

# Dell Wyse Management Suite

Guía del administrador versión 2.1

Identifier	GUID-5B8DE7B7-879F-45A4-88E0-732155904029
Version	15
Status	Translation Validated

## Notas, precauciones y advertencias

 **NOTA:** Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.

 **PRECAUCIÓN:** Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

 **AVISO:** Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

# Tabla de contenido

<b>Capítulo 1: Introducción a Wyse Management Suite.....</b>	<b>8</b>
Ediciones de Wyse Management Suite.....	8
Matriz de funciones de Wyse Management Suite.....	9
<b>Capítulo 2: Introducción a Wyse Management Suite.....</b>	<b>11</b>
Iniciar sesión en Wyse Management Suite en la nube pública.....	11
Requisitos previos para implementar Wyse Management Suