créer et déployer une politique d'application avancée pour Dell Hybrid Clients

Étapes

1. Copiez l'application et les scripts d'installation (si nécessaire) pour les déployer sur les clients légers.

   REMARQUE : Vous ne pouvez déployer et installer que des applications et des scripts signés par Dell sur Dell Hybrid Clients.
2. Copiez l'application et les scripts d'installation dans le dossier `hybridClientApps` du référentiel local ou du référentiel de Wyse Management Suite.
3. Accédez à **Applications et données** > **Inventaire d'applications** > **Client hybride** et vérifiez que l'application est enregistrée.
4. Accédez à **Applications et données** > **Politiques d'application** > **Client hybride**.
5. Cliquez sur **Ajouter une politique avancée**.
   La page **Ajouter une politique d'application avancée** s'affiche.

6. Saisissez un **nom de politique**.
7. Dans la liste déroulante **Groupe**, sélectionnez un groupe.
8. Cochez la case **Sous-groupes** pour appliquer la politique aux sous-groupes.
9. Dans la liste déroulante **Tâche**, sélectionnez la tâche.
10. Dans la liste déroulante **Type de système d'exploitation**, sélectionnez le système d'exploitation.
11. Cochez la case **Fichiers de filtre basés sur les extensions** pour filtrer les applications.
12. Cliquez sur **Ajouter une application**, et sélectionnez une ou plusieurs applications sous **Applications**. Pour chaque application, vous pouvez sélectionner un script de pré- et post-installation sous **Pré-installation**, **Post-installation** et **Paramètres d'installation**.
13. Si vous souhaitez que le système redémarre une fois l'application installée, sélectionnez **Redémarrage**.
14. Cliquez sur **Ajouter une application** et répétez l'étape pour ajouter plusieurs applications.

    REMARQUE : Pour arrêter la politique d'application au premier échec, sélectionnez **Activer la dépendance d'application**. Si cette option n'est pas sélectionnée, l'échec d'une application n'affecte pas la mise en œuvre de la politique.

    Si les fichiers de l'application sont disponibles sur plusieurs référentiels, le nombre de référentiels s'affiche à côté du nom de fichier.
15. Pour déployer cette politique sur un système d'exploitation ou une plate-forme spécifiques, sélectionnez **Filtre de sous-type de SE** ou **Filtre de plate-forme**.
16. Indiquez la durée d'affichage en minutes de la boîte de dialogue de message sur le client.
    Un message s'affiche sur le client, ce qui vous laisse le temps de sauvegarder votre travail avant le début de l'installation.
17. Pour autoriser un retard dans la mise en œuvre de la politique, cochez la case **Autoriser le retard d'exécution de la politique**. Si cette option est sélectionnée, les menus déroulants suivants s'activent :
    - Dans la liste déroulante **Nombre max. d'heures par retard**, sélectionnez le nombre maximal d'heures (1 à 24 heures) pendant lesquelles vous pouvez retarder l'exécution de la politique.
    - Dans la liste déroulante **Retards max.**, sélectionnez le nombre de fois (de 1 à 3) que vous pouvez retarder l'exécution de la politique.
18. Dans la liste déroulante **Appliquer automatiquement la politique**, sélectionnez l'une des options suivantes :
    - **Ne pas appliquer automatiquement** : les politiques ne sont pas automatiquement appliquées aux périphériques.
    - **Appliquer la politique aux nouveaux appareils** : la politique est automatiquement appliquée à un appareil enregistré qui appartient à un groupe sélectionné ou à l'appareil qui est déplacé vers un groupe sélectionné. Lorsque cette option est sélectionnée, la politique est appliquée à tous les nouveaux appareils qui sont enregistrés dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe. L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés.
    - **Appliquer la politique aux périphériques lors de la vérification** : la politique est automatiquement appliquée au périphérique lors de la vérification. Lorsque cette option est sélectionnée, la politique est appliquée à tous les appareils présents dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe immédiatement ou à une heure planifiée avant l'enregistrement de l'appareil, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe.

    REMARQUE : L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés dans Wyse Management Suite.
19. Indiquez le nombre de minutes pendant lesquelles la boîte de dialogue du message doit être affichée sur le client dans la zone **Délai d'expiration (1-999 min)**. La fonctionnalité Délai d'expiration affiche un message sur le client, ce qui vous laisse le temps de sauvegarder votre travail avant le début de l'installation.
20. Pour arrêter le processus d'installation après une valeur définie, spécifiez le nombre de minutes dans le champ **Délai d'expiration de l'installation de l'application**. La valeur par défaut est 60 minutes.
21. Cliquez sur **Enregistrer** pour créer une politique.
    Un message s'affiche pour permettre à l'administrateur de planifier cette politique sur les périphériques en fonction du groupe.
22. Sélectionnez **Oui** pour planifier une tâche sur la même page.
23. Sélectionnez l'une des options suivantes :
    - **Immédiatement** : le serveur exécute la tâche immédiatement.
    - **Sur le fuseau horaire du périphérique** : le serveur crée une tâche pour chaque fuseau horaire du périphérique et planifie la tâche à la date et à l'heure sélectionnées du fuseau horaire du périphérique.
    - **Sur le fuseau horaire sélectionné** : le serveur crée une tâche à exécuter à la date et à l'heure du fuseau horaire désigné.
24. Pour créer la tâche, cliquez sur **Aperçu**. Les planifications sont affichées sur la page suivante.
25. Vous pouvez consulter l'état de la tâche en accédant à la page **Tâches**.

Créer et déployer une politique d'application standard pour Dell Generic Clients

Étapes

1. Dans le référentiel local, accédez à **genericClientApps**, puis copiez les packages d'application dans le dossier.

   REMARQUE : Vous pouvez déployer et installer uniquement des applications signées par Dell (scripts DHC Fish, packages DCA-Enabler, packages DHC ou fichiers image ISO DHC) sur Dell Generic Clients.

2. Accédez à **Applications et données** > **Inventaire d'applications** > **Generic Client**, puis vérifiez que l'application est enregistrée dans Wyse Management Suite.

   REMARQUE : L'interface de l'inventaire d'applications met environ deux minutes à remplir les programmes récemment ajoutés.

3. Accédez à **Applications et données** > **Politiques d'application** > **Generic Client**.
4. Cliquez sur **Ajouter une politique**.
   La fenêtre **Ajouter une politique d'application standard** s'affiche.
5. Saisissez un **nom de politique**.
6. Dans la liste déroulante **Groupe**, sélectionnez un groupe.
7. Dans la liste déroulante **Tâche**, sélectionnez la tâche.
8. Dans la liste déroulante **Type de système d'exploitation**, sélectionnez le système d'exploitation.
9. Dans la liste déroulante **Application**, sélectionnez l'application.
   Si les fichiers de l'application sont disponibles sur plusieurs référentiels, le nombre de référentiels s'affiche à côté du nom de fichier.
10. Pour déployer cette politique sur un système d'exploitation ou une plate-forme spécifiques, sélectionnez **Filtre de sous-type de SE** ou **Filtre de plate-forme**.
11. Dans la liste déroulante **Appliquer automatiquement la politique**, sélectionnez l'une des options suivantes :
    - **Ne pas appliquer automatiquement** : les politiques ne sont pas automatiquement appliquées aux périphériques.
    - **Appliquer la politique aux nouveaux appareils** : la politique est automatiquement appliquée à un appareil enregistré qui appartient à un groupe sélectionné ou à l'appareil qui est déplacé vers un groupe sélectionné. Lorsque cette option est sélectionnée, la politique est appliquée à tous les nouveaux appareils qui sont enregistrés dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe. L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés.
    - **Appliquer la politique aux périphériques lors de la vérification** : la politique est automatiquement appliquée au périphérique lors de la vérification. Lorsque cette option est sélectionnée, la politique est appliquée à tous les appareils présents dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe immédiatement ou à une heure planifiée avant l'enregistrement de l'appareil, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe.

    REMARQUE : L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés dans Wyse Management Suite.

12. Indiquez le nombre de minutes pendant lesquelles la boîte de dialogue du message doit être affichée sur le client dans la zone **Délai d'expiration (1-999 min)**. Délai d'expiration affiche un message sur le client, ce qui vous laisse le temps d'enregistrer votre travail avant le début de l'installation.
13. Pour arrêter le processus d'installation après une valeur définie, spécifiez le nombre de minutes dans le champ **Délai d'expiration de l'installation de l'application**. La valeur par défaut est 60 minutes.
14. Cliquez sur **Enregistrer** pour créer une politique.
    Un message s'affiche pour permettre à l'administrateur de planifier cette politique sur les périphériques en fonction du groupe.
15. Sélectionnez **Oui** pour planifier une tâche sur la même page.
16. Sélectionnez l'une des options suivantes :
    - **Immédiatement** : le serveur exécute la tâche immédiatement.
    - **Sur le fuseau horaire du périphérique** : le serveur crée une tâche pour chaque fuseau horaire du périphérique et planifie la tâche à la date et à l'heure sélectionnées du fuseau horaire du périphérique.
    - **Sur le fuseau horaire sélectionné** : le serveur crée une tâche à exécuter à la date et à l'heure du fuseau horaire désigné.
17. Pour créer la tâche, cliquez sur **Aperçu**. Les planifications sont affichées sur la page suivante.
18. Vous pouvez consulter l'état de la tâche en accédant à la page **Tâches**.

Créer et déployer une politique d'application avancée pour Dell Generic Clients

Étapes

1. Copiez l'application et les scripts d'installation (si nécessaire) dans le dossier `genericClientApps` du référentiel local ou du référentiel à distance de Wyse Management Suite.

   REMARQUE : Vous pouvez déployer et installer uniquement des applications et des scripts signés par Dell (scripts DHC Fish, packages DCA-Enabler, packages DHC ou fichiers image ISO DHC) sur Dell Generic Clients.

2. Accédez à **Applications et données** > **Inventaire d'applications** > **Generic Client** et vérifiez que l'application est enregistrée.
3. Accédez à **Applications et données** > **Politiques d'application** > **Generic Client**.
4. Cliquez sur **Ajouter une politique avancée**.
   La page **Ajouter une politique d'application avancée** s'affiche.
5. Saisissez un **nom de politique**.
6. Dans la liste déroulante **Groupe**, sélectionnez un groupe.
7. Cochez la case **Sous-groupes** pour appliquer la politique aux sous-groupes.
8. Dans la liste déroulante **Tâche**, sélectionnez la tâche.
9. Dans la liste déroulante **Type de système d'exploitation**, sélectionnez le système d'exploitation.
10. Cochez la case **Fichiers de filtre basés sur les extensions** pour filtrer les applications.
11. Cliquez sur **Ajouter une application**, et sélectionnez une ou plusieurs applications sous **Applications**.
12. Si vous souhaitez que le système redémarre une fois l'application installée, sélectionnez **Redémarrage**.
13. Cliquez sur **Ajouter une application** et répétez l'étape pour ajouter plusieurs applications.

    REMARQUE : Pour arrêter la politique d'application au premier échec, sélectionnez **Activer la dépendance d'application**. Si cette option n'est pas sélectionnée, l'échec d'une application n'affecte pas la mise en œuvre de la politique.

    Si les fichiers de l'application sont disponibles sur plusieurs référentiels, le nombre de référentiels s'affiche à côté du nom de fichier.
14. Pour déployer cette politique sur un système d'exploitation ou une plate-forme spécifiques, sélectionnez **Filtre de sous-type de SE** ou **Filtre de plate-forme**.
15. Indiquez la durée d'affichage en minutes de la boîte de dialogue de message sur le client.
    Un message s'affiche sur le client, ce qui vous laisse le temps d'enregistrer votre travail avant le début de l'installation.
16. Pour activer le retard de mise en œuvre de la politique, cochez la case **Autoriser le retard d'exécution de la politique**. Si cette option est sélectionnée, les menus déroulants suivants s'activent :
    - Dans la liste déroulante **Nombre max. d'heures par retard**, sélectionnez le nombre maximal d'heures (1 à 24 heures) pendant lesquelles vous pouvez retarder l'exécution de la politique.
    - Dans la liste déroulante **Retards max.**, sélectionnez le nombre de fois (de 1 à 3) que vous pouvez retarder l'exécution de la politique.
17. Dans la liste déroulante **Appliquer automatiquement la politique**, sélectionnez l'une des options suivantes :
    - **Ne pas appliquer automatiquement** : les politiques ne sont pas automatiquement appliquées aux périphériques.
    - **Appliquer la politique aux nouveaux appareils** : la politique est automatiquement appliquée à un appareil enregistré qui appartient à un groupe sélectionné ou à l'appareil qui est déplacé vers un groupe sélectionné. Lorsque cette option est sélectionnée, la politique est appliquée à tous les nouveaux appareils qui sont enregistrés dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe. L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés.
    - **Appliquer la politique aux périphériques lors de la vérification** : la politique est automatiquement appliquée au périphérique lors de la vérification. Lorsque cette option est sélectionnée, la politique est appliquée à tous les appareils présents dans le groupe. Pour exécuter la tâche sur les appareils existants présents dans le groupe immédiatement ou à une heure planifiée avant l'enregistrement de l'appareil, vous devez planifier la politique. Une fois que vous avez planifié la politique, l'état de la tâche affiche le nombre d'appareils déjà présents dans le groupe.

    REMARQUE : L'état de la tâche n'affiche pas le nombre d'appareils nouvellement ajoutés qui sont enregistrés dans Wyse Management Suite.

18. Indiquez le nombre de minutes pendant lesquelles la boîte de dialogue du message doit être affichée sur le client dans la zone **Délai d'expiration (1-999 min)**. Délai d'expiration affiche un message sur le client, ce qui vous laisse le temps d'enregistrer votre travail avant le début de l'installation.

19. Pour arrêter le processus d'installation après une valeur définie, spécifiez le nombre de minutes dans le champ **Délai d'expiration de l'installation de l'application**. La valeur par défaut est 60 minutes.
20. Cliquez sur **Enregistrer** pour créer une politique.
    Un message s'affiche pour permettre à l'administrateur de planifier cette politique sur les périphériques en fonction du groupe.
21. Sélectionnez **Oui** pour planifier une tâche sur la même page.
22. Sélectionnez l'une des options suivantes :
    - **Immédiatement** : le serveur exécute la tâche immédiatement.
    - **Sur le fuseau horaire du périphérique** : le serveur crée une tâche pour chaque fuseau horaire du périphérique et planifie la tâche à la date et à l'heure sélectionnées du fuseau horaire du périphérique.
    - **Sur le fuseau horaire sélectionné** : le serveur crée une tâche à exécuter à la date et à l'heure du fuseau horaire désigné.
23. Pour créer la tâche, cliquez sur **Aperçu**. Les planifications sont affichées sur la page suivante.
24. Vous pouvez consulter l'état de la tâche en accédant à la page **Tâches**.

Politique d'image

Wyse Management Suite prend en charge les types suivants de politiques de déploiement d'image de système d'exploitation :

- Ajouter le système d'exploitation Windows Embedded Standard et des images ThinLinux au référentiel
- Ajouter le firmware ThinOS au référentiel
- Ajouter le fichier de package ThinOS au référentiel
- Ajouter le fichier BIOS ThinOS au référentiel
- Ajouter le firmware Teradici au référentiel
- Créer des politiques des images Windows Embedded Standard et ThinLinux
- Créer de politiques d'image de Dell Hybrid Client

Ajouter le système d'exploitation Windows Embedded Standard et des images ThinLinux au référentiel

Prérequis

- Si vous utilisez Wyse Management Suite avec un déploiement dans le Cloud, accédez à **Administration de portail** > **Paramètres de la console** > **Référentiel de fichiers**. Cliquez sur **Télécharger la version 3.2.0** pour télécharger le fichier `WMS_Repo.exe` et installez le programme d'installation du référentiel Wyse Management Suite.
- Si vous utilisez Wyse Management Suite avec un déploiement local, le référentiel local est installé au cours du processus d'installation de Wyse Management Suite.

Étapes

1. Copiez les images du système d'exploitation Windows Embedded Standard ou les images ThinLinux dans le dossier `<Repository Location>\repository\osImages\zipped`.

   Wyse Management Suite extrait les fichiers à partir du dossier compressé et les télécharge à l'emplacement `<Repository Location>\repository\osImages\valid`. L'extraction de l'image peut prendre plusieurs minutes selon la taille de l'image.

   REMARQUE : Pour le système d'exploitation ThinLinux, téléchargez l'image Merlin (`1.0.7_3030LT_merlin.exe`, par exemple), puis copiez-la dans le dossier `<Repository Location>\Repository\osImages\zipped`.

   L'image est ajoutée au référentiel.
2. Accédez à **Applications et données** > **Référentiel d'images SE** > **WES/ThinLinux** pour afficher l'image enregistrée.

Ajouter le firmware ThinOS au référentiel

Étapes

1. Dans l'onglet **Applications et données**, sous le **référentiel d'images SE**, cliquez sur **ThinOS**.
2. Cliquez sur **Ajouter un fichier de micrologiciel**.
   L'écran **Ajouter un fichier** s'affiche.
3. Pour sélectionner un fichier, cliquez sur **Parcourir** et accédez à l'emplacement où se trouve votre fichier.

4. Saisissez la description de votre fichier.
5. Cochez cette case si vous souhaitez remplacer un fichier existant.
6. Cliquez sur **Télécharger**.

   REMARQUE : Le fichier est ajouté au référentiel lorsque vous cochez la case, mais il n'est attribué à aucun des appareils ou groupes. Pour déployer un firmware sur un appareil ou un groupe d'appareils, accédez à la page de configuration de l'appareil ou du groupe correspondant.

Ajouter le fichier BIOS ThinOS au référentiel

Étapes

1. Dans l'onglet **Applications et données**, sous le **référentiel d'images SE**, cliquez sur **ThinOS**.
2. Cliquez sur **Ajouter un fichier de BIOS**.
   L'écran **Ajouter un fichier** s'affiche.
3. Pour sélectionner un fichier, cliquez sur **Parcourir** et accédez à l'emplacement où se trouve votre fichier.
4. Saisissez la description de votre fichier.
5. Cochez cette case si vous souhaitez remplacer un fichier existant.
6. Sélectionnez la plate-forme dans la liste déroulante des types de plates-formes BIOS.
7. Cliquez sur **Télécharger**.

   REMARQUE : Le fichier est ajouté au référentiel lorsque vous cochez la case, mais il n'est attribué à aucun des appareils ou groupes. Pour déployer le fichier BIOS sur un appareil ou un groupe d'appareils, accédez à la page de configuration de l'appareil ou du groupe correspondant.

Ajouter un fichier de package ThinOS au référentiel

Étapes

1. Dans l'onglet **Applications et données**, sous le **référentiel d'images SE**, cliquez sur **ThinOS**.
2. Cliquez sur **Ajouter un fichier de package**.
   L'écran **Ajouter un fichier** s'affiche.
3. Pour sélectionner un fichier, cliquez sur **Parcourir** et accédez à l'emplacement où se trouve votre fichier.
4. Saisissez la description de votre fichier.
5. Cliquez sur **Télécharger**.

   REMARQUE : Si l'application existe dans le référentiel public, la référence de l'application est ajoutée à l'inventaire. Sinon, l'application est téléchargée vers le référentiel public et la référence est ajoutée à l'inventaire. De même, les packages du BIOS et du firmware ThinOS téléchargés par l'opérateur ne peuvent pas être supprimés par les administrateurs des clients.

Créer des politiques des images Windows Embedded Standard et ThinLinux

Étapes

1. Dans l'onglet **Applications et données**, sous **Politiques d'image SE**, cliquez sur **WES/ThinLinux**.
2. Cliquez sur **Ajouter une politique**.
   L'écran **Ajouter une politique WES / ThinLinux** s'affiche.
3. Dans la page **Ajouter une politique WES / ThinLinux**, procédez comme suit :
   a. Saisissez un **nom de politique**.
   b. Dans le menu déroulant **Groupe**, sélectionnez un groupe.
   c. Dans le menu déroulant **Type de système d'exploitation**, sélectionnez le type de système d'exploitation.
   d. Dans le menu déroulant **Filtre de sous-type de SE**, sélectionnez le filtre de sous-type de SE.

e. Si vous souhaitez déployer une image sur un système d'exploitation ou une plate-forme spécifique, sélectionnez **Filtre de sous-type de SE** ou **Filtre de plate-forme**.
f. Dans le menu déroulant **Image SE**, sélectionnez le fichier d'image souhaité.
g. Dans le menu déroulant **Règle**, sélectionnez l'une des règles suivantes à définir pour la politique d'image :
   - Mise à niveau uniquement
   - Autoriser le passage à une version antérieure
   - Forcer cette version
h. Dans le menu déroulant **Appliquer automatiquement la politique**, sélectionnez l'une des options suivantes :
   - Ne pas appliquer automatiquement : la politique d'image n'est pas appliquée automatiquement à un appareil enregistré avec Wyse Management Suite.
   - Appliquer la politique aux nouveaux appareils : la politique d'image est appliquée à un nouvel appareil enregistré avec Wyse Management Suite.
   - Appliquer la politique aux appareils lors de la vérification : la politique d'image est appliquée à un nouvel appareil enregistré avec Wyse Management Suite lors de la vérification.

4. Cliquez sur **Enregistrer**.

Ajouter le firmware ThinOS 9.x au référentiel

Étapes

1. Connectez-vous à Wyse Management Suite.
2. Dans l'onglet **Applications et données**, sous **Référentiel d'images SE**, cliquez sur **ThinOS 9.x**.
3. Cliquez sur **Ajouter un fichier de firmware**.
   L'écran **Ajouter un fichier** s'affiche.
4. Pour sélectionner un fichier, cliquez sur **Parcourir** et accédez à l'emplacement où se trouve votre fichier.
5. Saisissez la description de votre fichier.
6. Cochez cette case si vous souhaitez remplacer un fichier existant.
7. Cliquez sur **Télécharger**.

   REMARQUE : Le fichier est ajouté au référentiel lorsque vous cochez la case, mais il n'est attribué à aucun des appareils ou groupes. Pour déployer un firmware sur un appareil ou un groupe d'appareils, accédez à la page de configuration de l'appareil ou du groupe correspondant.

   REMARQUE : L'opérateur peut télécharger le firmware à partir du compte opérateur et celui-ci est visible par toutes les organisations. Les organisations ne peuvent pas supprimer ou modifier les fichiers.

Ajouter le fichier BIOS de ThinOS 9.x au référentiel

Étapes

1. Dans l'onglet **Applications et données**, sous **Référentiel d'images SE**, cliquez sur **ThinOS 9.x**.
2. Cliquez sur **Ajouter un fichier de BIOS**.
   L'écran **Ajouter un fichier** s'affiche.
3. Pour sélectionner un fichier, cliquez sur **Parcourir** et accédez à l'emplacement où se trouve votre fichier.
4. Saisissez la description de votre fichier.
5. Cochez cette case si vous souhaitez remplacer un fichier existant.
6. Sélectionnez la plate-forme dans la liste déroulante des types de plates-formes BIOS.
7. Cliquez sur **Télécharger**.

   REMARQUE : Le fichier est ajouté au référentiel lorsque vous cochez la case, mais il n'est attribué à aucun des appareils ou groupes. Pour déployer le fichier BIOS sur un appareil ou un groupe d'appareils, accédez à la page de configuration de l'appareil ou du groupe correspondant.

   REMARQUE : L'opérateur peut télécharger le firmware à partir du compte opérateur et celui-ci est visible par toutes les organisations. Les organisations ne peuvent pas supprimer ou modifier les fichiers.

Ajout des packages d'application ThinOS au référentiel

Étapes

1. Connectez-vous à Wyse Management Suite à l'aide de vos informations d'identification de client.
2. Dans l'onglet **Applications et données**, sous **Référentiel d'images SE**, cliquez sur **ThinOS 9.x**.
3. Cliquez sur **Ajouter un fichier de package**.
   L'écran **Ajouter un package** s'affiche.
4. Pour sélectionner un fichier, cliquez sur **Parcourir** et accédez à l'emplacement où se trouve votre fichier.
   - Si le contrat EULA est intégré dans le package, les détails du contrat EULA du package et le nom des fournisseurs s'affichent. Vous pouvez cliquer sur les noms des fournisseurs pour lire le contrat de licence de chaque fournisseur. Cliquez sur **Accepter** pour charger le package. Vous pouvez sélectionner l'option **Ne plus afficher** si vous ne souhaitez plus voir les détails du contrat EULA du même fournisseur. Vous devez accepter le contrat de licence des packages individuellement. Le package n'est pas téléchargé si vous cliquez sur **Refuser**.
   - Si le contrat EULA n'est pas intégré dans le package, passez à l'étape 5.
5. Cliquez sur **Télécharger**.

   REMARQUE : L'opérateur peut télécharger le package à partir du compte opérateur et celui-ci est visible pour toutes les organisations. Les organisations ne peuvent pas supprimer ou modifier ces fichiers.

Création de politiques d'image de Dell Hybrid Client

Vous pouvez créer une politique d'image de Dell Hybrid Client pour convertir des Wyse 5070 Thin Clients exécutant Windows 10 IoT Enterprise, ThinLinux 2.x et Thinos 8.x vers des appareils Dell Hybrid Client.

Étapes

1. Dans l'onglet **Applications et données**, sous **Politiques d'image SE**, cliquez sur **Client hybride**.
2. Cliquez sur **Ajouter une politique**.
3. Dans la page **Ajouter une politique d'image des clients hybrides**, procédez comme suit :
   a. Saisissez un **nom de politique**.
   b. Dans le menu déroulant **Groupe**, sélectionnez un groupe.
   c. Dans le menu déroulant **Type de système d'exploitation**, sélectionnez le type de système d'exploitation.
   d. Dans le menu déroulant **Filtre de sous-type de SE**, sélectionnez le filtre de sous-type de SE.
   e. Si vous souhaitez déployer une image sur un système d'exploitation ou une plate-forme spécifique, sélectionnez **Filtre de sous-type de SE** ou **Filtre de plate-forme**.
   f. Dans le menu déroulant **Image SE**, sélectionnez le fichier d'image souhaité.
   g. Dans le menu déroulant **Règle**, sélectionnez **Forcer cette version**.
   h. Dans le menu déroulant **Appliquer automatiquement la politique**, sélectionnez l'une des options suivantes :
      - Ne pas appliquer automatiquement : la politique d'image n'est pas appliquée automatiquement à un appareil enregistré avec Wyse Management Suite.
      - Appliquer la politique aux nouveaux appareils : la politique d'image est appliquée à un nouvel appareil enregistré avec Wyse Management Suite.
4. Cliquez sur **Enregistrer**.

   REMARQUE : Le nombre de licences DHC doit être supérieur ou égal au nombre de Wyse 5070 Thin Clients convertis en appareils Dell Hybrid Client.

   REMARQUE : L'image du système d'exploitation de conversion DHC fournie au format compressé ou exe doit être copiée dans le dossier `\repository\osImages\zipped`. L'image du système d'exploitation DHC s'affiche sous **Applications et données** > **Référentiel d'images SE** > **Client hybride** après la synchronisation du référentiel.

   REMARQUE : Vous devez créer une politique d'image du système d'exploitation pour déployer l'image de conversion DHC vers des Wyse 5070 Thin Clients exécutant Windows Embedded, ThinLinux, ThinOS et ThinOS avec système d'exploitation PCoIP.

   REMARQUE : Assurez-vous que le package Merlin est mis à jour vers la version 408 ou supérieure pour les clients légers exécutant les systèmes d'exploitation Windows 10 IoT Enterprise et ThinLinux 2.x.

Gérer un référentiel de fichiers

Cette section vous permet d'afficher et de gérer les inventaires de référentiel de fichiers, tels que le fond d'écran, le logo, le fichier texte CLUF, le profil sans fil Windows et les fichiers de certificat.

Étapes

1. Dans l'onglet **Applications et données**, sous **Référentiel de fichiers**, cliquez sur **Inventaire**.
2. Cliquez sur **Ajouter un fichier**.

   L'écran **Ajouter un fichier** s'affiche.
3. Pour sélectionner un fichier, cliquez sur **Parcourir** et accédez à l'emplacement où se trouve votre fichier.
4. Dans le menu déroulant **Type**, sélectionnez l'option qui convient le mieux à votre type de fichier parmi les suivantes :
   - Certificat
   - Papier peint
   - Logo
   - Fichier texte CLUF
   - Profil sans fil Windows
   - Fichier INI
   - Paramètres régionaux
   - Mappages d'imprimante
   - Police
   - Hôtes
   - Règles

   REMARQUE : pour afficher la taille maximale et le format pris en charge des fichiers que vous pouvez charger, cliquez sur l'icône d'**information (i)**.
5. Cochez cette case si vous souhaitez remplacer un fichier existant.

   REMARQUE : Le fichier est ajouté au référentiel lorsque vous cochez la case, mais il n'est attribué à aucun des appareils ou groupes. Pour attribuer le fichier, accédez à la page de configuration des appareils respectifs.
6. Cliquez sur **Télécharger**.

Comment modifier le fond d'écran de tous les appareils appartenant au groupe marketing

Étapes

1. Accédez à l'onglet **Applications et données**.
2. Dans la barre de navigation du volet gauche, sélectionnez **Inventaire**.
3. Cliquez sur le bouton **Ajouter un fichier**.
4. Localisez et sélectionnez l'image que vous souhaitez utiliser comme fond d'écran.
5. Pour le type, sélectionnez **Fond d'écran**.
6. Saisissez la description, puis cliquez sur **Télécharger**.

Procédez comme suit pour modifier la politique de configuration d'un groupe en attribuant un nouveau fond d'écran :

1. Accédez à la page **Groupes et configurations**.
2. Sélectionnez un groupe de politiques.
3. Cliquez sur **Modifier les politiques**, puis sélectionnez **WES**.
4. Sélectionnez **Expérience de bureau**, puis cliquez sur **Configurer cet élément**.
5. Sélectionnez **Fond d'écran de bureau**.
6. Dans la liste déroulante, sélectionnez le fichier de fond d'écran.

7. Cliquez sur **Enregistrer et publier**.

Cliquez sur **Tâches** pour vérifier l'état de la politique de configuration. Vous pouvez cliquer sur le numéro en regard de l'indicateur de condition dans la colonne **Détails** pour afficher les appareils et leur état.

10

Gestion des règles

Cette section explique comment ajouter et gérer les règles dans la console Wyse Management Suite. Les options de filtrage disponibles sont les suivantes :

- **Enregistrement**
- **Attribution automatique d'appareils non gérés**
- **Notification d'alerte**

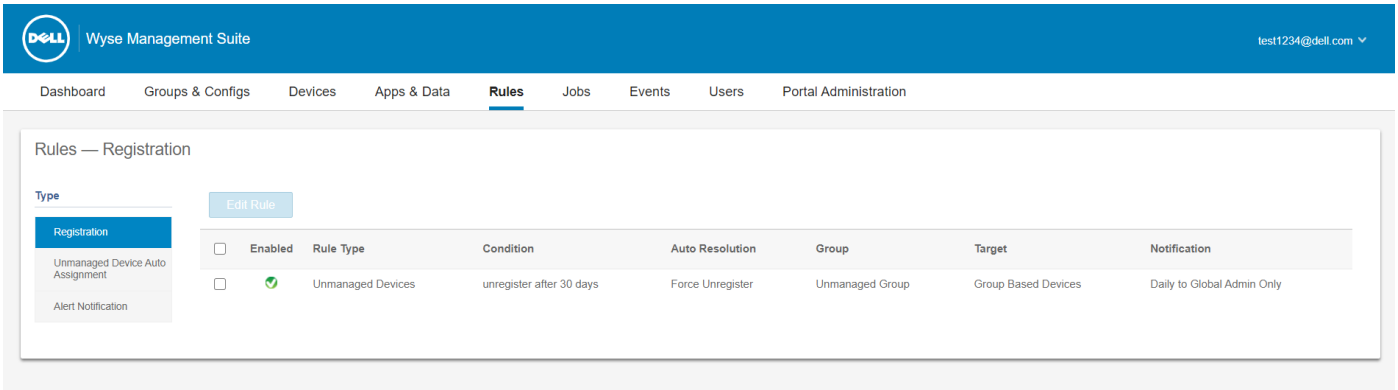


Figure 9. Page Règles

Sujets :

Modifier une règle d'enregistrement

Configurez les règles des appareils non gérés à l'aide de l'option **Enregistrement**.

Étapes

1. Cliquez sur **Règles**.
   La page **Règles** s'affiche.
2. Cliquez sur **Enregistrement** et sélectionnez l'option d'appareils non gérés.
3. Cliquez sur **Modifier une règle**.
   La fenêtre **Modifier une règle** s'affiche.

   Vous pouvez afficher les informations suivantes :
   - Règle
   - Description
   - Cible d'appareil
   - Groupe
4. Dans le menu déroulant, sélectionnez un client cible auquel appliquer l'option **Cible de notification** et la durée pour l'option **Fréquence de notification**.

REMARQUE : la fréquence de notification peut être configurée pour toutes les 4 heures, toutes les 12 heures, tous les jours ou toutes les semaines sur l'appareil cible.

5. Entrez le nombre de jours après lequel vous souhaitez appliquer la règle dans la zone **Appliquer la règle au bout de (1 à 30 jours)**.

   REMARQUE : Par défaut, l'enregistrement d'un appareil non géré est annulé au bout de 30 jours.

6. Cliquez sur **Enregistrer**.

Créer des règles d'attribution automatique pour les appareils non gérés

Étapes

1. Cliquez sur l'onglet **Règles**.
2. Sélectionnez l'option **Attribution automatique d'appareils non gérés**.
3. Cliquez sur l'onglet **Ajouter une règle**.
4. Saisissez le **nom** et sélectionnez le **groupe de destination**.
5. Cliquez sur l'option **Ajouter une condition**, puis sélectionnez les conditions pour les règles attribuées.
6. Cliquez sur **Enregistrer**.

   La règle est affichée dans la liste de groupes non gérés. Cette règle est appliquée automatiquement et l'appareil est répertorié dans le groupe de destination.

   REMARQUE : Les règles ne sont pas appliquées aux appareils présentant l'état **Inscription en attente**.

Modifier une règle d'attribution automatique d'appareils non gérés

Étapes

1. Cliquez sur l'onglet **Règles**.
2. Sélectionnez l'option **Attribution automatique d'appareils non gérés**.
3. Sélectionnez une règle, puis cliquez sur l'option **Modifier**.
4. Saisissez le **nom** et sélectionnez le **groupe de destination**.
5. Cliquez sur l'option **Ajouter une condition**, puis sélectionnez les conditions pour les règles attribuées.
6. Cliquez sur **Enregistrer**.

Désactiver et supprimer une règle d'attribution automatique d'appareils non gérés

Étapes

1. Cliquez sur l'onglet **Règles**.
2. Sélectionnez l'option **Attribution automatique d'appareils non gérés**.
3. Sélectionnez une règle et cliquez sur l'option **Désactiver la règle**.
   La règle sélectionnée est désactivée.
4. Sélectionnez la règle désactivée, puis cliquez sur l'option **Supprimer la ou les règles désactivées**.
   La règle est supprimée.

Enregistrer l’ordre des règles

Prérequis

Si plusieurs règles s'appliquent aux appareils, vous pouvez modifier leur priorité.

Étapes

1. Cliquez sur l'onglet **Règles**.
2. Sélectionnez l'option **Attribution automatique d'appareils non gérés**.
3. Sélectionnez la règle à déplacer, puis déposez-la en tête de liste.
4. Cliquez sur **Enregistrer la commande de règle**.

REMARQUE : Vous ne pouvez pas modifier l’ordre des règles de préfixe IPV6.

Ajouter une règle de notification d’alerte

Étapes

1. Cliquez sur l'onglet **Règles**.
2. Sélectionnez l'option **Notification d'alerte**.
3. Cliquez sur **Ajouter une règle**.
   La fenêtre **Ajouter une règle** s'affiche.
4. Dans la liste déroulante **Règle**, sélectionnez une règle.
5. Saisissez la **description**.
6. Dans la liste déroulante **Groupe**, sélectionnez l'option de votre choix.
7. Dans le menu déroulant, sélectionnez un appareil cible auquel appliquer la **cible de notification** et la durée de la **Fréquence de notification**.
8. Cliquez sur **Enregistrer**.

Modifier une règle de notification d’alerte

Étapes

1. Cliquez sur l'onglet **Règles**.
2. Sélectionnez l'option **Notification d'alerte**.
3. Cliquez sur **Modifier une règle**.
   La fenêtre **Modifier une règle** s'affiche.
4. Dans la liste déroulante **Règle**, sélectionnez une règle.
5. Saisissez la **description**.
6. Dans la liste déroulante **Groupe**, sélectionnez un groupe.
7. Dans la liste déroulante, sélectionnez un appareil cible auquel appliquer la **Cible de notification** et la durée de la **Fréquence de notification**.
8. Cliquez sur **Enregistrer**.

Créer une règle pour annuler automatiquement l’enregistrement d’un appareil

Vous pouvez créer une règle pour annuler automatiquement l’enregistrement d’un appareil s’il ne s’enregistre pas dans Wyse Management Suite pendant un certain temps à partir de Wyse Management Suite 3.2.

Étapes

1. Cliquez sur l'onglet **Règles**.
2. Cliquez sur l'option **Échec de l'enregistrement**.

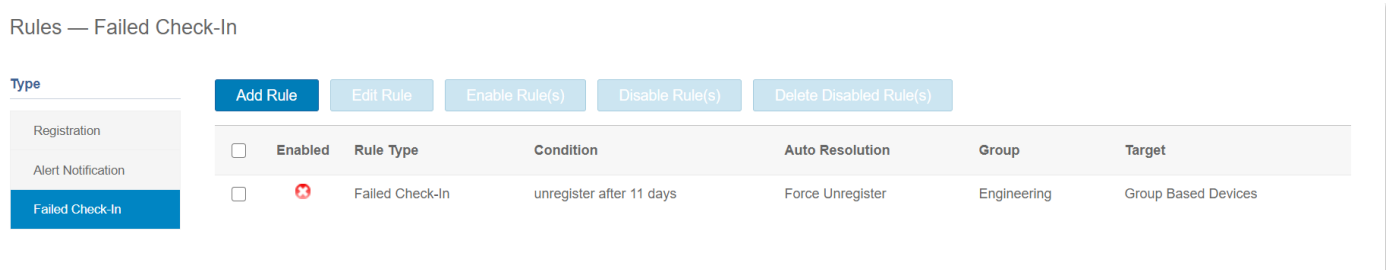


Figure 10. Onglet Échec de l'enregistrement

3. Cliquez sur **Ajouter une règle**.
   La fenêtre **Ajouter une règle** s'affiche.

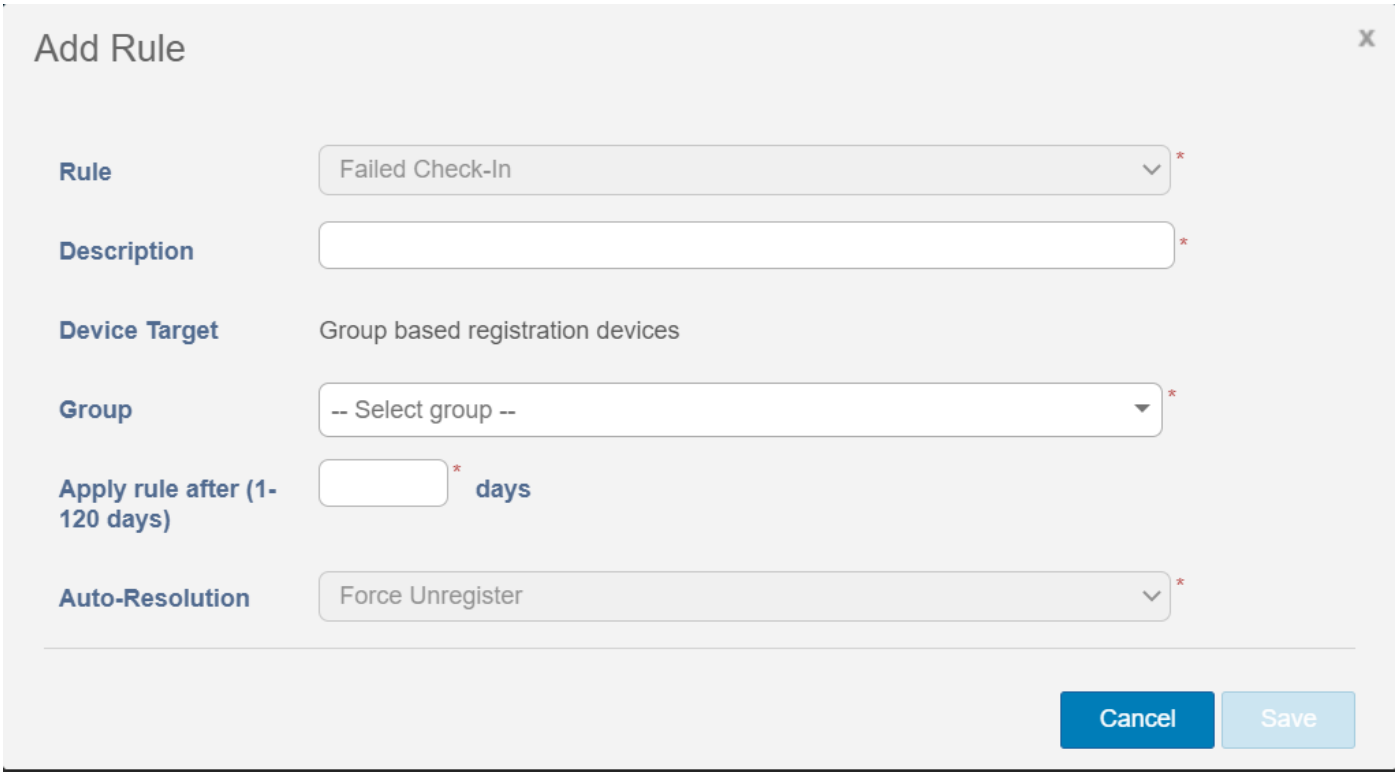


Figure 11. Ajouter une règle

4. Saisir une description pour la règle.
5. Sélectionnez le groupe dans lequel les enregistrements des appareils doivent être annulés.
6. Dans le champ **Appliquer la règle après (1 à 120 jours)**, saisissez la durée en jours après laquelle l'enregistrement de l'appareil est annulé sur Wyse Management Suite.

   REMARQUE : L'enregistrement de l'appareil est annulé sur Wyse Management Suite uniquement s'il ne s'enregistre pas pendant le nombre de jours spécifié.
7. Cliquez sur **Enregistrer**.
   Vous pouvez également modifier, activer, désactiver ou supprimer la règle.

11

Gestion des tâches

Cette section décrit la procédure à suivre pour planifier et gérer des tâches dans la console de gestion.

Sur cette page, vous pouvez afficher les tâches en fonction des options de filtrage suivantes :

- **Groupes de configuration** : dans le menu déroulant, sélectionnez le type de groupe de configuration.
- **Planifiée par** : dans le menu déroulant, sélectionnez un planificateur qui effectue l'activité de planification. Les options disponibles sont les suivantes :
  - Admin
    - Politique d'application
    - Politique d'image
    - Commandes du périphérique
  - Système
    - Publier la configuration de groupe
    - Autres
- **Type de système d'exploitation** : dans le menu déroulant, sélectionnez le système d'exploitation. Les options disponibles sont les suivantes :
  - ThinOS
  - WES
  - Linux
  - Thin Linux
  - Thin Client Wyse Software
  - Client hybride
  - Client générique
- **État** : dans le menu déroulant, sélectionnez l'état de la tâche. Les options disponibles sont les suivantes :
  - Planifié(s)
  - En cours d'exécution/En cours
  - Terminé
  - Annulé
  - Échec
- **État détaillé** : dans le menu déroulant, sélectionnez l'état en détail. Les options disponibles sont les suivantes :
  - 1 ou plusieurs échouée(s)
  - 1 ou plusieurs en attente
  - 1 ou plusieurs en cours
  - 1 ou plusieurs annulée(s)
  - 1 ou plusieurs terminée(s)
- **Autres actions** : dans le menu déroulant, sélectionnez l'option **Synchroniser le mot de passe admin BIOS**. La fenêtre Synchroniser la tâche du mot de passe admin BIOS s'affiche.

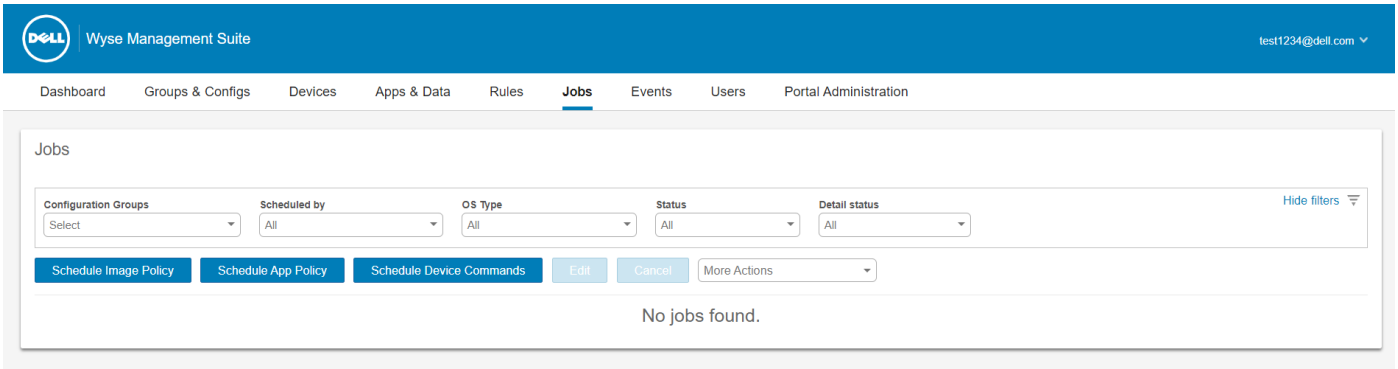


Figure 12. Page Tâches

Sujets :

Synchroniser le mot de passe admin BIOS

Étapes

1. Cliquez sur **Tâches**.
   La page **Tâches** s'affiche.
2. Dans le menu déroulant **Plus d'actions**, sélectionnez l'option **Synchroniser le mot de passe admin BIOS**.
   La fenêtre **Synchroniser la tâche du mot de passe admin BIOS** s'affiche.
3. Entrez le mot de passe. Le mot de passe doit comporter entre 4 et 32 caractères.
4. Cochez la case **Afficher le mot de passe** pour afficher le mot de passe.
5. Dans le menu déroulant **Type de système d'exploitation**, sélectionnez l'option souhaitée.
6. Dans le menu déroulant **Plate-forme**, sélectionnez l'option souhaitée.
7. Saisissez le nom de la tâche.
8. Dans le menu déroulant **Groupe**, sélectionnez l'option souhaitée.
9. Cochez la case **Inclure tous les sous-groupes** pour inclure les sous-groupes.
10. Saisissez la description dans la zone **Description**.
11. Cliquez sur **Aperçu**.

Rechercher une tâche planifiée en utilisant des filtres

Cette section décrit la procédure à suivre pour rechercher une tâche planifiée et gérer les tâches dans la console de gestion.

Étapes

1. Cliquez sur **Tâches**.
   La page **Tâches** s'affiche.
2. Dans le menu déroulant **Groupes de configuration**, sélectionnez soit le groupe de politiques par défaut, soit les groupes ajoutés par un administrateur.
3. Dans le menu déroulant **Planifiée par**, sélectionnez un planificateur qui effectue l'activité de planification.
   Les options disponibles sont les suivantes :
   - Admin
     - Politique d'application

- Politique d'image
- Commandes du périphérique

- Système
  - Publier la configuration de groupe
  - Autres

4. Dans le menu déroulant **Type de système d'exploitation**, sélectionnez le système d'exploitation.
   Les options disponibles sont les suivantes :
   - ThinOS
   - WES
   - Linux
   - Thin Linux
   - Thin Client Wyse Software
   - Teradici (Cloud privé)
   - Dell Hybrid Client
5. Dans le menu déroulant **État**, sélectionnez l'état de la tâche.
   Les options disponibles sont les suivantes :
   - Planifié(s)
   - En cours d'exécution/En cours
   - Terminé
   - Annulé
   - Échec
6. Dans le menu déroulant **État détaillé**, sélectionnez l'état en détail.
   Les options disponibles sont les suivantes :
   - 1 ou plusieurs échouée(s)
   - 1 ou plusieurs en attente
   - 1 ou plusieurs en cours
   - 1 ou plusieurs annulée(s)
   - 1 ou plusieurs terminée(s)
7. Dans le menu déroulant **Plus d'actions**, sélectionnez l'option **Synchroniser le mot de passe admin BIOS**.
   La fenêtre **Synchroniser la tâche du mot de passe admin BIOS** s'affiche. Pour plus d'informations, voir Synchroniser le mot de passe admin BIOS.

Planifier une tâche de commande d'appareil

Étapes

1. Sur la page **Tâches**, cliquez sur l'option **Planifier la commande de l'appareil**.
   L'écran **Tâche de commande d'appareil** s'affiche.
2. Configurez les options ci-dessous :
   a. Sélectionnez une commande dans la liste déroulante **Commande**. Les options disponibles sont les suivantes :
      - Redémarrer
      - Éveil par appel réseau
      - Arrêt
      - Requête
      - Relmage
      - Verrouillage : applicable aux appareils ThinOS 8.x et ThinOS 9.x
      - Envoyer un message : applicable aux appareils équipés de Windows Embedded, ThinLinux, ThinOS 8.x, ThinOS 9.x et Dell Hybrid Client.
      - Réinitialisation des paramètres d'usine : applicable aux appareils équipés de ThinOS 8.x, ThinOS 9.x et Dell Hybrid Client.

      La commande d'appareil est une tâche récurrente. Certains jours de la semaine et à un moment spécifique, les commandes sont envoyées à une sélection d'appareils.
   b. Dans la liste déroulante **Type de système d'exploitation**, sélectionnez le type de système d'exploitation.
   c. Dans le champ **Nom**, saisissez le nom de la tâche.

d. Dans la liste déroulante **Groupe**, sélectionnez un nom de groupe.
e. Saisissez la description de la tâche.
f. Dans la liste déroulante **Exécution**, sélectionnez la date et l'heure.
g. Saisissez ou sélectionnez les informations suivantes :
   - **Effectif** : saisissez l'heure de début et de fin.
   - **Commence entre** : saisissez l'heure de début et de fin.
   - **Le(s) jour(s)** : sélectionnez les jours de la semaine.

3. Cliquez sur l'option **Aperçu** pour afficher les détails de la tâche planifiée.
4. Sur la page suivante, cliquez sur l'option **Planifier** pour lancer la tâche.

Planifier la politique d'image

La politique d'image n'est pas une tâche récurrente. Chaque commande est spécifique à un appareil.

Étapes

1. Sur la page **Tâches**, cliquez sur l'option **Planifier la politique d'image**.
   L'écran **Tâche de mise à jour d'image** s'affiche.
2. Sélectionnez une politique dans la liste déroulante.
3. Saisissez la description de la tâche.
4. Dans la liste déroulante, sélectionnez la date et l'heure.
5. Saisissez/sélectionnez les informations suivantes :
   - **Effectif** : saisissez l'heure de début et de fin.
   - **Commence entre** : saisissez l'heure de début et de fin.
   - **Le(s) jour(s)** : sélectionnez les jours de la semaine.
6. Cliquez sur l'option **Aperçu** pour afficher les détails de la tâche planifiée.
7. Cliquez sur l'option **Planifier** pour lancer la tâche.

Planifier une politique d'application

La politique d'application n'est pas une tâche récurrente. Chaque commande est spécifique à un appareil.

Étapes

1. Sur la page **Tâches**, cliquez sur l'option **Planifier la politique d'application**.
   L'écran **Tâche de politique d'application** s'affiche.
2. Sélectionnez une politique dans la liste déroulante.
3. Saisissez la description de la tâche.
4. Dans la liste déroulante, sélectionnez la date et l'heure.
5. Saisissez/sélectionnez les informations suivantes :
   - **Effectif** : saisissez l'heure de début et de fin.
   - **Commence entre** : saisissez l'heure de début et de fin.
   - **Le(s) jour(s)** : sélectionnez les jours de la semaine.
6. Cliquez sur l'option **Aperçu** pour afficher les détails de la tâche planifiée.
7. Sur la page suivante, cliquez sur l'option **Planifier** pour lancer la tâche.

Redémarrer une tâché ayant échoué

Vous pouvez redémarrer une tâche liée aux commandes de l'appareil, à la politique d'application et à la politique d'image ayant échoué à partir de Wyse Management Suite 3.2. Vous pouvez également créer une planification pour une tâche ayant échoué. Cette option s'applique uniquement à la licence Pro de Wyse Management Suite.

Prérequis

- La tâche doit être planifiée et doit avoir échoué.
- La tâche planifiée doit être liée à une commande de l'appareil, une politique d'application ou une politique d'image.

Étapes

1. Cliquez sur l'onglet **Tâches**.
2. Sélectionnez la tâche qui a échoué et cliquez sur **Redémarrer la tâche ayant échoué**.
   L'état de la tâche est modifiée et devient **Redémarrée**.
3. Dans la liste déroulante **Exécuter**, planifiez la tâche.
4. Cliquez sur l'option **Aperçu** pour afficher les détails de la tâche planifiée.
5. Sur la page suivante, cliquez sur l'option **Planifier** pour lancer la tâche.

REMARQUE : L'administrateur global, l'utilisateur avec un rôle personnalisé (si des autorisations de travail sont attribuées) ou un administrateur de groupe pour un groupe spécifique peut redémarrer une tâche ayant échoué.

REMARQUE : Vous ne pouvez redémarrer une tâche qui a échoué qu'une seule fois, car une nouvelle tâche enfant est créée pour celle qui a échoué.

12

Gestion des événements

Sur la page **Événements**, vous pouvez afficher tous les événements et toutes les alertes du système de gestion à l'aide de la console de gestion. Il fournit également des instructions sur l'affichage d'un audit des événements et alertes pour un audit du système.

Un récapitulatif des événements et alertes est utilisé pour obtenir un résumé quotidien simple à lire de ce qui s'est produit dans le système. La fenêtre **Audit** organise les informations dans une vue de journal d'audit type. Vous pouvez afficher l'horodatage, le type d'événement, la source et la description de chaque événement dans l'ordre chronologique.

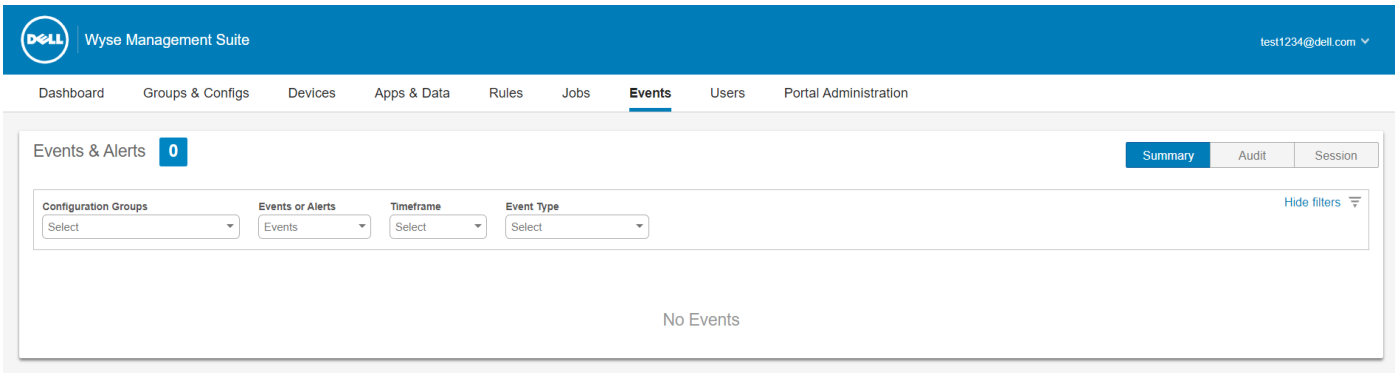


Figure 13. Page Événements

Sujets :

Rechercher un événement ou une alerte en utilisant des filtres

Étapes

1. Cliquez sur **Événements**.
   La page **Événements** s'affiche.
2. Dans le menu déroulant **Groupes de configuration**, sélectionnez soit le groupe de politiques par défaut, soit les groupes ajoutés par un administrateur.
3. Dans le menu déroulant **Événements ou alertes**, sélectionnez l'une des options suivantes :
   - Événements
   - Alertes actuelles
   - Historique des alertes
4. Dans le menu déroulant **Plage de temps**, sélectionnez l'un des systèmes d'exploitation suivants :
   Cette option vous permet d'afficher les événements qui se sont produits au cours d'une période particulière. Les options disponibles dans le menu déroulant sont les suivantes :
   - Aujourd'hui
   - Hier
   - Cette semaine
   - Personnaliser
5. Dans le menu déroulant **Type d'événement**, sélectionnez le type d'événement.

Tous les événements sont classés dans des groupes particuliers. Les options disponibles dans le menu déroulant sont les suivantes :

- Accès
- Enregistrement
- Configuration
- Commandes à distance
- Gestion
- Conformité

Afficher le résumé des événements

La fenêtre **Événements et alertes** affiche tous les événements et toutes les alertes qui ont eu lieu dans le système. Accédez à **Événements** > **Récapitulatif**.

Afficher le journal d'audit

La fenêtre **Audit** organise les informations dans une vue de journal d'audit type. Vous pouvez afficher l'horodatage, le type d'événement, la source et la description de chaque événement dans l'ordre chronologique.

Étapes

1. Accédez à **Événements** > **Audit**.
2. Dans la liste déroulante **Groupes de configuration**, sélectionnez un groupe pour lequel vous souhaitez afficher le journal d'audit.
3. Dans la liste déroulante **Plage de temps**, sélectionnez la plage de temps pour afficher les événements qui se sont produits au cours de cette période.

   REMARQUE : Les fichiers d'audit ne sont pas traduits et ne sont disponibles qu'en anglais.

Création de rapports de session d'utilisateur final

Vous pouvez utiliser l'option de création de rapports de session d'utilisateur final pour rapporter la session d'utilisateur pendant différents intervalles de temps.

Prérequis

L'option **Activer la création de rapports de session** doit être activée. Pour plus d'informations, consultez la section Configurer les paramètres du client Wyse Management Suite pour Dell Hybrid Client.

Étapes

1. Cliquez sur **Événements**.
   La page **Événements** s'affiche.
2. Cliquez sur **Session**.
   La page **Session d'utilisateurs finaux** s'affiche.
3. Dans le menu déroulant **Plage de temps**, sélectionnez une option pour afficher les événements. Les options disponibles dans le menu déroulant sont les suivantes :
   - Aujourd'hui
   - Hier
   - Cette semaine
   - Personnalisé

13

Gestion des utilisateurs

Cette section décrit comment exécuter une tâche de routine de gestion des utilisateurs dans la console de gestion. Les trois types d'utilisateurs suivants sont disponibles :

- **Administrateurs** : l'administrateur Wyse Management Suite peut se voir attribuer le rôle d'administrateur global, d'administrateur de groupe ou de lecteur.
  - Un administrateur global a accès à toutes les fonctions Wyse Management Suite.
  - Un administrateur de groupe a accès à tous les actifs et fonctions pour les groupes qui leur sont attribués.
  - Un lecteur dispose d'un accès en lecture seule pour toutes les données et peut se voir attribuer des droits pour déclencher des commandes spécifiques en temps réel, telles que l'arrêt et le redémarrage.

  Si vous sélectionnez administrateur, vous pouvez effectuer les actions suivantes :
  - Ajouter un administrateur
  - Modifier un administrateur
  - Activer un ou des administrateurs
  - Désactiver un ou des administrateurs
  - Supprimer un ou des administrateurs
  - Déverrouiller un ou des administrateurs

- **Administrateurs non affectés** : les utilisateurs importés depuis le serveur AD s'affichent sur la page **Administrateurs non affectés**. Vous pourrez attribuer un rôle à ces utilisateurs ultérieurement à partir du portail.

  Pour une gestion des utilisateurs plus efficace et plus rapide, sélectionnez les utilisateurs en fonction des options de filtre disponibles. Si vous sélectionnez **Utilisateurs non gérés**, vous pouvez effectuer les actions suivantes :
  - Ajouter un utilisateur
  - Modifier l'utilisateur
  - Activer un ou plusieurs utilisateurs
  - Désactiver un ou plusieurs utilisateurs
  - Supprimer un ou plusieurs utilisateurs

- **Utilisateurs finaux** : vous pouvez ajouter des utilisateurs individuels à Wyse Management Suite en utilisant l'onglet **Utilisateurs finaux**. Vous pouvez configurer et déployer les paramètres pour un utilisateur individuel. Les paramètres sont appliqués au compte d'utilisateur et sont appliqués au Thin Client lorsque l'utilisateur se connecte. Cette option s'applique uniquement aux clients légers utilisant le système d'exploitation ThinOS 9.x et Dell Hybrid Clients.

REMARQUE : Vous pouvez importer en bloc des utilisateurs uniquement à partir du fichier .CSV. Vous ne pouvez pas importer en bloc des utilisateurs finaux à partir d'un Active Directory.

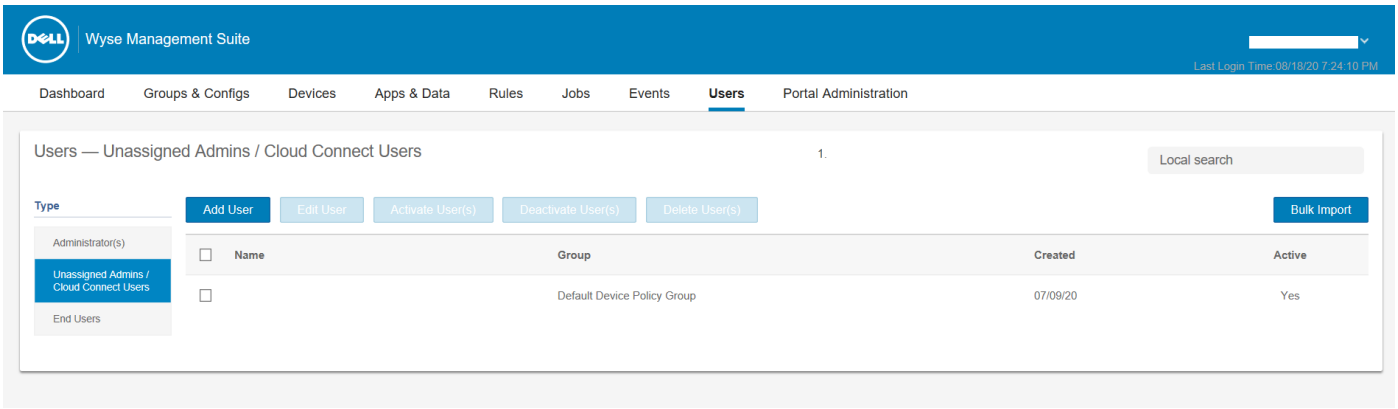


Figure 14. Page Utilisateurs

Sujets :

- Ajouter un nouveau profil d'administrateur

- Création d'un rôle WMS personnalisé dans Wyse Management Suite
- Attribuer des rôles personnalisés WMS aux groupes AD importés
- Importation en bloc des administrateurs non affectés ou des utilisateurs de Cloud Connect
- Modifier un profil d'administrateur
- Activer un profil d'administrateur
- Désactiver un profil d'administrateur
- Supprimer un profil d'administrateur
- Déverrouiller un profil d'administrateur
- Désactiver un profil d'administrateur
- Créer des règles d'attribution automatique pour les appareils non gérés
- Ajouter un utilisateur final
- Modifier un utilisateur final
- Configurer la politique d'utilisateur final
- Importation en bloc des utilisateurs finaux
- Suppression d'un utilisateur final
- Modifier un profil de l'utilisateur

Ajouter un nouveau profil d'administrateur

Étapes

1. Cliquez sur **Utilisateurs**.
2. Cliquez sur **Administrateur(s)**.
3. Cliquez sur **Ajouter un administrateur**.
   La fenêtre **Nouvel utilisateur administrateur** s'affiche.
4. Saisissez votre ID d'e-mail et le nom d'utilisateur dans les champs respectifs.
5. Cochez la case pour utiliser le même nom d'utilisateur que celui de l'e-mail.
6. Effectuez l'une des opérations suivantes :
   - Si vous cliquez sur l'onglet **Informations personnelles**, saisissez les détails suivants :
     - Prénom
     - Nom
     - Titre
     - Numéro de téléphone portable
   - Si vous cliquez sur l'onglet **Rôles**, saisissez les détails suivants :
     a. Dans la section **Rôles**, dans la liste déroulante **Rôle**, sélectionnez le **rôle d'administrateur**.
        - Administrateur général
        - Administrateur de groupe
        - Observateur

        REMARQUE : Si vous sélectionnez le **rôle d'administrateur Observateur**, les tâches administratives suivantes s'affichent :
        - Interroger le périphérique
        - Annuler l'enregistrement du périphérique
        - Redémarrer/arrêter le périphérique
        - Modifier l'attribution de groupe
        - Observation
        - Verrouiller le périphérique
        - Effacer le périphérique
        - Envoyer un message
        - Périphérique WOL

     b. Dans la section **Mot de passe**, saisissez le mot de passe personnalisé. Pour générer un mot de passe aléatoire, sélectionnez le bouton radio **Générer un mot de passe aléatoire**.
7. Cliquez sur **Enregistrer**.

Création d'un rôle WMS personnalisé dans Wyse Management Suite

À l'aide de Wyse Management Suite 3.1 ou versions ultérieures, un administrateur global peut créer un nouveau rôle d'administrateur et fournir des autorisations granulaires pour différentes fonctionnalités de Wyse Management Suite. Vous pouvez créer plusieurs utilisateurs à l'aide du rôle d'administrateur général personnalisé.

Étapes

1. Accédez à l'onglet **Utilisateurs**.
2. Cliquez sur **Administrateur(s)**.
3. Cliquez sur **Ajouter un administrateur**.
   La fenêtre **Nouvel utilisateur administrateur** s'affiche.
4. Saisissez l'ID d'e-mail et le nom d'utilisateur dans les champs respectifs.
5. Cliquez sur **Rôles**.
6. Dans la liste déroulante **Rôle**, sélectionnez **Rôle WMS personnalisé**.
7. Sous chaque catégorie, sélectionnez la fonction appropriée que l'utilisateur est autorisé à exécuter.
8. Cliquez sur **Enregistrer**.
   Le tableau suivant fournit des informations sur les autorisations prises en charge et non prises en charge pouvant être attribuées à un rôle personnalisé :

Tableau 9. Autorisations pour un rôle personnalisé

Pris en charge	Non pris en charge
Modifier ou supprimer une configuration	Exception d'appareil en bloc
Ajouter, modifier et supprimer des groupes	Création d'un administrateur de groupe
Télécharger des fichiers de référence	Création d'un administrateur global
Créer une exception de détails d'appareil	Création d'un administrateur observateur
Règles	Attribution d'un rôle à des administrateurs non attribués
Applications et données	Abonnement (exportation et importation de licence)
Importation en bloc des utilisateurs finaux	Modification de l'URL du serveur WMS
Gérer les référentiels distants	Modification de l'URL MQTT
Rapports	Chargement de l'interface utilisateur de configuration
Autres	Marque personnalisée
Active Directory sur la page d'administration du portail	

Attribuer des rôles personnalisés WMS aux groupes AD importés

Vous pouvez attribuer des rôles aux groupes importés depuis Active Directory, à partir de Wyse Management Suite 3.2. La permission attribuée au groupe est appliquée à tous les utilisateurs du groupe.

Étapes

1. Connectez-vous en tant qu'administrateur global.
2. Allez dans **Administration du portail** > **Active Directory** > **Importation ponctuelle** et saisissez les informations d'identification.
   Tous les groupes du domaine sont répertoriés dans le volet de gauche.
3. Sélectionnez les groupes que vous souhaitez importer.
   Les groupes sélectionnés sont déplacés vers le volet de droite de la page.

4. Cochez la case **Attribuer des rôles**.
5. Cliquez sur **Importer des groupes**.
   Les groupes sont importés et des rôles par défaut leur sont attribués.
6. Allez dans l'onglet **Utilisateurs** et cliquez sur **Attribution de groupe**.

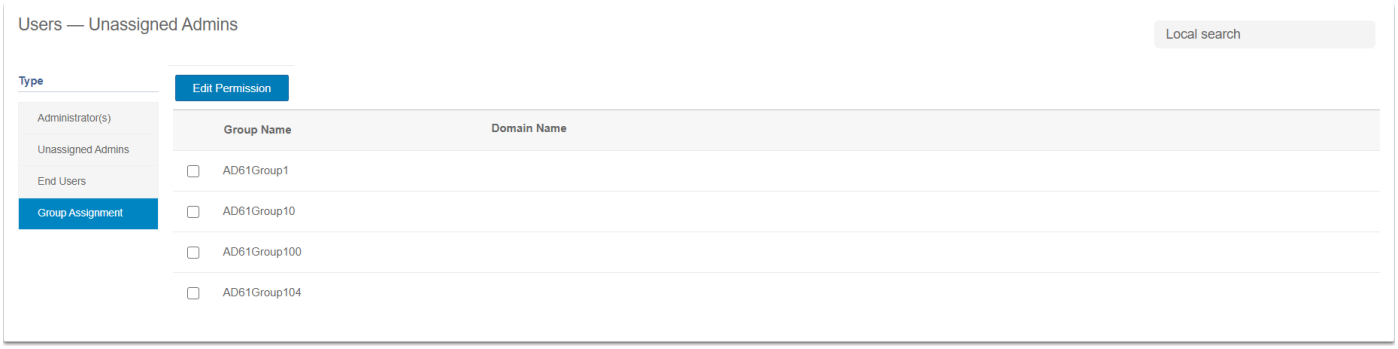


Figure 15. Attribution de groupe

Les groupes importés sont répertoriés dans l'onglet **Attribution de groupe**.

7. Sélectionnez le groupe auquel vous voulez attribuer des rôles et cliquez sur **Modifier les autorisations**.
   La fenêtre **Rôles** s'affiche.
8. Sélectionnez le rôle que vous souhaitez attribuer dans la liste déroulante et cliquez sur **Enregistrer**.

REMARQUE : Si des rôles sont déjà attribués à un utilisateur à l'aide de l'attribution de rôles à un groupe, accédez à **Utilisateurs** > **Administrateurs** et modifiez les autorisations des utilisateurs individuels ou des sous-groupes. Ces autorisations ont la priorité sur l'attribution de rôle de groupe.

REMARQUE : Pour le Cloud public, vous pouvez attribuer des rôles personnalisés à WMS en utilisant le référentiel de Wyse Management Suite version 3.2.

Importation en bloc des administrateurs non affectés ou des utilisateurs de Cloud Connect

Étapes

1. Cliquez sur **Utilisateurs**.
   La page **Utilisateurs** s'affiche.
2. Sélectionnez l'option **Administrateurs non affectés**.
3. Cliquez sur **Importation en bloc**.
   La fenêtre **Importer en bloc** s'affiche.
4. Cliquez sur **Parcourir** et sélectionnez le fichier CSV.
5. Sélectionnez le groupe d'utilisateurs auquel les utilisateurs importés doivent être attribués.
6. Cliquez sur **Importer**.

Modifier un profil d'administrateur

Étapes

1. Cliquez sur **Utilisateurs**.
2. Cliquez sur **Administrateur(s)**.
3. Cliquez sur **Modifier un administrateur**.
   La fenêtre **Modifier l'utilisateur administrateur** s'affiche.
4. Saisissez votre ID d'e-mail et le nom d'utilisateur dans les champs respectifs.

REMARQUE : lorsque vous mettez à jour le nom de connexion, vous êtes obligé de fermer la session à partir de la console. Connectez-vous à la console à l'aide de l'identifiant de compte mis à jour.

5. Effectuez l'une des opérations suivantes :
   - Si vous cliquez sur l'onglet **Informations personnelles**, saisissez les détails suivants :
     - Prénom
     - Nom
     - Titre
     - Numéro de téléphone portable
   - Si vous cliquez sur l'onglet **Rôles**, saisissez les détails suivants :
     a. Dans la section **Rôles**, dans la liste déroulante **Rôle**, sélectionnez le **rôle d'administrateur**.
     b. Dans la section **Mot de passe**, saisissez le mot de passe personnalisé. Pour générer un mot de passe aléatoire, sélectionnez le bouton radio **Générer un mot de passe aléatoire**.
6. Cliquez sur **Enregistrer**.

Activer un profil d'administrateur

Étapes

1. Cliquez sur **Utilisateurs**.
2. Cliquez sur **Administrateur(s)**.
3. Sélectionnez les administrateurs que vous souhaitez activer.
4. Cliquez sur **Activer un administrateur**.

Désactiver un profil d'administrateur

La désactivation du profil d'administrateur vous empêche de vous connecter à la console et supprime votre compte de la liste des appareils enregistrés.

Étapes

1. Cliquez sur **Utilisateurs**.
2. Cliquez sur **Administrateur(s)**.
3. Dans la liste, sélectionnez un utilisateur et cliquez sur **Désactiver un ou des administrateurs**.
   Une fenêtre d'alerte s'affiche.
4. Cliquez sur **OK**.

Supprimer un profil d'administrateur

À propos de cette tâche

Un administrateur doit d'abord être désactivé pour pouvoir être supprimé. Pour supprimer un profil d'administrateur, procédez comme suit :

Étapes

1. Cliquez sur **Utilisateurs**.
2. Cliquez sur **Administrateur(s)**.
3. Cochez la case en regard du ou des administrateurs à supprimer.
4. Cliquez sur **Supprimer un ou des administrateurs**.
   Une fenêtre **Alerte** s'affiche.
5. Indiquez la raison pour laquelle vous effectuez cette suppression pour activer le lien **Supprimer**.
6. Cliquez sur **Supprimer**.

Déverrouiller un profil d’administrateur

Étapes

1. Cliquez sur **Utilisateurs**.
2. Cliquez sur **Administrateur(s)**.
3. Sélectionnez les administrateurs que vous souhaitez déverrouiller.
4. Cliquez sur **Déverrouiller un ou des administrateurs**.

Désactiver un profil d’administrateur

Étapes

1. Cliquez sur **Utilisateurs**.
2. Cliquez sur **Administrateur(s)**.
3. Sélectionnez les administrateurs que vous souhaitez désactiver.
4. Cliquez sur **Désactiver un ou des administrateurs**.

Créer des règles d’attribution automatique pour les appareils non gérés

Étapes

1. Cliquez sur l'onglet **Règles**.
2. Sélectionnez l'option **Attribution automatique d'appareils non gérés**.
3. Cliquez sur l'onglet **Ajouter une règle**.
4. Saisissez le **nom** et sélectionnez le **groupe de destination**.
5. Cliquez sur l'option **Ajouter une condition** et sélectionnez les conditions pour les règles attribuées.
6. Cliquez sur **Enregistrer**.

   La règle est affichée dans la liste de groupes non gérés. Cette règle est appliquée automatiquement et l'appareil est répertorié dans le groupe de destination.

Ajouter un utilisateur final

Étapes

1. Cliquez sur l’onglet **Utilisateurs**.
2. Cliquez sur **Utilisateurs finaux**.
3. Cliquez sur **Ajouter un utilisateur**.
4. Saisissez le nom d’utilisateur, le domaine, le prénom, le nom, l’adresse e-mail, le titre et le numéro de téléphone
5. Cliquez sur **Enregistrer**.

Modifier un utilisateur final

Étapes

1. Cliquez sur l'onglet **Utilisateurs**.
2. Cliquez sur **Utilisateurs finaux**.
3. Cliquez sur **Modifier un utilisateur final**.
4. Saisissez votre ID d'e-mail et le nom d'utilisateur dans les champs respectifs.

5. Cliquez sur **Enregistrer**.

Configurer la politique d'utilisateur final

Vous pouvez configurer et déployer les paramètres pour un utilisateur individuel. Les paramètres sont appliqués au compte d'utilisateur et sont appliqués au Thin Client lorsque l'utilisateur se connecte. Cette option s'applique uniquement aux clients légers utilisant le système d'exploitation ThinOS 9.x et Dell Hybrid Clients.

Étapes

1. Cliquez sur l'onglet **Utilisateurs**.
2. Cliquez sur **Utilisateurs finaux**.
3. Sélectionnez un utilisateur.
   La page **Informations de l'utilisateur final** s'affiche.
4. Dans le menu déroulant **Modifier les politiques**, sélectionnez le système d'exploitation.
5. Configurez les politiques requises, puis cliquez sur **Enregistrer et publier**.

   REMARQUE : Le nombre d'utilisateurs dans un environnement sur site est illimité. Vous pouvez ajouter 10 000 utilisateurs dans un environnement Cloud public.

Importation en bloc des utilisateurs finaux

Étapes

1. Cliquez sur l'onglet **Utilisateurs**.
2. Cliquez sur **Utilisateurs finaux**.
3. Cliquez sur **Importation en bloc**.
4. Cliquez sur **Parcourir** et sélectionnez le fichier .csv.
5. Sélectionnez l'option **Le fichier CSV a une ligne d'en-tête** si le fichier .csv contient un en-tête.
6. Dans la liste déroulante **Choisir un groupe d'utilisateurs**, sélectionnez le groupe d'utilisateurs auquel vous voulez ajouter les utilisateurs.
7. Cliquez sur **Importer**.

   REMARQUE : Vous pouvez ajouter jusqu'à 100 utilisateurs par fichier à Wyse Management Suite et la taille du fichier .csv ne doit pas excéder 150 Ko.

   REMARQUE : Vous pouvez ajouter un maximum de 10 000 utilisateurs dans le Cloud public. Le nombre d'utilisateurs qui peuvent être ajoutés dans un Cloud privé est illimité.

Suppression d'un utilisateur final

Étapes

1. Cliquez sur l'onglet **Utilisateurs finaux**.
2. Cliquez sur **Supprimer l'utilisateur final**.
   Une fenêtre Alerte s'affiche. Indiquez la raison pour laquelle vous effectuez cette suppression pour activer le lien Supprimer.
3. Cliquez sur **Supprimer**.

Modifier un profil de l'utilisateur

Étapes

1. Cliquez sur **Utilisateurs**.

2. Cliquez sur **Administrateurs non affectés**.
3. Cliquez sur **Modifier un utilisateur**.
   La fenêtre **Modifier l'utilisateur administrateur** s'affiche.
4. Saisissez votre ID d'e-mail et le nom d'utilisateur dans les champs respectifs.

   REMARQUE : lorsque vous mettez à jour le nom de connexion, vous êtes obligé de fermer la session à partir de la console. Connectez-vous à la console à l'aide de l'identifiant de compte mis à jour.

5. Effectuez l'une des opérations suivantes :
   - Cliquez sur l'onglet **Informations personnelles**, et saisissez les détails suivants :
     - Prénom
     - Nom
     - Titre
     - Numéro de téléphone portable
   - Cliquez sur l'onglet **Rôles**, et saisissez les détails suivants :
     a. Dans la section **Rôles**, dans la liste déroulante **Rôle**, sélectionnez le **rôle d'administrateur**.
     b. Dans la section **Mot de passe**, saisissez le mot de passe personnalisé. Pour générer un mot de passe aléatoire, sélectionnez le bouton radio **Générer un mot de passe aléatoire**.
6. Cliquez sur **Enregistrer**.

14

Administration de portail

Cette section contient une brève présentation des tâches d'administration système que vous devez réaliser pour configurer et gérer votre système.

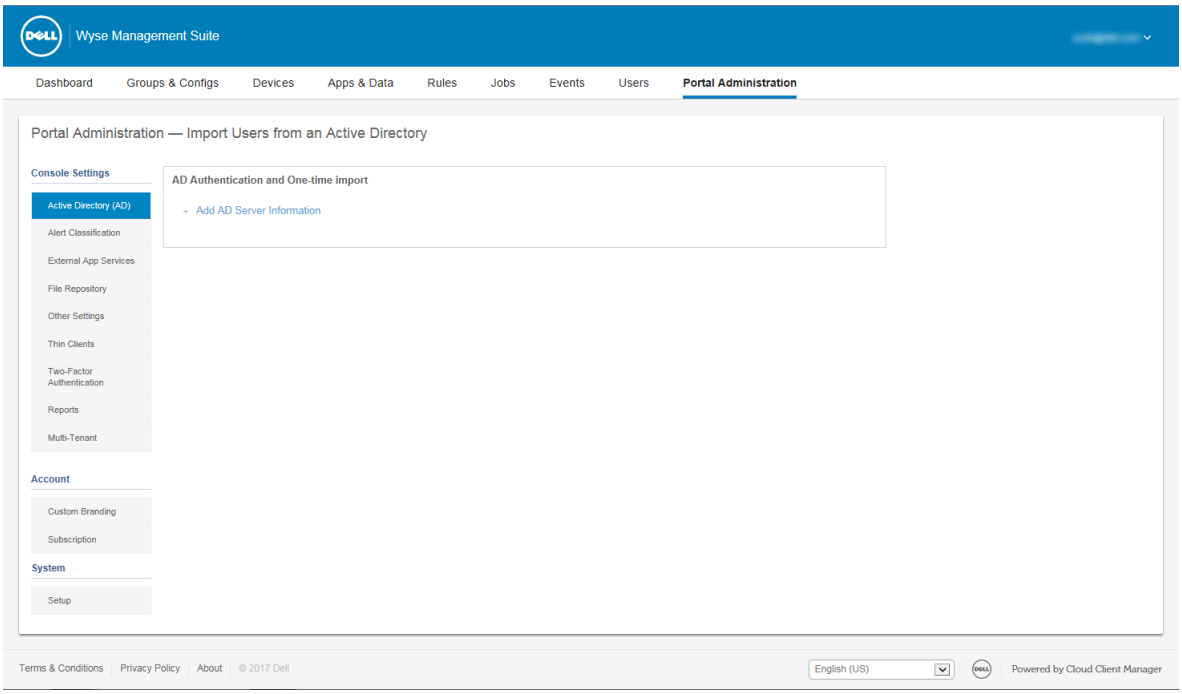


Figure 16. Administration du portail

Sujets :

- Importer des utilisateurs ou des groupes d'utilisateurs non affectés vers le Cloud public via Active Directory
- Ajout d'informations sur le serveur Active Directory
- Classifications d'alerte
- Créer des comptes d'API
- Accéder au référentiel de fichiers Wyse Management Suite
- Configuration des autres paramètres
- Gestion des configurations Teradici
- Activer l'authentification à deux facteurs
- Activation des comptes multi-locataires
- Générer des rapports
- Activation d'une marque personnalisée
- Gérer la configuration du système
- Configurer un MQTT sécurisé
- Activer Secure LDAP sur SSL

Importer des utilisateurs ou des groupes d'utilisateurs non affectés vers le Cloud public via Active Directory

Étapes

1. Téléchargez et installez le référentiel de fichiers. Reportez-vous à Accès au référentiel de fichiers. Le référentiel doit être installé à l'aide du réseau de la société et doit disposer d'un accès au serveur AD pour extraire les utilisateurs.
2. Enregistrez le référentiel dans le Cloud public. Une fois enregistré, suivez les étapes mentionnées dans l'interface utilisateur pour importer les utilisateurs vers le Cloud public Wyse Management Suite. Vous pouvez modifier les rôles de l'utilisateur AD après l'importation dans le Cloud public Wyse Management Suite.
3. Configurez ADFS sur le Cloud public.

Ajout d'informations sur le serveur Active Directory

Vous pouvez importer des utilisateurs Active Directory et des groupes d'utilisateurs vers le Cloud privé Wyse Management Suite.

Étapes

1. Connectez-vous au cloud privé Wyse Management Suite.
2. Accédez à **Administration de portail** > **Paramètres de console** > **Active Directory (AD)**.
3. Cliquez sur le lien **Ajouter des informations de serveur AD**.
4. Entrez les détails du serveur tels que **Nom du serveur AD**, **Nom du domaine**, **URL de serveur** et **Port**.
   Si vous vous connectez en utilisant le port LDAP 389, un message d'avertissement s'affiche pour activer le LDAP sécurisé. Pour configurer et activer le protocole LDAP sécurisé sur SSL, consultez Activer le protocole LDAP sécurisé sur SSL.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Importer**.
7. Saisissez le nom d'utilisateur et le mot de passe.

   REMARQUE : Pour rechercher des groupes et des utilisateurs, vous pouvez les filtrer en fonction des options **Base de recherche** et **Le nom de groupe contient**. Vous pouvez entrer les valeurs suivantes :

   - `OU=<OU Name>`.

     Par exemple, `OU=TestOU`.

   - `DC=<Child Domain>, DC=<Parent Domain>, DC=com,`.

     Par exemple, `DC=Skynet, DC=Alpha, DC=Com`.

   Vous pouvez entrer un espace après la virgule, mais vous ne pouvez pas utiliser de guillemets simples ou doubles.
8. Cliquez sur **Connexion**.
9. Sur la page **Groupe d'utilisateurs**, cliquez sur **Nom du groupe** et saisissez le nom du groupe.
10. Dans le champ **Rechercher**, saisissez le nom du groupe que vous souhaitez sélectionner.
11. Sélectionnez un groupe.
    Le groupe sélectionné est déplacé vers le volet de droite.
12. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur.
13. Cliquez sur **Importer des utilisateurs** ou **Importer des groupes**.

    Les entrées sont ignorées et ne peuvent pas être importées dans Wyse Management Suite pendant le processus d'importation des utilisateurs dans les scénarios suivants :
    - Si vous fournissez un nom invalide.
    - Si vous ne fournissez pas de nom de famille
    - Si vous fournissez une adresse email en tant que nom

    Un message de confirmation indiquant le nombre d'utilisateurs Active Directory importés s'affiche sur le portail. Les utilisateurs Active Directory importés sont répertoriés sous l'onglet **Utilisateurs Administrateurs non affectés**. Les messages de confirmation affichent également l'endroit où les groupes sont importés.
14. Pour attribuer des rôles ou des droits différents, sélectionnez un utilisateur et cliquez sur **Modifier l'utilisateur**.

Une fois les rôles affectés à l'utilisateur Active Directory, ils sont déplacés vers l'onglet **Administrateurs** de la page **Utilisateurs**.

REMARQUE : Pour fermer la page **Authentification AD et importation ponctuelle** pendant la configuration, cliquez sur l'option **Déconnexion AD**.

Étapes suivantes

Les utilisateurs Active Directory peuvent se connecter au portail de gestion Wyse Management Suite à l'aide des informations d'identification de domaine. Pour vous connecter au portail Wyse Management Suite, procédez comme suit :

1. Démarrez le portail de gestion Wyse Management Suite.
2. Sur l'écran d'ouverture de session, cliquez sur le lien **Connectez-vous avec les références de votre domaine**.
3. Saisissez les informations d'identification d'utilisateur de domaine, puis cliquez sur **Connexion**.

Pour vous connecter au portail Wyse Management Suite à l'aide des informations d'identification du domaine enfant, procédez comme suit :

1. Démarrez le portail de gestion Wyse Management Suite.
2. Sur l'écran d'ouverture de session, cliquez sur le lien **Connectez-vous avec les références de votre domaine**.
3. Cliquez sur **Changer de domaine utilisateur**.
4. Saisissez les informations d'identification de l'utilisateur et le nom de domaine complet.
5. Cliquez sur **Connexion**

Les utilisateurs Active Directory importés peuvent être activés ou désactivés depuis la page **Utilisateurs** en se connectant en tant qu'administrateur global. Si votre compte est désactivé, vous ne pouvez pas ouvrir de session sur le portail de gestion Wyse Management Suite.

REMARQUE : Pour importer les utilisateurs à l'aide du protocole LDAPS, procédez comme suit :

1. Importez manuellement le certificat racine du serveur de domaine AD dans le magasin de clés Java à l'aide de Keytool. Par exemple : `<C:\Program Files\DELL\WMS\jdk1.8.0_152\jre\bin>keytool.exe> -importcert -alias "WIN-O358EA52H8H" -keystore "<C:\Program Files\DELL\WMS\jdk1.8.0_152\jre\lib\security\cacerts>" -storepass changeit -file "Root Certificate Path"`
2. Redémarrez le service Tomcat.

Configuration de la fonctionnalité Active Directory Federation Services sur le cloud public

Vous pouvez configurer Active Directory Federation Services (ADFS) sur le Cloud public.

Étapes

1. Sur la page **Administration de portail**, sous **Paramètres de console**, cliquez sur **Active Directory (AD)**.
2. Saisissez les détails Wyse Management Suite pour ADFS. Pour connaître les détails de l'emplacement sur le serveur ADFS où vous devez charger les fichiers .xml Wyse Management Suite, pointez sur l'icône **information (i)** avec la souris.

   REMARQUE : Pour télécharger le fichier .xml Wyse Management Suite, cliquez sur le lien de téléchargement.

3. Définissez les règles Wyse Management Suite dans ADFS. Pour connaître les détails d'une règle de réclamation personnalisée, pointez sur l'icône **information (i)** avec la souris.

   REMARQUE : pour afficher les règles de gestion Wyse, cliquez sur le lien **Afficher les règles WMS**. Vous pouvez également télécharger les règles Wyse Management Suite en cliquant sur le lien fourni dans la fenêtre **Règles Wyse Management Suite**.

4. Pour configurer les détails ADFS, cliquez sur **Ajouter la configuration** et procédez comme suit :

   REMARQUE : pour autoriser les organisations à suivre la configuration ADFS, chargez le fichier de métadonnées ADFS.

   a. Pour télécharger le fichier .XML stocké sur votre client léger, cliquez sur **Charger le fichier XML**.

Le fichier est disponible à l'adresse `https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml`.

b. Saisissez les informations relatives à votre ID d'entité et au certificat de signature X.509 dans les champs correspondants.
c. Entrez l'adresse URL de connexion ADFS et l'adresse URL de déconnexion ADFS dans les champs correspondants.
d. Pour autoriser les organisations à configurer la connexion par authentification unique à l'aide d'ADFS, cochez la case **Activer la connexion unique avec ADFS**. Cette fonction est régie par la norme Security Assertion and Markup Language (SAML).
e. Pour valider les informations de configuration, cliquez sur **Tester la connexion ADFS**. Cela permet aux organisations de tester leur configuration avant d'enregistrer.

REMARQUE : les organisations peuvent activer/désactiver la connexion par authentification unique en utilisant ADFS.

5. Cliquez sur **Enregistrer**.
6. Une fois le fichier de métadonnées enregistré, cliquez sur **Mettre à jour la configuration**.

REMARQUE : Les clients peuvent se connecter et se déconnecter avec leurs informations d'identification AD configurées à partir de leurs ADFS. Vous devez vous assurer que les utilisateurs AD sont importés dans le serveur Wyse Management Suite. Sur la page de connexion, cliquez sur **Connexion** et saisissez vos informations d'identification de domaine. Vous devez fournir l'adresse e-mail de votre utilisateur AD et vous connecter. Pour importer un utilisateur vers le Cloud public, le référentiel distant doit être installé. Pour plus d'informations sur la documentation ADFS, rendez-vous sur Technet.microsoft.com.

Résultats

Une fois que le test de connexion à ADFS est réussi, importez les utilisateurs à l'aide du connecteur AD présent dans le référentiel distant.

Classifications d'alerte

La page des alertes classe les alertes en tant que **Critique**, **Avertissement** ou **Informations**.

REMARQUE : Pour recevoir des alertes par e-mail, sélectionnez l'option **Préférences d'alerte** dans le menu du nom d'utilisateur affiché dans le coin supérieur droit.

Sélectionnez le type de notification souhaité, par exemple, **Critique**, **Avertissement** ou **Informations** pour les alertes suivantes :

- Alerte de santé sur l'appareil
- Appareil non vérifié

Créer des comptes d'API

À propos de cette tâche

Cette section vous permet de créer des comptes d'API (Interface de programmation d'applications) sécurisés. Ce service permet de créer des comptes spéciaux. Pour configurer le service d'application externe, procédez comme suit :

Étapes

1. Connectez-vous au portail Wyse Management Suite, puis cliquez sur l'onglet **Administration de portail**.
2. Sélectionnez **Services d'application externes** sous **Paramètres de console**.
3. Sélectionnez l'onglet **Ajouter** pour ajouter un service d'API.
   La boîte de dialogue **Ajouter un service d'application externe** s'affiche.
4. Saisissez les détails suivants pour ajouter un service d'application externe.
   - Nom
   - Description
5. Cochez la case **Approuver automatiquement**.
   Si vous cochez cette case, l'approbation des administrateurs globaux n'est pas requise.
6. Cliquez sur **Enregistrer**.

Accéder au référentiel de fichiers Wyse Management Suite

Les **logithèques de fichiers** sont des endroits où les **fichiers** sont stockés et organisés. Wyse Management Suite comprend deux types de référentiels :

- **Référentiel local** : au cours de l'installation dans le cloud privé de Wyse Management Suite, fournissez le chemin du référentiel local au programme d'installation de Wyse Management Suite. Après l'installation, accédez à **Administration de portail** > **Logithèque de fichiers** et sélectionnez la logithèque locale. Cliquez sur l'option **Modifier** pour afficher et modifier les paramètres du référentiel.
- **Wyse Management Suite Repository** : connectez-vous au cloud public Wyse Management Suite, accédez à **Administration de portail** > **Référentiel de fichiers** et téléchargez le programme d'installation de Wyse Management Suite Repository. Après l'installation, enregistrez Wyse Management Suite Repository sur le serveur de gestion de Wyse Management Suite en fournissant les informations requises.

Vous pouvez activer l'option **Réplication automatique** pour répliquer les fichiers qui sont ajoutés à l'un des référentiels de fichiers vers d'autres référentiels. Lorsque vous activez cette option, un message d'alerte s'affiche. Vous pouvez cocher la case **Répliquer des fichiers existants** pour répliquer les fichiers existants vers vos référentiels de fichiers.

L'option **Répliquer un fichier existant** est applicable si le référentiel est déjà enregistré. Lorsqu'un nouveau référentiel est enregistré, alors tous les fichiers sont copiés vers le nouveau référentiel. Vous pouvez afficher l'état de réplication du fichier dans la page **Événements**.

Les modèles d'`extraction d'images` ne sont pas répliqués automatiquement vers d'autres référentiels. Vous devez copier ces fichiers manuellement.

La fonctionnalité de réplication de fichiers est prise en charge uniquement sur les référentiels de Wyse Management Suite 2.0 et versions supérieures.

Vous ne pouvez pas importer un certificat auto-signé du référentiel distant vers le serveur Wyse Management Suite. Si la validation par l'autorité de certification est activée pour le référentiel distant, alors la réplication de fichiers depuis le référentiel distant vers le référentiel local échoue.

Pour utiliser Wyse Management Suite Repository, procédez comme suit :

1. Téléchargez Wyse Management Suite Repository à partir de la console de cloud public.
2. Après le processus d'installation, démarrez l'application.
3. Sur la page Wyse Management Suite Repository, saisissez les informations d'identification pour enregistrer Wyse Management Suite Repository sur le serveur de Wyse Management Suite.
4. Si vous activez l'option **Enregistrer sur le portail de gestion public WMS**, vous pouvez enregistrer le référentiel dans le cloud public de Wyse Management Suite.
5. Cliquez sur l'option **Synchroniser les fichiers** pour envoyer la commande de synchronisation des fichiers.
6. Cliquez sur **Vérification**, puis sur **Envoyer la commande** pour envoyer la commande d'informations sur l'appareil à l'appareil.
7. Cliquez sur l'option **Annuler l'enregistrement** pour désenregistrer le service sur site.
8. Cliquez sur **Modifier** pour apporter des modifications aux fichiers.
9. Dans la liste déroulante **Téléchargements de fichiers simultanés**, sélectionnez le nombre de fichiers.
10. Activez ou désactivez l'option **Wake on LAN**.
11. Activez ou désactivez l'option **Téléchargement de fichier rapide (HTTP)**.
    - Lorsque HTTP est activé, ce protocole est utilisé pour le chargement et le téléchargement de fichiers.
    - Lorsque HTTP n'est pas activé, le protocole HTTPS est utilisé pour le chargement et le téléchargement de fichiers.
12. Sélectionnez la case à cocher **Validation de certificat** pour activer la validation de l'autorité de certification pour les Clouds publics.

    REMARQUE : Si la validation de l'autorité de certification à partir du serveur Wyse Management Suite est activée, le certificat doit être présent sur le client. Toutes les opérations effectuées sur des applications et des données, ainsi que toutes les actions Push/Pull sur des images aboutiront. Si le certificat n'est pas présent sur le client, le serveur Wyse Management Suite génère le message d'événement d'audit générique **Échec de la validation de l'autorité de certification** sur la page **Événements**. Toutes les opérations effectuées sur des applications et des données, ainsi que toutes les actions Push/Pull sur des images n'aboutiront pas. De même, lorsque la validation CA à partir du serveur Wyse Management Suite est désactivée, les communications à partir du serveur et du client se font par le biais d'un canal sécurisé sans validation de la signature du certificat.
13. Ajoutez une note dans la zone prévue à cet effet.
14. Cliquez sur **Enregistrer les paramètres**.

Mappage de sous-réseau

À compter de Wyse Management Suite 2.0, vous pouvez attribuer un sous-réseau à un référentiel de fichiers. Vous pouvez associer à un référentiel de fichiers jusqu'à 25 sous-réseaux ou plages. Vous pouvez également définir la priorité des sous-réseaux qui sont associés au référentiel.

Vous pouvez déployer les packages du BIOS à l'aide du mappage de sous-réseau à partir de Wyse Management Suite 2.1. Vous pouvez télécharger et déployer plusieurs packages de firmware à partir du référentiel distant, du référentiel Cloud du locataire ou du référentiel Cloud de l'opérateur. Cette fonctionnalité s'applique uniquement à la licence Pro de Wyse Management Suite.

REMARQUE : La proximité des sous-réseaux n'est pas prise en charge pour les appareils ThinOS 9.x.

Configurer le mappage de sous-réseau

Étapes

1. Accédez à **Administration de portail** > **Référentiel de fichiers**.

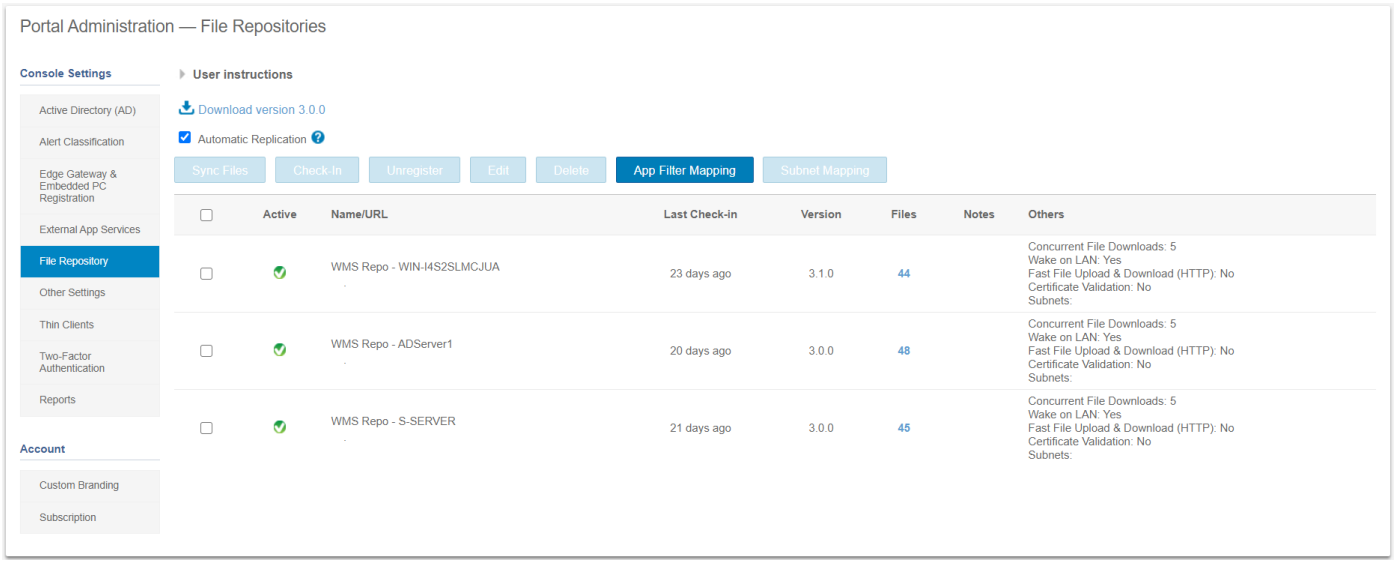


Figure 17. Référentiel de fichiers

2. Sélectionnez un référentiel de fichiers.
3. Cliquez sur l'option **Mappage de sous-réseau**.
4. Saisissez des sous-réseaux ou des plages, une valeur par ligne. Vous devez utiliser un trait d'union pour séparer les plages.
5. Si vous le souhaitez, décochez la case **Autoriser les appareils des sous-réseaux non mappés à ce référentiel de fichiers à télécharger les fichiers à partir de ce référentiel comme méthode de secours à l'aide de la proximité des sous-réseaux** si vous souhaitez que le référentiel de fichiers soit accessible uniquement via les sous-réseaux ou plages configuré(e)s.

   REMARQUE : L'option **Autoriser les appareils des sous-réseaux non mappés à ce référentiel de fichiers à télécharger les fichiers à partir de ce référentiel comme méthode de secours à l'aide de la proximité des sous-réseaux** est sélectionnée par défaut. Cette fonctionnalité n'est pas prise en charge sur les appareils ThinOS 9.x.

Configuration des autres paramètres

Vous pouvez utiliser les paramètres suivants pour faire appliquer les **avertissements APNS**, les **avertissements d'expiration de licence** et d'autres **accords juridiques de libre-service**.

- **Ignorer l'avertissement d'expiration de licence sur la page Tableau de bord** : cochez cette case pour désactiver l'avertissement d'expiration d'une licence de l'affichage sur la page **Tableau de bord**.

- **Activer les options avancées Dell Wyse Cloud Connect sur la page de configuration de la politique Paramètres Android (remarque : niveau professionnel uniquement)** : sélectionnez cette option pour activer les options avancées Dell Wyse Cloud Connect de la page de configuration de la politique des paramètres Android.
- **Intervalle de pulsation** : saisissez l'intervalle. L'appareil envoie un signal de pulsation toutes les 60 à 360 minutes. L'intervalle minimum est de 5 minutes pour le Cloud privé.
- **Intervalle de vérification** : saisissez l'intervalle. L'appareil envoie un signal de vérification complète toutes les 8 à 24 heures.
- **Alerte de conformité Non vérifiée** : saisissez le nombre de jours avant qu'un appareil déclenche une **alerte de conformité Non vérifiée**. La plage s'étend de 1 à 99.
- **Délai d'expiration de la console WMS** : saisissez le délai d'inactivité en minutes après lequel l'utilisateur est déconnecté de la console. Ce paramètre peut être configuré par n'importe quel administrateur global. La valeur par défaut est 30 minutes.
- **Validation de l'inscription** : lorsque l'option **Validation de l'inscription** est activée, les appareils automatiquement détectés présentent l'état **Validation en attente** sur la page **Appareils**. Le client peut sélectionner un ou plusieurs périphériques sur la page **Périphériques** et valider l'inscription. Une fois validés, les périphériques sont déplacés vers le groupe prévu.
- **Réinitialiser l'acceptation du CLUF** : cochez cette case si vous souhaitez réinitialiser la page **Acceptation du CLUF** pour afficher à nouveau l'Assistant pendant le téléchargement du firmware/des packages intégrés au CLUF pour ThinOS 9.x.
- **API WMS** : cochez cette case pour activer l'API de Wyse Management Suite.

Activer l'API Wyse Management Suite

Le serveur de Wyse Management Suite utilise une API propriétaire pour servir les requêtes générées par les composants de l'interface utilisateur. L'interface utilisateur est créée à l'aide de scripts Java qui utilisent un appel API de type Rest pour obtenir les données requises au format JSON. Le format JSON est spécifique à la demande. Vous pouvez récupérer les détails de l'appareil ou effectuer des actions à partir du serveur de Wyse Management Suite et intégrer le serveur avec votre client personnalisé tel que Service Now.

Prérequis

Une licence Pro est nécessaire pour utiliser les API de Wyse Management Suite.

Étapes

1. Connectez-vous en tant qu'administrateur.
2. Accédez à **Administration du portail** > **Autres paramètres**.
3. Cochez la case **Activer l'API WMS**.
4. Cliquez sur **Enregistrer les paramètres**.

   Pour obtenir des informations sur les API prises en charge et la documentation correspondante, consultez les API de Wyse Management Suite sur https://api-marketplace.dell.com.

Gestion des configurations Teradici

Pour ajouter un nouveau serveur Teradici, procédez comme suit :

Étapes

1. Dans l'onglet **Administration de portail**, sous **Paramètres de la console**, cliquez sur **Teradici**.
2. Cliquez sur **Ajouter un serveur**.
   L'écran **Ajouter un serveur** s'affiche.
3. Saisissez le **Nom du serveur**. Le numéro de port est automatiquement renseigné.
4. Cochez la case **Validation CA** pour activer la validation CA.
5. Cliquez sur **Test**.

Activer l'authentification à deux facteurs

Vous devez disposer d'au moins deux utilisateurs administrateurs globaux actifs dans le système.

Prérequis

Créez au moins deux administrateurs globaux avant d'effectuer cette tâche.

À propos de cette tâche

1. Ouvrez une session sur le portail Wyse Management Suite, puis cliquez sur l'onglet d'administration du portail.
2. Cliquez sur **Authentification bifactorielle** sous **Paramètres de console**.
3. Vous devez cocher la case pour activer l'authentification bifactorielle.
   REMARQUE : Les administrateurs doivent vérifier le deuxième facteur d'authentification à l'aide d'un code secret à usage unique pour se connecter au portail de gestion.
4. Vous recevrez un code secret à usage unique à votre adresse e-mail. Saisissez le code secret ponctuel.

Par défaut, vous avez droit à huit essais. Si vous échouez, le compte est verrouillé. Seuls les administrateurs globaux sont autorisés à déverrouiller les comptes.

Activation des comptes multi-locataires

Cette section vous permet de créer des comptes de client qui peuvent être gérés indépendamment l'un de l'autre. Vous pouvez gérer les organisations indépendamment. Chaque compte doit posséder sa propre clé de licence et peut configurer son propre ensemble de comptes administrateur, politiques, images de système d'exploitation, applications, règles, les alertes, etc. L'opérateur de niveau élevé crée ces organisations.

Pour activer les comptes multi-locataires, procédez comme suit :

1. Ouvrez une session sur le portail Wyse Management Suite, puis cliquez sur l'onglet d'administration du portail.
2. Sélectionnez **Multi-locataires** sous **Paramètres de console**.
3. Cochez la case pour activer l'option d'organisations multiples.
4. Saisissez les informations suivantes :
   - Nom d'utilisateur
   - Mot de passe
   - Confirmer le mot de passe
   - Messagerie électronique
5. Cliquez sur **Enregistrer les paramètres**.

Générer des rapports

Vous pouvez télécharger des rapports sur les tâches, les appareils, les groupes, les événements, les alertes et les politiques. Les rapports peuvent être partagés avec l'administrateur si vous souhaitez dépanner les points de terminaison.

Étapes

1. Sélectionnez **Administration de portail** > **Rapports**.
2. Cliquez sur l'option **Générer un rapport**.
   La fenêtre **Générer un rapport** s'affiche.
3. Dans la liste déroulante **Type**, sélectionnez le type de rapport.
4. Dans la liste déroulante **Groupes**, sélectionnez un groupe.
5. Sélectionnez le délimiteur.
6. Cliquez sur **Enregistrer**.

Activation d'une marque personnalisée

À propos de cette tâche

Cette option vous permet d'ajouter le nom de votre société et son logo ou sa marque. Vous pouvez charger votre propre logo d'en-tête, favicon, ajouter un titre en en-tête et modifier les couleurs de l'en-tête pour personnaliser le portail Wyse Management Suite. Pour accéder à et spécifier une marque personnalisée :

Étapes

1. Accédez à **Administration de portail** > **Compte** > **Marque personnalisée**.

2. Cliquez sur **Activer la marque personnalisée**.
3. Dans **Logo d'en-tête**, cliquez sur **Navigateur**, puis sélectionnez l'image du logo d'en-tête à partir de l'emplacement du dossier.
   La taille maximale du logo d'en-tête doit être de 500*50 pixels.
4. Saisissez le titre sous l'option **Titre**.
5. Cochez la case **Afficher le titre dans la fenêtre de navigateur/l'onglet** pour afficher le titre dans le navigateur.
6. Saisissez les codes de couleur pour **Couleur d'arrière-plan de l'en-tête** et **Couleur du texte de l'en-tête**.
7. Cliquez sur **Parcourir**, puis sélectionnez le **Favicon**.
   Le favicon s'affiche dans la barre d'adresse du navigateur en regard de l'URL du site web.
   REMARQUE : Vous devez enregistrer les images en tant que fichiers **.ico** uniquement.
8. Cliquez sur **Enregistrer les paramètres**.

Gérer la configuration du système

Vous pouvez modifier les détails SMTP, les certificats, les détails MQTT et les détails de l'URL Wyse Management Suite externe configurés lors de l'installation.

À partir de Wyse Management Suite 2.1, la **configuration de schéma dynamique** est prise en charge pour les appareils ThinOS 9.x. Vous pouvez ainsi mettre à jour les paramètres de configuration les plus récents sans aucun changement côté serveur. Dans le Cloud public, l'opérateur Wyse Management Suite peut mettre à niveau l'interface utilisateur de configuration 9.x. Pour le Cloud privé (fonctionnalité Pro uniquement), l'utilisateur global peut mettre à niveau l'interface utilisateur de configuration 9.x. Si la fonctionnalité **Multiclient** est activée, l'opérateur Wyse Management Suite peut télécharger le dernier schéma à partir de la section **Administration**.

Étapes

1. Ouvrez une session sur le portail Wyse Management Suite, puis cliquez sur l'onglet d'administration du portail.
2. Cliquez sur **Configuration** sous **Systèmes**.
3. Cochez cette case pour valider le certificat du serveur pour toutes les communications établies entre les périphériques et le serveur.
4. Saisissez les détails suivants dans la zone **Mettre à jour le SMTP pour les alertes par e-mails** :
   - Serveur SMTP
   - Envoyer à partir de l'adresse
   - Nom d'utilisateur
   - Mot de passe
   - Tester l'adresse

   Certificat en cours : cochez la case **Validation de certificat** pour activer la validation CA pour le Cloud privé. Toutes les communications du serveur et du client, y compris le téléchargement de fichier et le téléchargement d'image de système d'exploitation à partir du référentiel local, utilisent le certificat.
   REMARQUE : Si la validation de l'autorité de certification à partir du serveur Wyse Management Suite est activée, le certificat doit être présent sur le client. Toutes les opérations effectuées sur des applications et des données, ainsi que toutes les actions Push/Pull sur des images aboutiront. Si le certificat n'est pas présent sur le client, le serveur Wyse Management Suite génère le message d'événement d'audit générique **Échec de la validation de l'autorité de certification** sur la page **Événements**. Toutes les opérations effectuées sur des applications et des données, ainsi que toutes les actions Push/Pull sur des images n'aboutiront pas. De même, lorsque la validation CA à partir du serveur Wyse Management Suite est désactivée, les communications à partir du serveur et du client se font alors par le biais d'un canal sécurisé sans validation de la signature du certificat.
5. Sélectionnez les options suivantes, puis saisissez les informations suivantes :
   - **Clé/certificat :** téléchargez la paire de fichiers clé/certificat HTTPS (seul le format PEM est pris en charge).
   - **PKCS-12 :** téléchargez HTTPS PKCS-12 (.pfx, .p12). Un certificat intermédiaire Apache est requis pour IIS pfx.
6. Pour mettre à jour les détails du MQTT externe, cliquez sur l'option **Modifier le MQTT externe** et configurez les détails.
7. Pour mettre à jour l'URL externe de Wyse Management Suite, cliquez sur l'option **Modifier l'URL externe WMS** et configurez les détails.
   REMARQUE : Pour rétablir les configurations précédentes, cliquez sur l'option **Rétablir les dernières URL** et cliquez sur **Enregistrer**.
8. Si vous souhaitez mettre à niveau l'interface utilisateur de configuration 9.x, cliquez sur **Choisir des fichiers** dans le champ **Package de l'interface utilisateur de configuration**, puis accédez au fichier .zip.
   REMARQUE : Cette option n'est pas disponible si la fonctionnalité **Multiclient** est activée.

9. Cliquez sur **Enregistrer**.

Configurer un MQTT sécurisé

Depuis Wyse Management Suite 3.2, vous pouvez configurer des connexions sécurisées MQTT pour Windows 10 IoT Enterprise, Dell Hybrid Clients, ThinOS 9.1 MR1 et le référentiel distant.

Étapes

1. Accédez à **Administration du portail** > **Systèmes** > **Configuration**.
2. Pour configurer un MQTT sécurisé, sélectionnez **MQTT sécurisé externe** dans la liste déroulante **MQTT privilégié** dans le champ **URLs WMS**.

Informations importantes

Les appareils dotés d'anciens agents continuent de communiquer avec le port non sécurisé et les appareils dotés de nouveaux agents, tels que les appareils Windows Embedded et les appareils Dell Hybrid Client, peuvent communiquer avec le port sécurisé.

La sélection par défaut pour le MQTT privilégié est MQTT externe : `tcp://<WMS URL>:1883`.

Pour le cloud public, la sélection par défaut pour le MQTT privilégié est MQTT externe : `tcp://<WMS URL>:443`.

Tout appareil enregistré sur le serveur public de Wyse Management Suite se connecte au MQTT externe. Dans le cas où le port distant 1883 est bloqué, l'agent se reconnecte au serveur sécurisé MQTT.

La sélection du MQTT privilégié entre le MQTT externe et le MQTT sécurisé externe n'est disponible que sur le serveur sur site de Wyse Management Suite. En fonction des besoins, le MQTT privilégié peut être mis à jour vers le MQTT sécurisé externe (`tls://<WMS URL>:8443`).

Tout appareil équipé du dernier agent prenant en charge le MQTT sécurisé se connecte au MQTT sécurisé externe. L'ancien agent qui ne prend pas en charge le MQTT sécurisé continue d'utiliser le MQTT externe : `tcp://<WMS URL>:1883`.

Activer Secure LDAP sur SSL

Étapes

1. Exportez la clé publique du certificat au format .cer.
2. Connectez-vous à Wyse Management Suite.
3. Allez dans **Administration du portail** > **Configuration** > **Certificats du magasin de confiance** et importez le certificat.

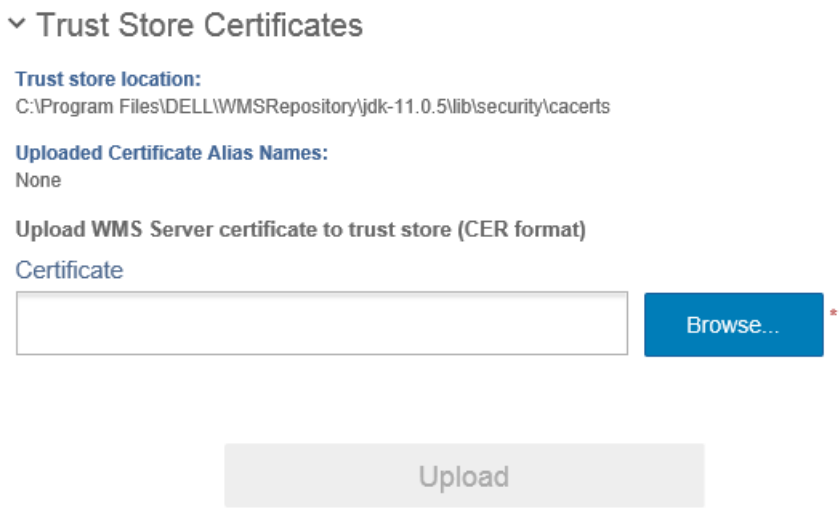


Figure 18. Certificat du magasin de confiance

4. Une fois le certificat LDAP téléchargé, vous pouvez cliquer sur **Enregistrer** ou **Enregistrer et redémarrer**.

   REMARQUE : Vous pouvez également cliquer sur **Annuler** pour arrêter le processus de téléchargement.

5. Sur votre client léger, allez dans **Démarrer** > **Services**, et redémarrez **Dell WMS: Tomcat Service**.
6. Connectez-vous à nouveau à Wyse Management Suite.
7. Allez dans **Administration du portail** > **Active Directory** > **Authentification AD et importation ponctuelle**.
8. Dans le champ **URL du serveur**, entrez l'adresse LDAPS.
9. Dans le champ **Port**, entrez le port sécurisé configuré. Par exemple, 636 ou 3269.
10. Cliquez sur **Enregistrer**.
11. Saisissez les informations d'identification AD et connectez-vous à Active Directory.

    REMARQUE : Après l'installation sur site, vous pouvez importer le certificat du serveur et configurer le LDAP sécurisé en mettant à jour le certificat dans l'écran OOBE.

Étapes suivantes

- Après l'installation sur site avec une seule organisation, accédez à **Administration du portail** > **Configuration** pour importer la clé publique du certificat dans le magasin de confiance. Pour une configuration avec plusieurs organisations, allez dans **Administration de l'opérateur WMS** > **Paramètres du système** > **LDAPS**. Une fois la clé publique importée, cliquez sur **Enregistrer et redémarrer** et le service Tomcat est redémarré.
- Après avoir importé le certificat à l'aide de l'écran OOBE, cliquez sur **Redémarrer maintenant** et Tomcat redémarre automatiquement.

15

Convertir les appareils Dell Wyse 5070 et Dell Ubuntu Generic Clients en Dell Hybrid Client

Vous pouvez convertir les appareils Dell Wyse 5070 exécutant Windows 10 IoT Enterprise LTSB, Windows 10 IoT Enterprise LTSC, ThinLinux 2.x et ThinOS 8.6 vers Dell Hybrid Client à l'aide de Wyse Management Suite Pro 3.1 ou versions ultérieures. Vous pouvez également convertir les systèmes Dell OptiPlex 7070 Ultra exécutant Ubuntu 18.04 et Windows 10 vers Dell Hybrid Client à l'aide de Wyse Management Suite Pro 3.1 ou versions ultérieures.

Sujets :

Conversion des appareils Dell Wyse 5070

Prérequis

- Si l'appareil Wyse 5070 exécutant Windows 10 ou ThinLinux 2.x ne dispose pas de la version la plus récente de l'agent de démarrage, soit une version égale ou supérieure à 4.0.8, téléchargez-la à partir du site de support Dell.
- Si l'appareil Wyse 5070 exécutant ThinOS 8.6_511 ne dispose pas de la version la plus récente de l'agent de démarrage, soit une version égale ou supérieure à 4.0.8, téléchargez-la à partir du site de support Dell.
- Si vous convertissez des appareils Windows 10 IoT Enterprise, téléchargez l'image de Dell Hybrid Client DHC_Wyse_5070_Conversion_Merlin_Image_xxxx_32GB.exe à partir du site de support Dell.
- Si vous convertissez des appareils ThinLinux 2.x ou ThinOS 8.6, téléchargez l'image de Dell Hybrid Client DHC_Wyse_5070_Conversion_Merlin_Image_xxxx_16GB.exe à partir du site de support Dell.
- Assurez-vous d'utiliser Wyse Management Suite Pro 3.1 ou une version supérieure.
- Assurez-vous que le nombre de licences de client hybride est supérieur ou égal au nombre d'appareils qui doivent être convertis en Dell Hybrid Client. Les licences Dell Hybrid Client peuvent être importées dans Wyse Management Suite.
- Si Wyse Management Suite est configuré sur un Cloud public et que vous souhaitez enregistrer l'image de conversion dans un Cloud public, le référentiel sur site doit être installé et configuré localement. Pour plus d'informations, voir la rubrique Référentiel distant.

À propos de cette tâche

Le processus de conversion de Windows 10 IoT Enterprise LTSB, Windows 10 IoT Enterprise LTSC, ThinLinux 2.x et ThinOS 8.6 vers Dell Hybrid Client supprime le contenu et la structure des partitions du lecteur existant. Le processus de conversion conserve uniquement les certificats et les paramètres nécessaires à l'enregistrement de l'appareil dans Wyse Management Suite. Les autres données, certificats et paramètres de configuration ne sont pas conservés. Une fois la conversion vers Dell Hybrid Client effectuée, il n'est pas possible de convertir à nouveau l'appareil à l'état d'origine. Toutefois, vous pouvez restaurer le système d'exploitation d'origine à l'aide de Dell Wyse USB Imaging Tool, disponible sur le site de support Dell. Les données et les paramètres existants ne sont pas restaurés.

Étapes

1. Enregistrez l'image de Dell Hybrid Client dans Wyse Management Suite. Pour plus d'informations sur l'enregistrement, reportez-vous à la section Ajout d'images de client hybride au référentiel.
   - Si la taille de stockage de l'appareil est supérieure à 16 Go, utilisez DHC_CONVERSION_5070.exe.
   - Si la taille de stockage de l'appareil est de 16 Go, utilisez DHC_CONVERSION_5070_16GB.exe.
2. Créez la politique d'image de Dell Hybrid Client. Pour plus d'informations sur la création d'une politique d'image de client hybride, reportez-vous à la section Création de politiques d'image de client hybride.
3. Convertissez l'appareil en Dell Hybrid Client. Pour plus d'informations sur la manière de planifier une image, reportez-vous à la section Planification de la politique d'image.

- L'appareil reçoit une notification de mise à jour de l'image. L'agent de démarrage télécharge l'image à partir du référentiel Wyse Management Suite et installe l'image de Dell Hybrid Client en démarrant en interne l'utilitaire Dell Recovery Tool. Une fois l'opération avec l'image terminée, l'appareil démarre Dell Hybrid Client.
- Dell Client Agent enregistre l'appareil dans Wyse Management Suite en tant que Dell Hybrid Client.
- Wyse Management Suite gère l'appareil en tant que périphérique Dell Hybrid Client.

Ajout d'images de Dell Hybrid Client au référentiel

Étapes

1. Copiez l'image de conversion de Dell Hybrid Client vers l'emplacement du référentiel ou le dossier images du système d'exploitation à l'aide de Wyse Management Suite.

   REMARQUE : Dell Technologies recommande de copier le fichier image sur le système local, puis de copier le fichier dans l'emplacement du référentiel de Wyse Management Suite. Wyse Management Suite extrait les fichiers à partir du dossier compressé et les charge dans l'emplacement du référentiel ou dans le dossier images du système d'exploitation.

   L'image est ajoutée au référentiel.
2. Accédez à **Applications et données** > **Référentiel d'images SE** > **Client hybride** pour afficher l'image enregistrée.

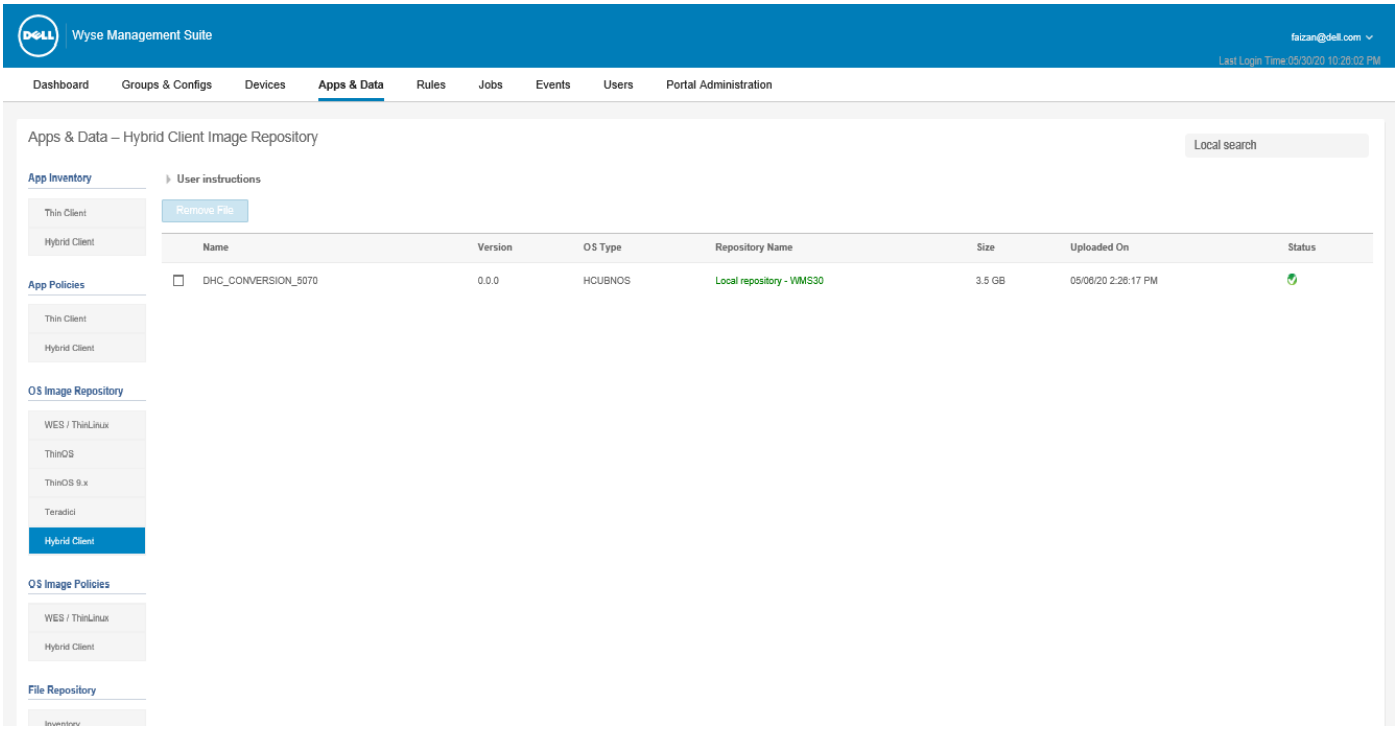


Figure 19. Ajout d'images de Dell Hybrid Client au référentiel

Création de politiques d'image de client hybride

Étapes

1. Accédez à **Applications et données**, puis cliquez sur **Client hybride** sous **Politiques d'image SE**.
2. Cliquez sur **Ajouter une politique**, puis accédez à l'onglet **Modifier la politique des clients hybrides**.
3. Saisissez le **Nom de la politique** et sélectionnez un groupe dans le menu déroulant de l'onglet **Groupe**.
4. Sélectionnez le type de système d'exploitation dans le menu déroulant de l'onglet **Type de système d'exploitation**.
5. Sélectionnez un filtre de sous-type de système d'exploitation dans le menu déroulant de l'onglet **Filtre de sous-type de système d'exploitation**.

REMARQUE : Si vous souhaitez déployer une image sur un système d'exploitation ou une plate-forme spécifique, sélectionnez **Filtre de sous-type de SE** ou **Filtre de plate-forme**.

6. Sélectionnez un fichier image dans le menu déroulant de l'onglet **Image du système d'exploitation**.
7. Sélectionnez **Forcer cette version** dans le menu déroulant de l'onglet **Règle**.
8. Sélectionnez l'une des options suivantes dans le menu déroulant de l'onglet **Appliquer automatiquement la politique** :
   - **Ne pas appliquer automatiquement** : la politique d'image n'est pas appliquée automatiquement à un appareil enregistré avec Wyse Management Suite.
   - **Appliquer la politique aux nouveaux appareils** : la politique d'image est appliquée à un nouvel appareil enregistré avec Wyse Management Suite.
9. Cliquez sur **Enregistrer**.

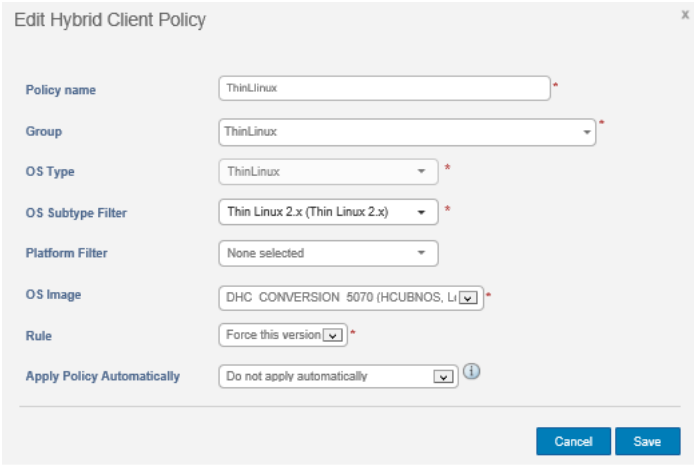


Figure 20. Création de politiques d'image de client hybride

Planification de la politique d'image

Étapes

1. Accédez à **Tâches**, puis cliquez sur l'onglet **Planifier la politique d'image**.
   L'onglet **Tâche de mise à jour d'image** s'affiche.
2. Sélectionnez une politique dans le menu déroulant de l'onglet **Politique**.
3. Saisissez la description de la tâche dans l'onglet **Description**.
4. Sélectionnez la date ou l'heure dans la liste déroulante de l'onglet **Exécuter** comme suit :
   - **Effectif** : saisissez l'heure de début et de fin.
   - **Commence entre** : saisissez l'heure de début et de fin.
   - **Le(s) jour(s)** : sélectionnez les jours de la semaine.
5. Cliquez sur **Aperçu** pour afficher des détails sur la tâche planifiée.
6. Cliquez sur **Planifier** pour lancer la tâche.

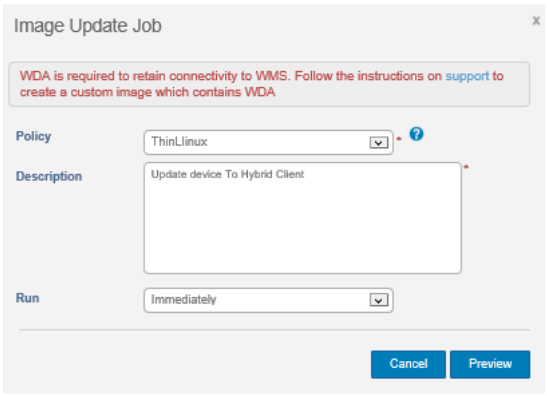


Figure 21. Planification d'une tâche

Convertir Dell Generic Client en Dell Hybrid Client

Prérequis

- DCA-Enabler version 1.2 est nécessaire pour convertir Ubuntu 18.04 ou 20.04 sur l'appareil Dell Ubuntu Generic en Dell Hybrid Client. Vous pouvez télécharger le package à partir de la page **Pilotes et téléchargements** sur www.dell.com/support.
- Si DCA-Enabler version 1.0 ou 1.1 est installé sur votre appareil, vous devez le mettre à niveau vers la version 1.2. Pour mettre à niveau DCA-Enabler, vous devez enregistrer l'appareil dans Wyse Management Suite 3.2 et transmettre `DCA_Enabler_ Package 1.2.0-xx` vers l'appareil à l'aide de Wyse Management Suite, puis déployer `DCA-Enabler 1.2.0-xx`.
- Si l'appareil n'est pas préchargé avec le paquet Dell Hybrid client dans la partition de récupération, vous devez d'abord déployer et installer le package DHC-Fish-Scripts.

REMARQUE : Si la version de DCA-Enabler est 1.1.0-17 ou inférieure, les appareils Dell Ubuntu sont enregistrés dans Wyse Management Suite en tant que Dell Hybrid Client. Si la version de DCA-Enabler est 1.2.0-xx ou supérieure, les appareils sont enregistrés en tant que Dell Generic Client.

Étapes

1. Enregistrez l'appareil auprès de Wyse Management Suite en utilisant DCA-Enabler version 1.2.
2. Convertissez le Generic Client en Hybrid Client en utilisant l'une des méthodes suivantes :
   - À l'aide de la commande Convertir en Hybrid Client : reportez-vous à la rubrique Convertir votre Dell Generic Client en Hybrid Client.
   - Déploiement des paquets ou des fichiers image ISO du Dell Hybrid Client 1.1/1.5 à l'aide de la politique d'application : reportez-vous à la rubrique Créer et déployer une politique d'application standard sur les Dell Generic Clients et Créer et déployer une politique d'application avancée sur les Dell Generic Clients.

     REMARQUE : Avant de lancer la conversion d'appareil, DCA-Enabler sauvegarde les données de connexion de Wyse Management Suite, puis déclenche l'ISO de Dell Hybrid Client ou le pack d'installation.

   Le programme d'installation termine la conversion et l'appareil redémarre automatiquement. Après la conversion, l'appareil démarre dans le système d'exploitation Dell Hybrid Client converti. Dell Client Agent lit les données de connexion sauvegardées de Wyse Management Suite et s'enregistre auprès du serveur Wyse Management Suite en tant qu'appareil Dell Hybrid Client.

Exemple

Pour convertir des Dell Generic Clients fonctionnant sous Ubuntu 18.04 LTS :

- vers Dell Hybrid Client 1.0 ou 1.1, vous devez transmettre les fichiers de package Dell Hybrid Client 1,0 ou 1,1 à l'aide de la politique d'application.
- vers Dell Hybrid Client 1.5, vous devez transmettre le package ISO Dell Hybrid Client à l'aide de la politique d'application. Vous devez transmettre le package de l'outil de mise à niveau de l'image OS `os-upgrade_1.1-10_amd64.deb` , puis transmettre le fichier de package ISO Dell Hybrid Client 1.5.

Pour convertir les Dell Hybrid Clients exécutant Ubuntu 20.04 LTS en Dell Hybrid Client 1.5, vous devez transmettre les fichiers de package Dell Hybrid Client 1.5 à l'aide de la politique d'application.

16

Configurations de sécurité

Cette section décrit les fonctions clés de sécurité de Wyse Management Suite et fournit les procédures nécessaires pour assurer la protection des données et un contrôle d'accès approprié.

Sujets :

Prise en charge de la configuration de versions de TLS dans le programme d'installation de Wyse Management Suite

À partir de Wyse Management Suite 3.0, le programme d'installation sur site est amélioré pour sélectionner la version du protocole TLS lors de l'installation ou de la mise à niveau de Wyse Management Suite. La version recommandée du protocole TLS est 1.2. Assurez-vous de sélectionner toutes les versions de TLS appropriées en fonction de l'agent d'appareil et de l'image Merlin. Les versions plus anciennes de Windows Embedded System, Wyse Device Agent (versions antérieures à WDA_14.4.0.135_Unified) et les versions d'image Merlin 32 bits sont uniquement compatibles avec TLS v1.0. En outre, l'outil d'importation n'est compatible qu'avec TLS v1.0.

REMARQUE : Vous devez sélectionner TLS 1.2 pour configurer Dell Hybrid Client 1.5.

Configuration de la fonctionnalité Active Directory Federation Services sur le Cloud public

Prérequis

- Notepad++ ou une application équivalente doit être installé sur le serveur.
- ADFS doit être installé sur le serveur.

Étapes

1. Sur la page **Administration de portail**, sous **Paramètres de console**, cliquez sur **Active Directory (AD)**.
2. Cliquez sur **Télécharger le fichier xml WMS** dans la section **Fournir les informations WMS à ADFS**.
   `CCM_SP_Metadata.xml` Le fichier est téléchargé.
3. Cliquez avec le bouton droit de la souris sur le fichier et sélectionnez **Modifier avec Notepad++**.
4. Copiez la valeur de l'ID à partir du fichier. Par exemple, ccm-sq3.
5. Accédez à la console de configuration d'ADFS.
6. Cliquez avec le bouton droit de la souris sur **Approbations de partie de confiance** et sélectionnez **Ajouter une approbation de partie de confiance**.
   La fenêtre **Ajouter une approbation de partie de confiance** s'affiche.
7. Cliquez sur **Démarrer**.
   La fenêtre **Sélectionner la source de données** s'affiche.
8. Sélectionnez l'option **Importer les données concernant la partie de confiance à partir du fichier** et accédez au fichier téléchargé `CCM_SP_Metadata.xml`.
9. Cliquez sur **Suivant**.
10. Saisissez la valeur de l'ID (ccm-sq3) dans le champ **Nom d'affichage**, puis cliquez sur **Suivant**.

11. Sur la page **Choisir une stratégie de contrôle d'accès**, cliquez sur **Suivant**.
12. Sur la page **Prêt à ajouter une approbation**, cliquez sur **Suivant**.
13. Cliquez sur **Fermer**.
    L'approbation de partie de confiance créée est répertoriée dans la console de **Approbation de partie de confiance**.
14. Connectez-vous au serveur de Cloud public Wyse Management Suite.
15. Accédez à **Administration de portail** > **Active Directory**, puis cliquez sur **Afficher les règles WMS**.
16. Copiez le contenu affiché dans la fenêtre **Règles WMS**.
17. Accédez à la console ADFS, cliquez avec le bouton droit de la souris sur l'approbation de partie de confiance, puis sélectionnez **Modifier la règle d'émission des revendications**.
18. Cliquez sur **Ajouter une règle** sous l'onglet **Règles de transformation d'émission**.
19. Cliquez sur **OK**.
    La fenêtre **Sélectionner le modèle de règle** s'affiche.
20. Dans la liste déroulante **Modèle de règle de revendication**, sélectionnez l'option **Envoyer des revendications à l'aide d'une règle personnalisée**, puis cliquez sur **Suivant**.
21. Cliquez sur **Ajouter une règle**.
22. Saisissez le **Nom de la règle de revendication** et collez le contenu copié à l'étape 16 dans le champ **Règle personnalisée**.
23. Cliquez sur **Terminer**.
24. Cliquez sur **Appliquer**, puis sur **Ok**.
25. Accédez à **Administration de portail** > **Active Directory**, puis cliquez sur **Ajouter une configuration**.
26. Pour charger le fichier .xml stocké sur votre client léger, cliquez sur **Charger le fichier XML**.
    Le fichier est disponible à l'adresse `https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml`.
27. Cliquez sur **Mettre à jour la configuration**.
28. Pour autoriser les organisations à configurer la connexion par authentification unique à l'aide d'ADFS, cochez la case **Activer la connexion unique avec ADFS**. Cette fonction est régie par la norme Security Assertion and Markup Language (SAML).
29. Pour valider les informations de configuration, cliquez sur **Tester la connexion ADFS**. Cela permet aux organisations de tester leur configuration avant d'enregistrer.
30. Saisissez les informations d'identification ADFS, puis cliquez sur **Connexion**.
    Une fois qu'ADFS est configuré, le message **Test réussi** s'affiche.
31. Importez les utilisateurs de domaine AD à partir de l'espace de stockage distant dans le Cloud public de Wyse Management Suite.
32. Accédez à la page **Utilisateurs** et attribuez des rôles aux utilisateurs de domaine AD importés.
33. Accédez au portail du Cloud public de Wyse Management Suite, puis cliquez sur le lien **Connectez-vous avec vos informations d'identification de domaine**.
34. Saisissez l'adresse e-mail de l'utilisateur de domaine AD importé, puis cliquez sur **Se connecter**.
    Vous êtes redirigé vers le serveur Wyse Management Suite dès que vous vous connectez à ADFS.

Définition d'une configuration LDAP sécurisée ou LDAPS

Pour demander le certificat racine aux services de certificats Active Directory et définir une configuration LDAP sécurisé ou LDAPS, procédez comme suit :

Étapes

1. Accédez au serveur de domaine Active Directory.
2. Accédez à **Démarrer** > **Exécuter**.
3. Saisissez `mmc` et cliquez sur **Ok**.
   La fenêtre **Console1** s'affiche.
4. Accédez à **Fichier** > **Ajouter ou supprimer des snap-ins** (composants logiciels enfichables).
5. Ajoutez les certificats au système local, puis cliquez sur **Ok**.
6. Développez le dossier `Personal` dans le volet de gauche.
7. Cliquez avec le bouton droit de la souris sur Certificats, puis accédez à **Toutes les tâches** > **Demander un nouveau certificat**.
   La fenêtre **Inscription de certificat** s'affiche.

8. Cliquez sur **Suivant**.
9. Sous l'onglet **Sélectionner une politique d'inscription de certificat**, cliquez sur **Suivant**.
10. Sélectionnez **Contrôleur de domaine** et cliquez sur **Inscrire**.
    Le certificat de domaine est installé sur votre contrôleur de domaine.
11. Cliquez sur **Terminer**.
    Le certificat émis à votre contrôleur de domaine s'affiche sur la page des certificats.
12. Cliquez avec le bouton droit de la souris sur le certificat et exportez le certificat sur votre bureau.
13. Importez le certificat de serveur de domaine AD dans le magasin de clés Java de Wyse Management Suite manuellement dans la configuration du serveur Wyse Management Suite. Pour importer le certificat, procédez comme suit :
    a. Accédez au serveur sur lequel est installé Wyse Management Suite.
    b. Ouvrez une fenêtre d'**invite de commande** et exécutez la commande `<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>`.
14. Une fois le certificat installé, redémarrez le service Tomcat de Wyse Management Suite.
15. Connectez-vous au serveur Wyse Management Suite.
16. Accédez à **Administration de portail** > **Active Directory (AD)**.
17. Cliquez sur le lien **Ajouter des informations de serveur AD**.
18. Saisissez le nom de domaine AD.
19. Saisissez l'URL du serveur en tant que **`ldaps://hostname.domain.com`**. Par exemple, **`ldaps://WMS-DC97.WMSAD97.com`**.
20. Saisissez **`636`** comme nom du port.
21. Cliquez sur **Enregistrer**.
22. Cliquez sur **Importer**.
23. Saisissez le nom d'utilisateur et le mot de passe.
24. Cliquez sur **Connexion**.
25. Sur la page **Groupe d'utilisateurs**, cliquez sur **Nom du groupe** et saisissez le nom du groupe.
26. Dans le champ **Rechercher**, saisissez le nom du groupe que vous souhaitez sélectionner.
27. Sélectionnez un groupe.
    Le groupe sélectionné est déplacé vers le volet de droite de la page.
28. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur.
29. Cliquez sur **Importer des utilisateurs** ou **Importer des groupes**.

    Un message de confirmation indiquant le nombre d'utilisateurs Active Directory importés s'affiche sur le portail. Les utilisateurs Active Directory importés sont répertoriés sous l'onglet **Utilisateurs** > **Administrateurs non affectés**.

Protocole obsolète

Le protocole SMB (Server Message Block) version 2.0 est obsolète.

17

Gestion des appareils Teradici

La section Gestion des appareils Teradici fournit des informations sur la gestion et la découverte des périphériques Teradici. La console Gestion des appareils Teradici utilise le SDK pour prendre en charge la gestion et la configuration des périphériques Teradici. Ceci s'applique uniquement au Cloud privé Wyse Management Suite avec le type de licence pro.

Sujets :

Découverte des appareils Teradici

Prérequis

- Installez la dernière version de Wyse Management Suite sur Microsoft Windows 2012 ou une version supérieure. Les appareils Threadx 5.x et 6.x fonctionnent avec la dernière version du système d'exploitation.
- Installez et activez le composant **EMSDK**.
- Le FQDN du serveur Wyse Management Suite doit être disponible pour les configurations **DHCP** ou **DNS**.
- `Cert.pem` Doivent être placés dans le chemin par défaut `C:\Program Files\Dell\WMS\Teradici\EMSDK`. Il est utilisé pour découvrir les appareils Threadx.

Niveau de sécurité

Selon le niveau de sécurité configuré d'un point de terminaison, vous devez également provisionner les points de terminaison avec un certificat EBM/EM.

Les points de terminaison configurés pour le niveau de sécurité moyen ou élevé doivent avoir un certificat de confiance dans leur magasin de certificats avant de pouvoir être connectés à un EBM ou EM. Pour certains points de terminaison, les certificats peuvent être pré-téléchargés par défaut en usine par le fournisseur. Sinon, vous pouvez télécharger manuellement les certificats en utilisant une AWI de point de terminaison.

Les points de terminaison qui sont configurés à un niveau de sécurité faible n'ont pas besoin d'un certificat MC dans leur magasin de certificats de confiance si ce qui suit est vrai :

- Ils utilisent la détection DHCP ou DNS et le serveur DHCP ou DNS les a provisionné avec les empreintes digitales du certificat EBM.
- Ils sont détectés à l'aide de la méthode de détection manuelle.

Tableau 10. Exigences en matière de certificat pour les points de terminaison

Méthode de détection	Sécurité faible	Sécurité moyenne	Sécurité élevée
Détection DHCP/DNS sans empreinte digitale EBM provisionnée	Certificat requis	Certificat requis	Non applicable
Détection DHCP/DNS avec empreinte digitale EBM provisionnée	Certificat non requis	Certificat requis	Non applicable
Détection lancée par un point de terminaison configuré pour un environnement au niveau de sécurité élevé	Non applicable	Non applicable	Certificat requis
Détection manuelle lancée par le MC	Certificat non requis	Non applicable	Non applicable

Découverte manuelle à partir du client

1. Allez à `https://<clientIP>`.
2. Acceptez le message d'avertissement de certificat.
3. Saisissez le mot de passe administrateur (le mot de passe par défaut est Administrator) et connectez-vous.
4. Allez à **téléchargercertificat**. Sélectionnez le fichier `Cert.pem` à partir du chemin par défaut et cliquez sur **Télécharger**.
5. Allez à **Gestion de la configuration**. Cliquez sur le bouton **effacer l'état de gestion** pour enregistrer l'appareil sur le nouveau serveur de gestion.
6. Définissez le **mode découverte du manager** sur manuel
7. Saisissez l'**URL d'amorçage du point de terminaison** selon le format suivant : **wss://<adresse IP du serveur WMS>**.

   REMARQUE : Si EMSDK est installé avec un port personnalisé, fournissez l'**URL d'amorçage du point de terminaison** au format suivant : **wss://<adresse IP:port personnalisé>.**
8. Cliquez sur **Appliquer**, puis sur **Continuer**.
9. L'**état de gestion** s'affiche comme étant Connecté au serveur du point de terminaison.

Ajout de la classe fournisseur du point de terminaison PCoIP au serveur DHCP

1. Connectez-vous au serveur DHCP.
2. Cliquez avec le bouton droit de la souris sur le serveur DHCP dans le volet **SERVEURS** et sélectionnez **Gestionnaire DHCP**.
3. Cliquez avec le bouton droit de la souris sur l'option **IPv4**, puis sélectionnez **Définir les classes de fournisseurs**.
4. Cliquez sur **Ajouter** pour ajouter une nouvelle classe de fournisseur DHCP.
5. Saisissez le **Point de terminaison PCoIP** dans le champ **Nom d'affichage**.
6. Saisissez **Point de terminaison PCoIP** dans la colonne **ASCII** en tant qu'ID de fournisseur.
7. Cliquez sur **OK** pour enregistrer les paramètres.

Configuration des options DHCP

1. Cliquez avec le bouton droit de la souris sur l'option **IPv4** et sélectionnez **Définir les options prédéfinies**.
2. Sélectionnez **Point de terminaison PCoIP** dans la classe **Option,** puis cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Type d'option**, saisissez le nom **EBM URI**, le type de données **Chaîne**, le code **10** et la description **URL d'amorçage du point de terminaison**, puis cliquez sur **OK**.
4. Cliquez sur **OK** pour enregistrer les paramètres.
5. Développez l'étendue DHCP à laquelle vous souhaitez appliquer les options.
6. Cliquez avec le bouton droit de la souris sur **Options d'étendue** et sélectionnez **Configurer les options**.
7. Cliquez sur l'onglet **Avancé**, puis sélectionnez la classe fournisseur du **point de terminaison PCoIP**.
8. Cochez la case **010 EBM URI**, puis saisissez un URI de console de gestion valide dans le champ **Chaîne**. Cliquez sur **Appliquer**. Cet URI nécessite un préfixe WebSocket, comme par exemple, `wss://<adresse IP du MC>:[numéro de port]`. 5172 est le port d'écoute du MC. La saisie de ce numéro de port est une étape facultative.
9. Cliquez sur **OK** pour enregistrer les paramètres.
10. Sélectionnez **Point de terminaison PCoIP** dans la classe **Option,** puis cliquez sur **Ajouter**.
11. Dans la boîte de dialogue **Type d'option**, saisissez le nom **Empreinte digitale EBM X.509 SHA-256**, le type de données **Chaîne**, le code **11** et la description **Empreinte digitale EBM X.509 SHA-256**, puis cliquez sur **OK**.
12. Développez l'étendue DHCP à laquelle vous souhaitez appliquer les options.
13. Cliquez avec le bouton droit de la souris sur **Options d'étendue** et sélectionnez **Configurer les options**.

14. Cliquez sur l'onglet **Avancé**, puis sélectionnez la classe fournisseur du **point de terminaison PCoIP**.
15. Cochez la case **Empreinte digitale 011 EBM X.509 SHA-256** et collez l'empreinte SHA-256.
16. Cliquez sur **OK** pour enregistrer les paramètres.
17. Rendez-vous sur le navigateur Web client.
18. Allez à **Gestion de la** > **configuration** et définissez le **mode découverte du manager** sur Automatique
19. Le client est connecté au serveur qui est mentionné dans le serveur DHCP.

Création de l'enregistrement SRV de DNS

1. Connectez-vous au **serveur DNS**.
2. Cliquez avec le bouton droit de la souris sur le serveur DNS, volet **SERVEURS** et sélectionnez le **Gestionnaire DNS** dans le menu contextuel.
3. Dans l'option **Zones de recherche directe**, cliquez avec le bouton droit de la souris sur le domaine et sélectionnez **Autres nouveaux enregistrements** dans le menu contextuel.
4. Dans la boîte de dialogue **Type d'enregistrement de ressource**, sélectionnez **Emplacement du service (SRV)** dans la liste, puis cliquez sur **Créer un enregistrement**.
5. Définissez **Service** sur **_pcoip-bootstrap**, le protocole sur **_tcp** et **Numéro de port** sur **5172**, c'est-à-dire le port d'écoute par défaut du MC. Dans **Hôte offrant ce service**, saisissez le FQDN du MC.

   REMARQUE : Le nom de domaine complet du MC doit être renseigné car la spécification DNS n'autorise pas d'adresse IP dans les enregistrements SRV.
6. Cliquez sur **OK**.

Ajout d'un enregistrement TXT de DNS

1. Dans l'option **Zones de recherche directe**, cliquez avec le bouton droit de la souris sur le domaine et sélectionnez **Autres nouveaux enregistrements** dans le menu contextuel.
2. Dans la boîte de dialogue **Type d'enregistrement de ressource**, sélectionnez **Texte (TXT)** dans la liste, puis cliquez sur **Créer un enregistrement**.
3. Saisissez les informations suivantes :
   a. Dans le champ **Nom d'enregistrement**, saisissez le nom d'hôte du serveur Wyse Management Suite offrant le service. Le champ FQDN est automatiquement renseigné. Il doit correspondre au FQDN du serveur Wyse Management Suite.
   b. Dans le champ **Texte**, entrez **pcoip-Bootstrap-cert=** et collez l'empreinte digitale SHA-256 du certificat de serveur Wyse Management Suite.
4. Cliquez sur **OK**.
5. Rendez-vous sur le navigateur Web client.
6. Le client est connecté au serveur Wyse Management Suite qui est mentionné dans le serveur DHCP.

Création d'empreintes digitales SHA-256

1. Lancez Mozilla Firefox.
2. Allez dans l'onglet **Options > Avancées**
3. Cliquez sur **Certificats** pour afficher les certificats.
4. Sous **Gestionnaire de certificat**, cliquez sur **Autorités**, puis sur **Importer**.
5. Parcourez le certificat, puis cliquez sur **Afficher**.

6. Copiez l'empreinte digitale **SHA-256**.

DLCI_UG Scénarios de cas d'utilisation CIFS

Les cas d'utilisation suivants sont pris en charge dans Wyse Management Suite :

- Lorsque vous sélectionnez **Wyse Management Suite** comme **type d'installation** lors de l'installation du Cloud privé Wyse Management Suite.
  - La page de configuration CIFS s'affiche. Cette page est requise car nous devons configurer le dossier partagé.
    REMARQUE : L'option **Configuration des informations d'identification de l'utilisateur du système CIFS** est désactivée par défaut.
- Lorsque vous sélectionnez **EMSDK Teradici** comme **type d'installation** lors de l'installation du Cloud privé Wyse Management Suite.
  - Pour les informations d'identification CIFS, vous pouvez utiliser un compte existant ou en créer un.
- Lorsque vous sélectionnez **Wyse Management Suite** et **EMSDK Teradici** comme **type d'installation** lors de l'installation du Cloud privé Wyse Management Suite.
  - La page de configuration CIFS s'affiche. Cette page est requise car nous devons configurer le dossier partagé.
    REMARQUE : L'option **Configuration des informations d'identification de l'utilisateur du système CIFS** est désactivée par défaut.
  - Pour les informations d'identification CIFS, vous pouvez utiliser un compte existant ou en créer un.
- Lorsque vous installez uniquement EMSDK sur un système sur lequel le service EMSDK est déjà installé.
  - Si EMSDK Teradici est sélectionné, un message d'avertissement s'affiche lorsque vous cliquez sur **Suivant** dans la page **Type d'installation**. Le message est **Le programme d'installation a détecté que l'EMSDK Teradici est déjà installé. L'EMSDK sera mis à jour si nécessaire**. Aucun numéro de port n'est requis.
    - Si l'option **Configuration des informations d'identification de l'utilisateur du système CIFS** est sélectionné (par défaut)
      1. Arrêtez le service.
      2. Mettez à jour le service EMSDK.
      3. Redémarrez le service. Il fonctionne sous le même utilisateur pré-configuré.
    - Si l'option **Configuration des informations d'identification de l'utilisateur du système CIFS** est sélectionnée avec l'option **Utiliser un utilisateur existant**.
      1. Arrêtez le service.
      2. Mettez à jour le service EMSDK.
      3. Mettez à jour le journal de service de l'utilisateur en fonction de celui sélectionné.
      4. Redémarrez le service. Il fonctionne sous le même utilisateur pré-configuré.
    - Si l'option **Configuration des informations d'identification de l'utilisateur du système CIFS** est sélectionnée avec l'option **Créer un nouvel utilisateur**.
      1. Arrêtez le service.
      2. Mettez à jour le service EMSDK.
      3. Mettez à jour le journal de service de l'utilisateur en fonction du nouvel utilisateur créé.
      4. Redémarrez le service. Il fonctionne sous le même utilisateur pré-configuré.
- Lorsque vous installez **Wyse Management Suite** et **EMSDK Teradici** sur un système qui a déjà le service EMSDK installé.
  - Identique à **Lorsque vous installez uniquement EMSDK sur un système sur lequel le service EMSDK est déjà installé** sauf que l'option **Configuration des informations d'identification de l'utilisateur du système CIFS** est sélectionnée par défaut et est grisée. Vous devez saisir les informations d'identification CIFS.

18

Gestion des abonnements de licence

Cette section vous permet d'afficher et de gérer l'abonnement de licence de la console de gestion et son utilisation.

Sur la page **Administration de portail**, vous pouvez afficher l'option **Abonnement**. Cette page fournit les informations suivantes :

- Abonnement de licence
- Commandes de licences
- Utilisation des licences : appareils clients légers enregistrés
- Informations sur le serveur
- Importer une licence : Cloud privé
- Exporter la licence pour le Cloud privé : Cloud public

Sujets :

Importer des licences à partir du Cloud public Wyse Management Suite

Vous pouvez importer des licences du Cloud public Wyse Management Suite vers le Cloud privé Wyse Management Suite.

Étapes

1. Connectez-vous à la console du Cloud privé de Wyse Management Suite.
2. Accédez à **Administration de portail** > **Comptes** > **Abonnement**.
3. Indiquez les détails du Cloud public Wyse Management Suite :
   - Nom d'utilisateur
   - Mot de passe
   - Datacenter
   - Nombre d'emplacements TC
   - Nombre d'emplacements Edge Gateway et PC intégré
   - Nombre d'emplacements Thin Client Wyse Software
   - Nombre d'emplacements pour client hybride
   - Nombre d'emplacements/appareils Generic Client
4. Cliquez sur **Importer**.

   REMARQUE : Le Cloud privé Wyse Management Suite doit être connecté au Cloud public Wyse Management Suite.

   REMARQUE : Le nombre total d'appareils Generic gérables dépend du nombre total d'appareils disponibles pour les licences Hybrid Client et Thin Client.

Exporter des licences vers le Cloud privé Wyse Management Suite

Vous pouvez exporter des licences vers le Cloud privé Wyse Management Suite à partir du Cloud public Wyse Management Suite.

Étapes

1. Connectez-vous à la console du cloud public Wyse Management Suite.
2. Accédez à **Administration de portail** > **Comptes** > **Abonnement**.
3. Saisissez le nombre d'emplacements Thin Client qui doivent être exportés vers le cloud privé Wyse Management Suite.
4. Cliquez sur **Exporter**.
5. Copiez la clé de licence générée.
6. Connectez-vous à la console du cloud privé de Wyse Management Suite.
7. Accédez à **Administration de portail** > **Comptes** > **Abonnement**.
8. Saisissez la clé de licence générée dans la zone.
9. Cliquez sur **Importer**.

Allocation de licences Thin Client

Vous pouvez allouer des licences Thin Client entre le compte de Cloud privé Wyse Management Suite et le compte de Cloud public Wyse Management Suite.

Étapes

1. Connectez-vous à la console de cloud public Wyse Management Suite.
2. Accédez à **Administration de portail** > **Comptes** > **Abonnement**.
3. Saisissez le nombre d'emplacements des clients légers.

   REMARQUE : Les emplacements Thin Client peuvent être gérés dans le cloud public. Le nombre saisi d'emplacements Thin Client ne doit pas dépasser le nombre affiché dans l'option **Gérable**.

4. Cliquez sur **Exporter**.

   REMARQUE : Le nombre de licences de cloud public est ajusté en fonction du nombre d'emplacements Thin Client exportés vers le cloud privé.

5. Copiez la clé de licence générée.
6. Connectez-vous à la console du Cloud privé de Wyse Management Suite.
7. Accédez à **Administration de portail** > **Comptes** > **Abonnement**.
8. Importez la clé de licence exportée vers le cloud privé.

   REMARQUE : La licence ne peut pas être importée si le nombre d'emplacements Thin Client est insuffisant pour gérer le nombre de périphériques actuellement gérés dans le cloud privé. Dans ce cas, répétez les étapes 3 à 8 pour allouer des emplacements Thin Client.

   REMARQUE : À partir de Wyse Management Suite 3.2, les anciens serveurs de Wyse Management Suite ne peuvent plus être activés en ligne depuis le Cloud public.

Commandes de licences

Dans le Cloud public, la section **Commandes de licences** affiche la liste des commandes passées, y compris des licences expirées. Par défaut, les commandes expirées ne sont pas affichées. Cochez la case **Inclure les commandes expirées** pour afficher les commandes expirées. Les commandes expirées s'affichent en rouge et les commandes qui expirent dans un délai de 30 jours ou moins s'affichent en orange.

REMARQUE : Cette fonctionnalité est non applicable au déploiement sur site, car elle n'affiche pas l'historique des commandes. Cependant, l'historique des commandes de licences sur site est disponible lorsque vous vous connectez au portail du Cloud public en tant qu'admin client.

19

Mise à niveau de micrologiciel

Vous pouvez utiliser Wyse Management Suite pour mettre à niveau votre firmware.

Sujets :

Mise à niveau de ThinLinux 1.x vers 2.1 et versions supérieures

Si vous souhaitez extraire une image personnalisée de TL 2.x avant la mise à niveau, vous devez préparer ThinLinux 2.x puis mettre à niveau l'image de ThinLinux 1.x.

Préparation de l'image ThinLinux 2.x

Prérequis

Utilisez Wyse Management Suite version 1.4 pour mettre à niveau ThinLinux version 2.0.19 ou 2.1 vers la version 2.2.

Étapes

1. Rendez-vous sur www.dell.com/support.
2. Cliquez sur **Support du produit**, saisissez le **numéro de série** de votre client léger, puis cliquez sur **Envoyer**.

   REMARQUE : Si vous ne disposez pas du **numéro de série**, recherchez manuellement votre modèle de client léger.
3. Cliquez sur **Pilotes et téléchargements**.
4. Dans la liste déroulante **Système d'exploitation**, sélectionnez **ThinLinux**.
5. Téléchargez les modules complémentaires `merlin_nonpxe-4.0.1-0 0.04.amd64.deb` et `wda_3.4.6-05_amd64.tar`.
6. Copiez et téléchargez le module complémentaire vers `<drive C>/wms/localrepo/repository/thinClientsApps/`.
7. Sur le client léger exécutant ThinLinux 2.x, accédez à **Paramètres** > **Gestion** > **Wyse Device Agent**.
8. Enregistrez l'appareil sur le serveur Wyse Management Suite.
9. Fermez la fenêtre **Paramètres**.

   REMARQUE : Si la fenêtre Paramètres n'est pas fermée, le message d'erreur **Profil verrouillé** s'affiche après avoir déployé l'image.
10. Connectez-vous à la console Wyse Management Suite.
11. Créez et déployez une politique d'application pour les modules complémentaires `merlin_nonpxe-4.0.1-0 0.04.amd64.deb` et `wda_3.4.6-05_amd64.tar`.
12. Redémarrez le client léger.
13. Connectez-vous au serveur Wyse Management Suite.
14. Accédez à la page de l'appareil et assurez-vous que les versions Merlin et WDA sont mises à jour.
15. Cliquez sur l'appareil enregistré, puis accédez à **Autres actions** > **Extraire l'image du SE**.
    La fenêtre **Extraire l'image du SE** s'affiche.
16. Saisissez le nom de l'image.
17. À partir de la liste déroulante Référentiel de fichiers, sélectionnez le référentiel de fichiers.
18. Sélectionnez le type d'opération d'extraction que vous souhaitez effectuer.

- **Par défaut** : cochez la case **SE + restauration** pour extraire l'image (compressée/non compressée).
- **Avancé** : sélectionnez le modèle `Compress_OS_Recovery_Commandsxml/uncompress_OS_Recovery_CommandsXml` pour extraire l'image.

Résultats

REMARQUE :
- Si vous utilisez le référentiel distant Wyse Management Suite 1.3, le fichier .xml n'est pas disponible dans le référentiel. Vous devez mettre à niveau Wyse Management Suite vers la version 1.4 ou des versions supérieures pour accéder au fichier.
- La restauration de l'opération d'extraction ne conserve pas les paramètres utilisateur.

Mise à niveau de ThinLinux 1.x vers la version 2.x

Étapes

1. Rendez-vous sur www.dell.com/support.
2. Cliquez sur **Support du produit**, saisissez le **numéro de série** de votre client léger, puis cliquez sur **Envoyer**.

   REMARQUE : Si vous ne disposez pas du **numéro de série**, recherchez manuellement votre modèle de client léger.
3. Cliquez sur **Pilotes et téléchargements**.
4. Dans la liste déroulante **Système d'exploitation**, sélectionnez **ThinLinux**.
5. Faites défiler la page et procédez comme suit :
   - Téléchargez les modules complémentaires `Platform_util-1.0.26-0.3.x86_64.rpm`, `wda-2.1.23-00.01.x86_64.rpm`, et `merlin-nonpxe_3.7.7-00.05_amd64.deb`.
   - Téléchargez le fichier image le plus récent de ThinLinux version 2.x (`2.1.0.01_3040_16GB_merlin.exe` ou `2.2.0.00_3040_merlin_16GB.exe`).
6. Sur le client léger, accédez à **Paramètres** > **Gestion** > **Wyse Device Agent**.
7. Enregistrez l'appareil sur le serveur Wyse Management Suite.
8. Connectez-vous à la console Wyse Management Suite.
9. Créez et déployez une politique d'application pour les modules complémentaires `Platform_util-1.0.26-0.3.x86_64.rpm`, `wda-2.1.23-00.01.x86_64.rpm`, et `merlin-nonpxe_3.7.7-00.05_amd64.deb`.
10. Redémarrez le client léger.
11. Connectez-vous au serveur Wyse Management Suite.
12. Copiez le fichier image téléchargé (`2.2.0.00_3040_merlin_16GB.exe`) vers `<drive C>/wms/localrepo/repository/osimages/zipped/`.

    REMARQUE : L'image dans le dossier compressé est extraite vers un dossier valide. Le processus d'extraction peut prendre 10 à 15 minutes.
13. Connectez-vous à la console Wyse Management Suite.
14. Accédez à **Applications et données** > **Référentiel d'images SE** > **WES/ThinLinux**, puis vérifiez que l'image ThinLinux est disponible.
15. Accédez à **Applications et données** > **Politiques d'image SE (WES/ThinLinux)** et cliquez sur **Ajouter une politique**.
16. Dans la fenêtre Ajouter une politique, configurez les options suivantes :
    - **Type de système d'exploitation** : ThinLinux
    - **Sous-filtre du système d'exploitation** : ThinLinux(ThinLinux)
    - **Règle** : Mise à niveau uniquement/Forcer cette version

    REMARQUE : Sélectionnez l'image extraite/image à jour copiée dans le référentiel lors de la création de la politique.
17. Mettez à jour les autres champs obligatoires tel que requis, puis cliquez sur **Enregistrer**.
18. Planifiez la tâche.
19. Cliquez sur **Mettre à jour maintenant** sur le client pour mettre à jour l'image.

Mise à niveau de ThinOS 8.x vers 9.0

Vous devez utiliser Wyse Management Suite 2.0 et versions supérieures pour mettre à niveau votre firmware ThinOS vers la version 9.0.

Le tableau suivant répertorie les images du firmware ThinOS :

Tableau 11. Images de firmware

Plateforme	Image de firmware ThinOS
Wyse 3040 Thin Client	A10Q_wnos
Wyse 5070 Thin Client avec processeur Celeron	X10_wnos
Wyse 5070 Thin Client avec processeur Pentium	X10_wnos
Wyse 5070 Extended Thin Client avec processeur Pentium	X10_wnos
Wyse 5470 Thin Client	X10_wnos
Wyse 5470 Thin Client tout-en-un	X10_wnos

Ajouter le firmware ThinOS 9.x au référentiel

Étapes

1. Connectez-vous à Wyse Management Suite.
2. Dans l'onglet **Applications et données**, sous **Référentiel d'images SE**, cliquez sur **ThinOS 9.x**.
3. Cliquez sur **Ajouter un fichier de firmware**.
   L'écran **Ajouter un fichier** s'affiche.
4. Pour sélectionner un fichier, cliquez sur **Parcourir** et accédez à l'emplacement où se trouve votre fichier.
5. Saisissez la description de votre fichier.
6. Cochez cette case si vous souhaitez remplacer un fichier existant.
7. Cliquez sur **Télécharger**.

   REMARQUE : Le fichier est ajouté au référentiel lorsque vous cochez la case, mais il n'est attribué à aucun des appareils ou groupes. Pour déployer un firmware sur un appareil ou un groupe d'appareils, accédez à la page de configuration de l'appareil ou du groupe correspondant.

   REMARQUE : L'opérateur peut télécharger le firmware à partir du compte opérateur et celui-ci est visible par toutes les organisations. Les organisations ne peuvent pas supprimer ou modifier les fichiers.

Mettre à niveau ThinOS 8.6 vers ThinOS 9.x

Prérequis

- L'image de conversion ThinOS doit être ajoutée au référentiel du firmware ThinOS. Pour plus d'informations, voir Ajouter le firmware ThinOS au référentiel.
- Créez un groupe dans Wyse Management Suite à l'aide d'un jeton de groupe. Utilisez ce jeton de groupe pour enregistrer les appareils ThinOS 8.6.
- Le client léger doit être enregistré pour Wyse Management Suite.
- Ne configurez aucun paramètre de fond d'écran sur Wyse Management Suite.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **ThinOS**.
   La fenêtre **Sélectionner le mode de configuration de ThinOS** s'affiche.
3. Sélectionnez **Mode Configuration avancée**.
4. Accédez à **Mise à niveau du firmware**, puis cliquez sur **Configurer cet élément**.

5. Désactivez les options **Désactiver la mise à niveau en direct** et **Vérifier la signature**.
6. Dans la liste déroulante **Type de plate-forme**, sélectionnez une plate-forme.
7. Dans la liste déroulante **Firmware à déployer automatiquement**, sélectionnez le firmware ajouté au référentiel.
8. Cliquez sur **Enregistrer et publier**.
   Le firmware est déployé sur le client léger. Le processus de conversion prend entre 15 et 20 s et le client léger redémarre automatiquement.

   REMARQUE : Une fois le firmware mis à niveau, l'appareil est automatiquement enregistré dans Wyse Management Suite. Les configurations de build 8.6 ne sont pas héritées suite à la mise à niveau du firmware.

Mise à niveau de ThinOS 9.x vers des versions supérieures à l'aide de Wyse Management Suite

Prérequis

- Assurez-vous d'avoir créé un groupe dans Wyse Management Suite à l'aide d'un jeton de groupe. Utilisez ce jeton de groupe pour enregistrer les appareils ThinOS 9.x.
- Assurez-vous que le client léger est enregistré auprès de Wyse Management Suite.

Étapes

1. Accédez à la page **Groupes et configurations**, puis sélectionnez un groupe.
2. Dans le menu déroulant **Modifier les politiques**, cliquez sur **ThinOS 9.x**.
   La fenêtre **Contrôle de configuration | ThinOS** s'affiche.
3. Cliquez sur **Avancé**.
4. Dans le champ **Firmware**, sélectionnez **Mises à jour du firmware du système d'exploitation**.
5. Cliquez sur **Parcourir** pour localiser et télécharger le firmware.
   Les détails du contrat EULA du package et le nom des fournisseurs s'affichent.
6. Cliquez sur les noms des fournisseurs pour lire le contrat de licence de chaque fournisseur, puis cliquez sur **Accepter** pour charger le package.

   Vous pouvez sélectionner l'option **Ne plus afficher** si vous ne souhaitez plus voir les détails du contrat EULA du même fournisseur.

   REMARQUE : Si vous chargez plusieurs packages, les détails du contrat EULA de chaque package s'affichent. Vous devez accepter le contrat de licence des packages individuellement. Le firmware n'est pas chargé si vous cliquez sur **Refuser**.
7. Dans le menu déroulant **Sélectionner le firmware ThinOS à déployer**, sélectionnez le firmware téléchargé.
8. Cliquez sur **Enregistrer et publier**.
   Le client léger télécharge le firmware et redémarre. La version du firmware est mise à niveau.

20

Logithèque distante

Wyse Management Suite vous permet d'avoir des logithèques locales et distantes pour des applications, des images de système d'exploitation et ainsi de suite. Si les comptes d'utilisateur sont répartis entre différentes zones géographiques, avoir une logithèque locale pour chaque compte d'utilisateur réparti peut être utile afin que les appareils puissent télécharger des images de leur logithèque locale. Cette flexibilité est fournie avec le logiciel `WMS_Repo.exe`. `WMS_Repo.exe` est un logiciel de logithèque de fichiers Wyse Management Suite qui aide à créer des logithèques distantes réparties pouvant être enregistrées avec Wyse Management Suite. Le logiciel `WMS_Repo.exe` est disponible uniquement pour les abonnés licence **Pro**.

Prérequis

- Si vous utilisez Wyse Management Suite avec un déploiement dans le Cloud, accédez à **Administration de portail** > **Paramètres de la console** > **Référentiel de fichiers**. Cliquez sur **Télécharger la version x.x** et téléchargez le fichier `WMS_Repo.exe`.
- Les exigences du serveur pour installer le logiciel Wyse Management Suite Repository sont les suivantes :
  - Windows 2012 R2 ou Windows Server 2016 Standard
  - 4 CPU
  - 8 Go de RAM
  - Espace de stockage de 40 Go

À propos de cette tâche

Procédez comme suit pour installer le logiciel **WMS-Repo** :

Étapes

1. Ouvrez une session en tant qu'**Administrateur** et installez `WMS_Repo.exe` sur le serveur de logithèque.
2. Cliquez sur **Suivant** et conformez-vous aux instructions affichées à l'écran pour terminer l'installation.
3. Cliquez sur **Lancer** pour lancer l'écran d'**enregistrement de la logithèque WMS** sur le navigateur Web.
4. Sélectionnez **Enregistrer sur le portail de gestion public WMS** si vous êtes enregistré sur le cloud public.

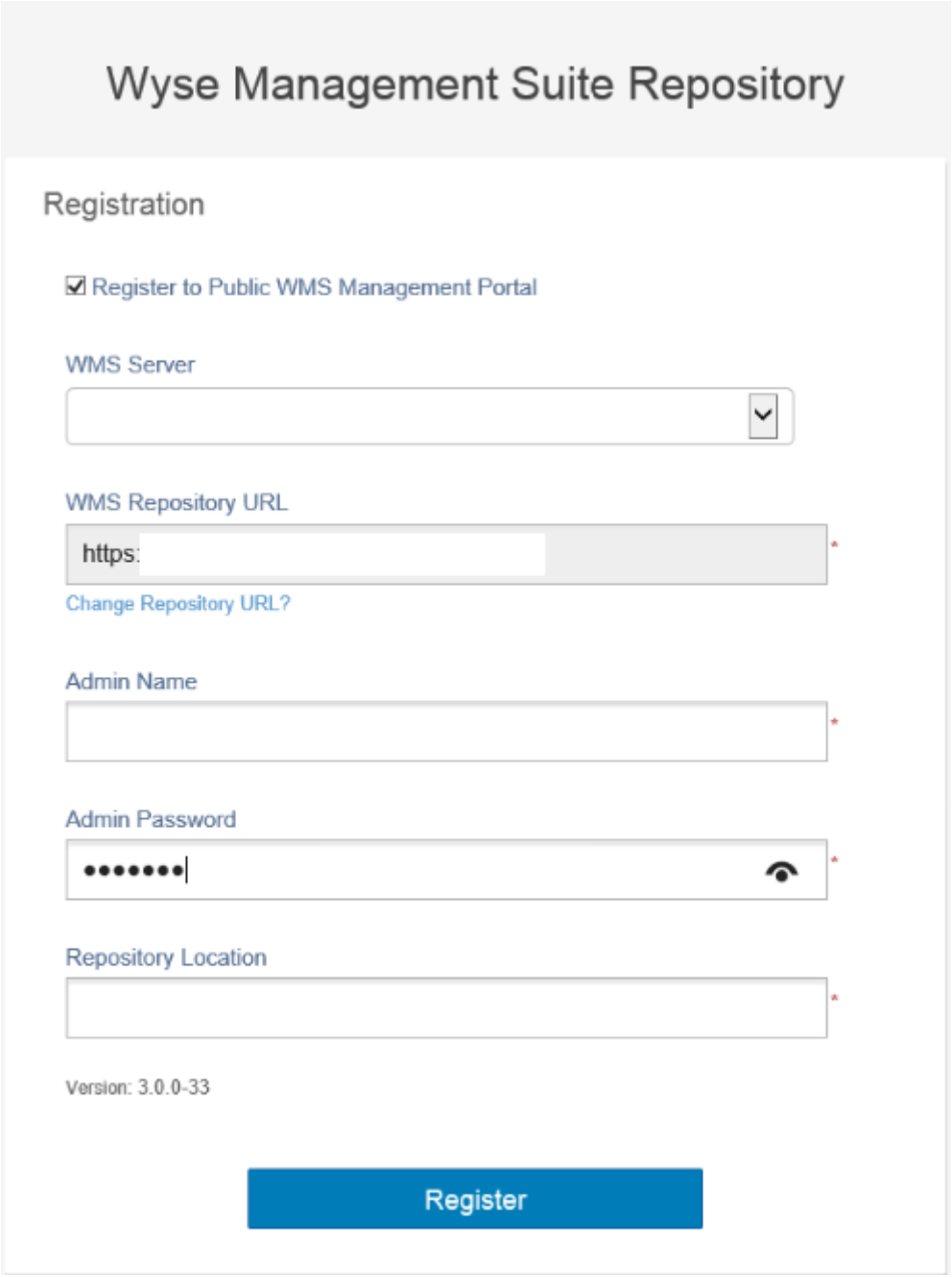


Figure 22. S'enregistrer sur un cloud public

5. Saisissez les informations suivantes :
   a. URL de serveur Wyse Management Suite

      REMARQUE : À moins de vous être enregistré avec Wyse Management Suite version 1.0, vous ne pouvez pas utiliser l'URL du serveur MQTT.

   b. URL de WMS Repository (mettez à jour l'URL avec le nom de domaine)
   c. Informations sur le nom d'utilisateur de l'administrateur Wyse Management Suite
   d. Informations sur le mot de passe de connexion de l'administrateur Wyse Management Suite
   e. Informations sur le chemin de la logithèque
6. Cliquez sur **Enregistrer**.
7. Si l'enregistrement est réussi, la fenêtre **Enregistrement** s'affiche :

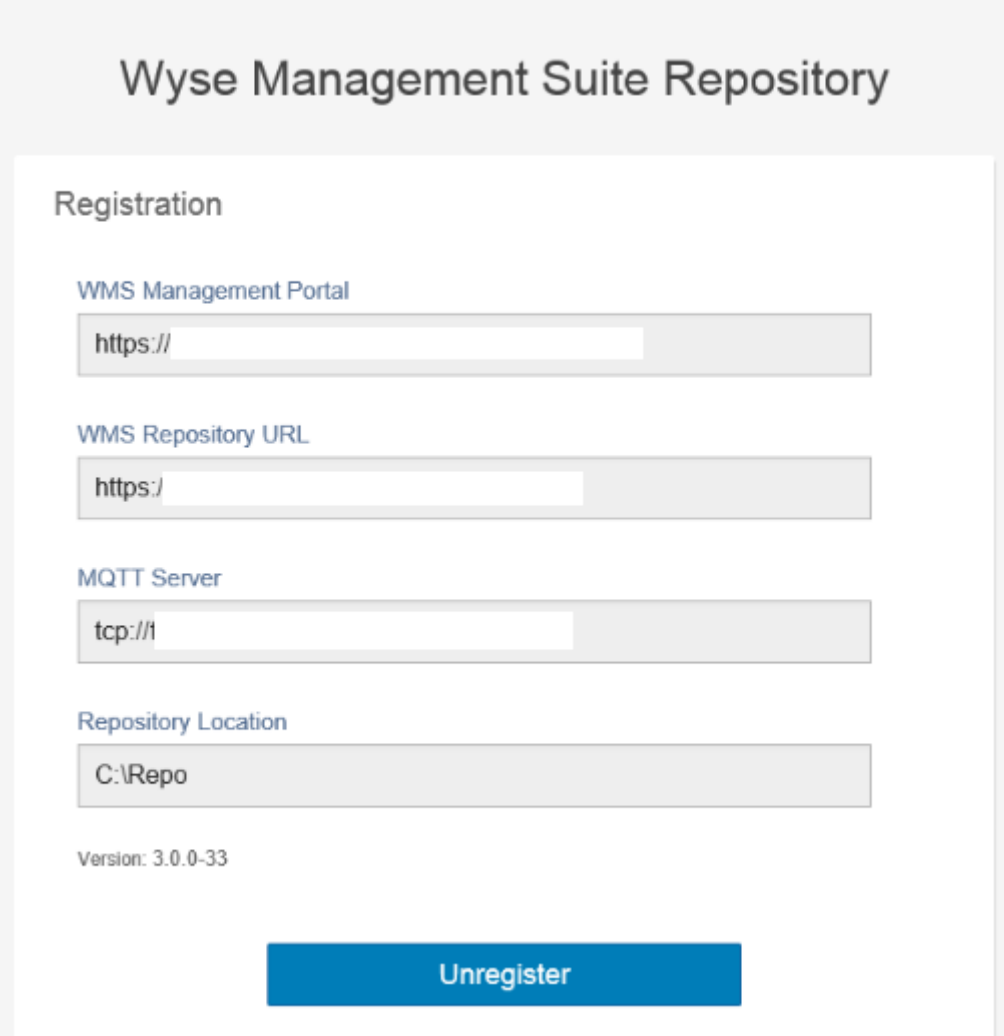


Figure 23. Enregistrement réussi

8. L'écran suivant sur le portail Wyse Management Suite confirme la réussite de l'enregistrement de la logithèque distante :

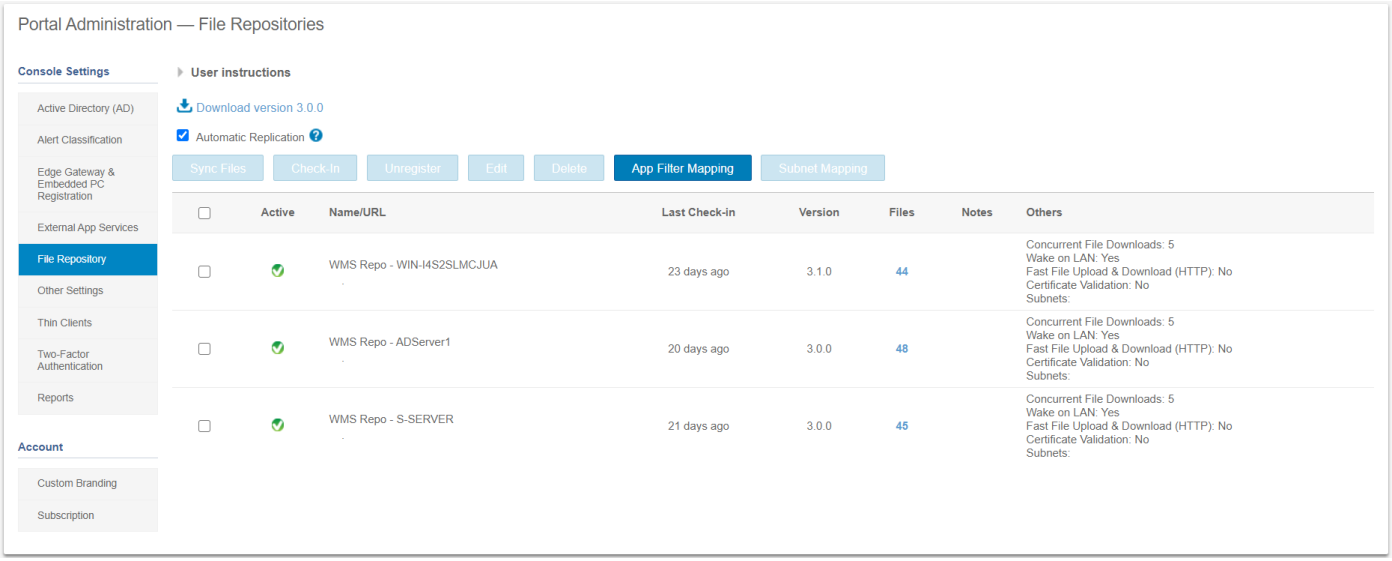


Figure 24. Enregistrement réussi sur le portail

9. HTTPS est activé par défaut avec `WMS_Repo.exe` et est installé avec le certificat auto-signé. Pour installer votre propre certificat spécifique au domaine, faites défiler la page d'enregistrement pour charger les certificats SSL.

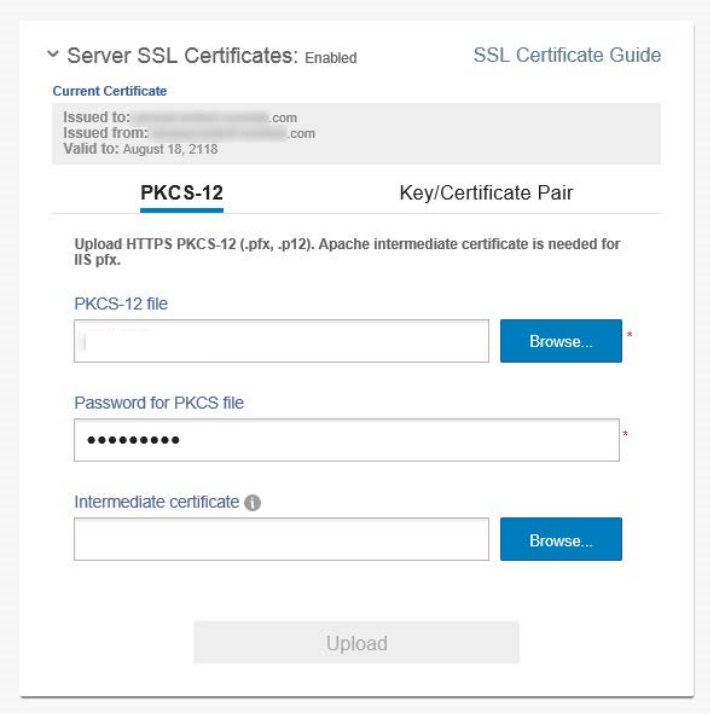


Figure 25. Téléchargement d'un certificat

10. Le serveur redémarre et le certificat chargé s'affiche.

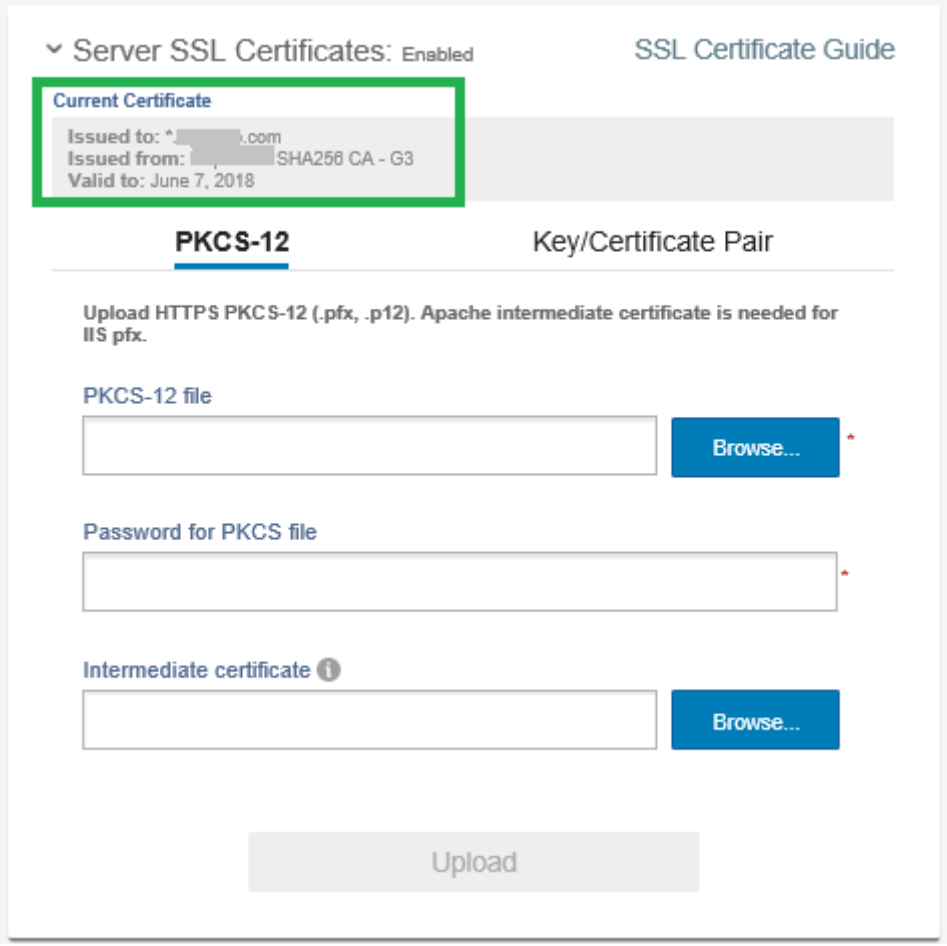


Figure 26. Certificat SSL activé

11. Si Wyse Management Suite est activé avec un certificat auto-signé ou un certificat de domaine privé, vous pouvez le charger sur le serveur Wyse Management Suite Repository pour valider les informations d'identification CA Wyse Management Suite.

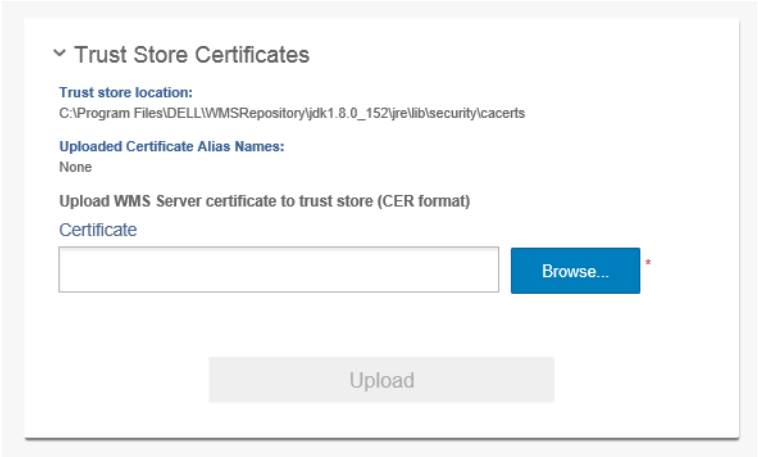


Figure 27. Certificats du magasin de confiance

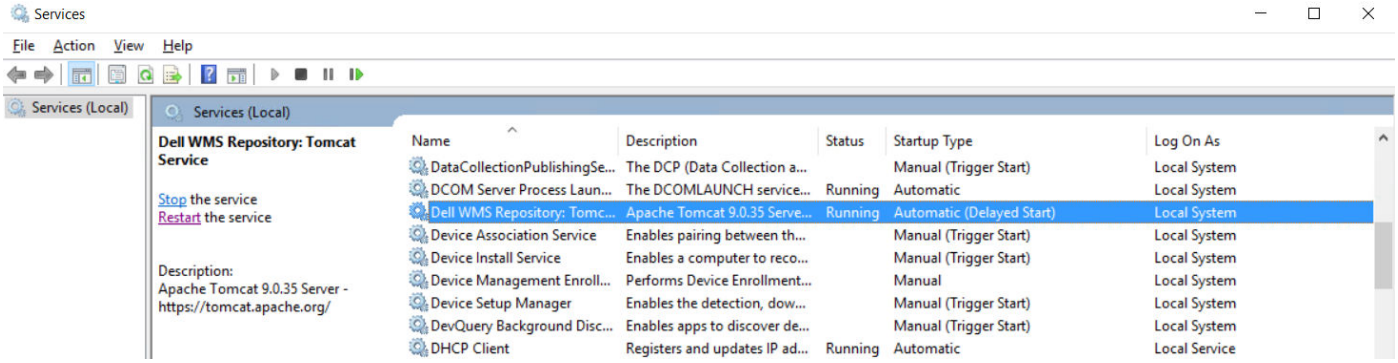
12. Accédez à l'emplacement C:\wmsrepo que vous avez saisi lors de votre enregistrement pour afficher les dossiers dans lesquels tous les fichiers de la logithèque sont enregistrés et gérés.

Sujets :

- Gestion du service Wyse Management Suite Repository
- Prise en charge du proxy des référentiels distants de Wyse Management Suite

Gestion du service Wyse Management Suite Repository

Wyse Management Suite Repository s'affiche en tant que **Dell WMS Repository : service Tomcat** dans la fenêtre Services Locaux de Windows et est configuré pour démarrer automatiquement lorsque le serveur redémarre.



Prise en charge du proxy des référentiels distants de Wyse Management Suite

Les référentiels à distance prennent en charge le proxy SOCKS5 et HTTPS pour toutes les communications HTTPS et MQTT vers Wyse Management Suite à partir de Wyse Management Suite 3.2.

Seuls les proxys au niveau du système sont pris en charge, car le référentiel distant s'exécute en tant que service Windows. En outre, seuls sont pris en charge les proxys avec authentification AD ou sans authentification. Vous pouvez configurer les serveurs proxy à l'aide de n'importe quelle méthode. Vous trouverez ci-dessous quelques exemples sur la façon de configurer les informations de serveur proxy :

- À l'aide de la commande netsh : vous pouvez utiliser la commande suivante pour configurer les informations du serveur proxy.
  - Proxy SOCKS5

```
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
```

  - Proxy HTTPs

```
netsh winhttp set proxy proxy-server="https=<ProxyServerIP>:<Port number>" bypass-
list="localhost"

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

Current WinHTTP proxy settings:

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

- À l'aide du fichier WPAD configuré dans DHCP : le serveur de référentiel Wyse Management Suite doit être configuré avec l'adresse IP DHCP et Internet Explorer doit être configuré pour détecter automatiquement les paramètres. Vous devez configurer la balise d'option DHCP 252 avec le fichier WPAD.pac. Vous trouverez ci-dessous un exemple de contenu du fichier PAC :

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

```
    return "DIRECT";
}
```

Vous pouvez également configurer les paramètres de proxy à l'aide des politiques de groupe.

REMARQUE : Les paramètres de proxy sont lus lorsque le service de référentiel démarre. Si vous apportez des modifications aux paramètres de proxy ultérieurement, vous devez redémarrer le service de référentiel.

REMARQUE : La résolution du nom de l'hôte n'est pas définie si le proxy SOCKS4 est utilisé. Vous devez mettre à jour le fichier hôtes présent dans `C:\Windows\System32\drivers\etc` pour résoudre l'URL ou le nom de l'hôte du Cloud public sur le serveur sur lequel le référentiel Wyse Management Suite est installé. En cas d'utilisation d'un proxy SOCKS5, le nom de l'hôte est résolu à l'aide des DNS configurés dans les paramètres réseau du serveur.

21

Prise en charge du proxy pour Windows Embedded Standard WDA et Dell Hybrid Client DCA

Windows Embedded Standard WDA prend en charge le proxy HTTPS, et Dell Hybrid Client DCA prend en charge les proxy HTTP et SOCKS5 pour toutes les communications HTTP et sécurisées MQTT avec le serveur public de Wyse Management Suite. Seuls les proxys au niveau du système sont pris en charge, car WDA et DCA s'exécutent en tant que service.

Les proxys avec authentification AD ou sans authentification sont pris en charge. Le script PAC qui est configuré en utilisant l'option DHCP tag 252 est pris en charge. Les paramètres du proxy sont lus lorsque les services WDA et DCA démarrent. En cas de modification des paramètres du proxy, les services WDA et DCA doivent être redémarrés.

Les limitations de la prise en charge du proxy sont les suivantes :

- Les proxy qui sont configurés au niveau de l'utilisateur ne sont pas pris en charge.
- L'utilisateur n'a pas à saisir de nom d'utilisateur et de mot de passe.
- Il n'y a pas d'interface utilisateur pour saisir l'URL du proxy car les détails du proxy sont lus à partir du système d'exploitation sous-jacent.
- Le MQTT externe avec 1883 ne prend pas en charge le proxy.
- Le proxy HTTP n'est pas pris en charge.
- Le fichier PAC proxy via DNS n'est pas pris en charge.

Sujets :

Configurer les informations du serveur proxy en utilisant le proxy WININET pour Windows Embedded Standard WDA

Vous devez configurer la politique de domaine pour définir le paramètre WININET proxy au niveau du système pour tous les appareils.

Étapes

1. Ouvrez l'**invite de commande** en tant qu'administrateur.
2. Exécutez la commande `gpedit.msc`.
3. Configurez la politique de groupe à partir du contrôleur de domaine pour activer la configuration du proxy IE par machine. Pour configurer la politique, allez dans **Configuration de l'ordinateur** > **Modèles administratifs** > **Composants Windows** > **Internet Explorer** > **Paramètres de proxy par-machine** et activez l'option.
4. Exécutez `gpupdate/force` dans la même invite de commande.
5. Ouvrez Internet Explorer en tant qu'administrateur et allez dans **Connexions** > **Paramètres LAN**.
6. Configurez le proxy et cliquez sur **OK**.

Configuration des informations du serveur proxy à l'aide de la balise d'option DHCP pour Windows Embedded Standard WDA et Dell Hybrid Client DCA

Les appareils Windows Embedded Standard et Dell Hybrid Client doivent être configurés avec l'IP DHCP. Pour la configuration DHCP, la balise d'option DHCP 252 doit être configurée avec le fichier WPAD.pac.

Vous trouverez ci-dessous un exemple de contenu de fichier PAC (WPAD.dat) :

```
function FindProxyForURL(url, host)
{
        if (shExpMatch(host, "*wysemanagementsuite.com*"))
{
        return "SOCKS 100.xxx.xxx.xxx:1080";
}
        return "DIRECT";
}
```

Les limitations sont les suivantes :

- Seule la communication sécurisée MQTT prend en charge le proxy.
- Le port 1833 de MQTT ne prend pas en charge le proxy.

22

Troubleshooting your device

Vous pouvez afficher et gérer les informations de dépannage à l'aide de la page **Appareils**.

Étapes

1. Sur la page **Détails sur le périphérique**, cliquez sur l'onglet **Dépannage**.
2. Cliquez sur **Demander une capture d'écran**.
   Vous pouvez capturer l'écran du client léger avec ou sans l'autorisation du client. Si vous cochez la case **Exiger l'acceptation de l'utilisateur**, un message s'affiche sur le client. Cette option s'applique uniquement aux appareils Windows Embedded Standard, Linux et ThinLinux.
3. Cliquez sur **Demander la liste des processus** pour afficher la liste des processus en cours d'exécution sur le Thin Client.
4. Cliquez sur **Demander la liste des services** pour afficher la liste des services en cours d'exécution sur le Thin Client.
5. Cliquez sur **Lancer le suivi** pour accéder à la console Mesures de performance.
   Dans la console **Mesures de performance**, les détails suivants s'affichent :
   - Moyenne de la dernière minute du processeur
   - Utilisation moyenne de la mémoire de dernière minute

Sujets :

Demander un fichier journal à l'aide de Wyse Management Suite

Prérequis

L'appareil doit être activé pour pouvoir extraire le fichier journal.

Étapes

1. Rendez-vous sur la page **Appareils**, puis cliquez sur un appareil particulier.
   Les détails de l'appareil s'affichent.
2. Cliquez sur l'onglet **Journal de l'appareil**.
3. Cliquez sur **Demander un fichier journal**.
4. Une fois les fichiers journaux chargés sur le serveur Wyse Management Suite, activez le lien **Cliquez ici**, puis téléchargez les journaux.

   REMARQUE : L'appareil ThinOS charge les journaux système.

Afficher les journaux d'audit à l'aide de Wyse Management Suite

Étapes

1. Accédez à **Événements** > **Audit**.

2. Dans la liste déroulante **Groupes de configuration**, sélectionnez un groupe pour lequel vous souhaitez afficher le journal d'audit.
3. Dans la liste déroulante **Plage de temps**, sélectionnez la plage de temps pour afficher les événements qui se sont produits au cours de cette période.
   La fenêtre **Audit** organise les informations dans une vue de journal d'audit type. Vous pouvez afficher l'horodatage, le type d'événement, la source et la description de chaque événement dans l'ordre chronologique.

L'appareil ne parvient pas à s'enregistrer sur Wyse Management Suite lorsque le proxy WinHTTP est configuré

WDA est un client WinHTTP qui récupère les informations du proxy WinHTTP à partir du système local.

Si vous avez configuré le proxy WinHTTP et que le périphérique ne parvient pas à contacter le serveur Wyse Management Suite, procédez comme suit pour activer les informations de Proxy disponibles au niveau du système :

- **Cas 1** : lorsque l'appareil est ajouté à un domaine, activez les configurations de proxy IE pour chaque utilisateur à l'aide de la stratégie de groupe du domaine. Vous devez configurer la stratégie de groupe à partir du contrôleur de domaine pour activer les configurations de proxy IE pour chaque client, et non pour chaque utilisateur.

  Accédez à `Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Make proxy settings per-machine`, puis sélectionnez **Activer**. Accédez également à `Paramètres d'IE > Options Internet > Connexions > Paramètres réseau` dans Internet Explorer, puis cochez la case **Détecter automatiquement les paramètres de connexion**.

- **Cas 2** : lorsque l'appareil n'est pas ajouté à un domaine, accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings`, créez un **DWORD 32 bits** nommé **ProxySettingsPerUser**, puis définissez-le sur 0. Accédez également à `Paramètres d'IE > Options Internet > Connexions > Paramètres réseau` dans Internet Explorer, puis cochez la case **Détecter automatiquement les paramètres de connexion**.

La politique de redirection USB RemoteFX ne s'applique pas aux appareils de stockage de masse USB

Étapes

1. Connectez-vous à l'appareil en tant qu'administrateur.
2. Désactivez le filtre d'écriture.
3. Accédez à la commande **Exécuter** et saisissez **`Regedit`**.
4. Rendez-vous sur `HKLM\Software\Policies\Microsoft\Windows NT\Terminal Services\Client\UsbSelectDeviceByInterfaces`.
5. Ajoutez la clé de registre de chaîne **`100`** et définissez la valeur d'appareil de stockage de masse comme `{53F56307-B6BF-11D0-94F2-00A0C91EFB8B} for CD ROM : {53F56308-B6BF-11D0-94F2-00A0C91EFB8B}`.

   REMARQUE : L'utilisation d'accolades est obligatoire.

Les paramètres WiFi configurés à partir de Wyse Management Suite ne sont pas persistants sur plusieurs Wyse 5070 Thin Clients

Lorsque vous configurez une connexion WiFi sur Wyse 5070 Thin Client, celui-ci se connecte à un réseau sans fil spécifique (SSID) sans demander le mot de passe. Lorsque la même configuration est exportée vers Wyse Management Suite et déployée sur d'autres

Wyse 5070 Thin Clients, la configuration est appliquée et vous êtes invité à saisir un mot de passe pour vous connecter au même réseau sans fil. Pour rendre les paramètres WiFi persistants, procédez comme suit :

Étapes

1. Connectez Wyse 5070 Thin Client au réseau sans fil.
2. Exécutez le fichier `DWirelessProfileEditor.exe`.
   La fenêtre **Éditeur de mots de passe de profils sans fil** s'affiche.
3. Accédez au chemin de destination pour enregistrer le profil sous forme de fichier xml et cliquez sur **Enregistrer**.
4. Cliquez sur le bouton **Exporter les profils WiFi** dans la fenêtre **Éditeur de mots de passe de profils sans fil**.
5. Dans la liste déroulante **Profils**, sélectionnez le profil pour déployer la configuration.
6. Effacez le champ **Mot de passe**, et saisissez à nouveau le mot de passe.
7. Cliquez sur **Modifier le mot de passe**.

   REMARQUE : Ne cliquez pas à nouveau sur le bouton **Exporter les profils WiFi**.

8. Fermez la fenêtre **Éditeur de mots de passe de profils sans fil**.
9. Connectez-vous à Wyse Management Suite.
10. Accédez à **Applications et Données** > **Référentiel de fichiers** > **Inventaire**.
11. Cliquez sur **Ajouter un fichier**.
12. Accédez au fichier xml.
13. Dans la liste déroulante **Type**, sélectionnez **Profil sans fil Windows**.
14. Saisissez la description.
15. Sélectionnez l'option **Remplacer un fichier existant** si vous souhaitez écraser la configuration actuelle.
16. Cliquez sur **Télécharger**.
17. Accédez à **Groupes et configurations** > **Modifier les profils** > **WES** > **Réseau**.
18. Cliquez sur **Configurer cet élément**.
19. Dans la liste déroulante **Profil sans fil Windows**, sélectionnez le fichier téléchargé.
20. Cliquez sur **Enregistrer et publier**.

23

Questions fréquemment posées

Sujets :

Entre Wyse Management Suite et l'interface utilisateur ThinOS, lequel des deux est prioritaire lorsque des paramètres en conflit sont appliqués ?

Tous les paramètres configurés à l'aide de Wyse Management Suite sont prioritaires sur les paramètres qui ont été configurés localement sur le client ThinOS ou publiés à l'aide de l'outil de politique d'administration.

L'ordre suivant définit la priorité définie pour les configurations ThinOS :

Politiques Wyse Management Suite > **Outil de politique d'administration** > **Interface utilisateur ThinOS locale**

Comment utiliser le référentiel de fichiers Wyse Management Suite ?

Étapes

1. Téléchargez Wyse Management Suite Repository à partir de la console de cloud public.
2. Après le processus d'installation, démarrez l'application.
3. Sur la page Wyse Management Suite Repository, saisissez les informations d'identification pour enregistrer le référentiel Wyse Management Suite sur le serveur Wyse Management Suite.
4. Pour enregistrer le référentiel dans le Cloud public Wyse Management Suite, activez l'option **Enregistrer sur le portail de gestion public WMS**.
5. Cliquez sur l'option **Synchroniser les fichiers** pour envoyer la commande de synchronisation des fichiers.
6. Cliquez sur **Vérification**, puis sur **Envoyer la commande** pour envoyer la commande d'informations sur l'appareil à l'appareil.
7. Cliquez sur l'option **Annuler l'enregistrement** pour désenregistrer le service sur site.
8. Cliquez sur **Modifier** pour apporter des modifications aux fichiers.
   a. Dans la liste déroulante **Téléchargements de fichiers simultanés**, sélectionnez le nombre de fichiers.
   b. Activez ou désactivez l'option **Wake on LAN**.
   c. Activez ou désactivez l'option **Téléchargement de fichier rapide (HTTP)**.
      - Lorsque HTTP est activé, ce protocole est utilisé pour le chargement et le téléchargement de fichiers.
      - Lorsque HTTP n'est pas activé, le protocole HTTPS est utilisé pour le chargement et le téléchargement de fichiers.
   d. Cochez la case **Validation de certificat** pour activer la validation de l'autorité de certification (CA) pour un Cloud public.

   REMARQUE :

- Si la validation CA à partir du serveur Wyse Management Suite est activée, le certificat doit être présent sur le client. Toutes les opérations, comme celles effectuées sur des applications et des données, ainsi que toutes les actions d'extraction/envoi d'images aboutiront. Si le certificat n'est pas présent sur le client, le serveur Wyse Management Suite génère le message d'événement d'audit générique **Échec de la validation de l'autorité de certification** sur la page **Événements**. Toutes les opérations, comme celles effectuées sur des applications et des données, ainsi que toutes les actions d'extraction/envoi d'images n'aboutiront pas.
- Si la validation CA à partir du serveur Wyse Management Suite est désactivée, les communications à partir du serveur et du client se font par le biais d'un canal sécurisé sans validation de la signature du certificat.

e. Ajoutez une note dans la zone prévue à cet effet.
f. Cliquez sur **Enregistrer les paramètres**.

Comment importer des utilisateurs à partir d'un fichier .csv ?

Étapes

1. Cliquez sur **Utilisateurs**.
   La page **Utilisateurs** s'affiche.
2. Sélectionnez l'option **Administrateurs non affectés**.
3. Cliquez sur **Importer en bloc**.
   La fenêtre **Importer en bloc** s'affiche.
4. Cliquez sur **Parcourir** et sélectionnez le fichier .csv.
5. Cliquez sur **Importer**.

Comment vérifier la version de Wyse Management Suite

Étapes

1. Connectez-vous à Wyse Management Suite.
2. Accédez à **Administration de portail** > **Abonnement**.
   La version de Wyse Management Suite s'affiche dans le champ **Informations sur le serveur**.

Créer et configurer des balises d'option DHCP

Étapes

1. Ouvrez le gestionnaire de serveur.
2. Sélectionnez **Outils** et cliquez sur l'**option DHCP**.
3. Accédez à **FQDN** > **IPv4** et cliquez avec le bouton droit de la souris sur **IPv4**.
4. Cliquez sur **Définir les options prédéfinies**.
   La fenêtre **Options et valeurs prédéfinies** s'affiche.
5. Dans la liste déroulante **Classe d'options**, sélectionnez la valeur **Option standard DHCP**.
6. Cliquez sur **Ajouter**.
   La fenêtre **Type d'option** s'affiche.
7. Configurez les balises d'option DHCP requises.
   - Pour créer la balise d'option 165 d'URL du serveur Wyse Management Suite, procédez comme suit :
     a. Saisissez les valeurs suivantes, puis cliquez sur **OK**.
        - Nom : WMS
        - Type de données : chaîne
        - Code : 165

- Description : WMS_Server

b. Saisissez la valeur suivante, puis cliquez sur **OK**.

Chaîne : `WMS FQDN`

- Pour créer la balise d'option 166 d'URL du serveur MQTT, procédez comme suit :

a. Saisissez les valeurs suivantes, puis cliquez sur **OK**.
   - Nom : MQTT
   - Type de données : chaîne
   - Code : 166
   - Description : Serveur MQTT

b. Saisissez la valeur suivante, puis cliquez sur **OK**.

Chaîne : `MQTT FQDN`

Par exemple, **`NomServeurWMS.VotreDomaine.Com:1883`**

- Pour créer la balise d'option 167 d'URL du serveur de validation CA Wyse Management Suite, procédez comme suit :

a. Saisissez les valeurs suivantes, puis cliquez sur **OK**.
   - Nom : validation CA
   - Type de données : chaîne
   - Code : 167
   - Description : validation CA

b. Saisissez les valeurs suivantes, puis cliquez sur **OK**.

Chaîne : VRAI ou FAUX

- Pour créer la balise d'option 199 d'URL du serveur jeton de groupe Wyse Management Suite, procédez comme suit :

a. Saisissez les valeurs suivantes, puis cliquez sur **OK**.
   - Nom : jeton de groupe
   - Type de données : chaîne
   - Code : 199
   - Description : jeton de groupe

b. Saisissez les valeurs suivantes, puis cliquez sur **OK**.

Chaîne : defa-quarantine

REMARQUE : Les options doivent être ajoutées aux options de serveur du serveur DHCP ou aux options d'étendue de l'étendue DHCP.

Créer et configurer des enregistrements SRV DNS

Étapes

1. Ouvrez le gestionnaire de serveur.
2. Accédez à **Outils**, puis cliquez sur **DNS**.
3. Accédez à **DNS** > **Nom d'hôte du serveur DNS** > **Zones de recherche directes** > **Domaine** > **_tcp** et cliquez avec le bouton droit sur l'option **_tcp**.
4. Cliquez sur **Nouveaux enregistrements**.
   La fenêtre **Type d'enregistrement de ressource** s'affiche.
5. Sélectionnez **Emplacement du service (SRV)**, cliquez sur **Créer un enregistrement** et procédez comme suit :

a. Pour créer un enregistrement de serveur Wyse Management Suite, saisissez les détails suivants et cliquez sur **OK**.
   - Service : _WMS_MGMT
   - Protocole : _tcp
   - Numéro du port : 443
   - Hôte offrant ce service : FQDN du serveur WMS.

b. Pour créer un enregistrement de serveur MQTT, saisissez les valeurs suivantes, puis cliquez sur **OK**.
   - Service : _WMS_MQTT
   - Protocole : _tcp
   - Numéro du port : 1883
   - Hôte offrant ce service : FQDN du serveur MQTT.

6. Accédez à **DNS** > **Nom d'hôte du serveur DNS** > **Zones de recherche directes** > **Domaine** , puis cliquez avec le bouton droit de la souris sur le domaine.
7. Cliquez sur **Nouveaux enregistrements**.
8. Sélectionnez **Texte (TXT)**, cliquez sur **Créer un enregistrement** et procédez comme suit :
   a. Pour créer un enregistrement de jeton de groupe Wyse Management Suite, saisissez les détails suivants et cliquez sur **OK**.
      - Nom d'enregistrement : _WMS_GROUPTOKEN
      - Texte : jeton de groupe WMS

   b. Pour créer un enregistrement de validation CA Wyse Management Suite, saisissez les détails suivants et cliquez sur **OK**.
      - Nom d'enregistrement : _WMS_CAVALIDATION
      - Texte : VRAI/FAUX

Modifier le nom d'hôte en adresse IP

À propos de cette tâche

Vous devez modifier le nom d'hôte en adresse IP en cas d'échec de la résolution du nom d'hôte.

Étapes

1. Ouvrez l'invite du DOS en mode administrateur élevé.
2. Changer le répertoire en **`C:\Program Files\DELL\WMS\MongoDB\bin`**.
3. Entrez la commande **`mongo localhost -username stratus -p --authenticationDatabase admin`**
   Sortie : MongoDB shell version v4.2.12
4. Entrez le mot de passe.
   Sortie—
   - Connexion à : mongodb://127.0.0.1:27017/localhost
   - Version du serveur MongoDB : 4.2.12
5. Entrée : utiliser stratus
   Sortie—passé à db stratus
6. Entrez la commande **`> db.bootstrapProperties.updateOne( {'name': 'stratusapp.server.url'}, {$set : {'value' : "https://IP:443/ccm-web"}} )`**
   Sortie—{ "acknowledged" : true, "matchedCount" : 1, "modifiedCount" : 1 }
7. Entrez la commande **`> db.getCollection('bootstrapProperties').find({'name': 'stratusapp.server.url'})`**
   Sortie—{ "_id" : ObjectId("5b97905e48b7b7e99ad22aa6"), "name" : "stratusapp.server.url", "value" : "https://IP:443/ccm-web", "isActive" : true, "committed" : true }

Créer une image de l'appareil à l'aide d'un référentiel distant auto-signé

Vous pouvez créer une image des appareils Windows Embedded Standard et ThinLinux à partir du référentiel local du Cloud privé ou à partir du référentiel distant du Cloud public.

Prérequis

Si l'image est déployée à partir du référentiel local du Cloud privé ou à partir du référentiel distant du Cloud public avec un certificat auto-signé, l'administrateur doit envoyer le certificat auto-signé aux clients légers pour créer des images lorsque la validation CA est activée.

Étapes

1. Exportez le certificat auto-signé à partir d'Internet Explorer ou de MMC.
2. Téléchargez le certificat vers Wyse Management Suite : voir Politique d'image.
3. Envoyez le certificat aux clients ou groupes de clients cibles à l'aide de la politique de sécurité.
   Attendez que la **tâche de politique de configuration** se termine.
4. Activez la validation CA à partir du référentiel local du Cloud privé ou à partir du référentiel distant du Cloud public.
5. Créez une politique d'image et planifiez-la dans le groupe.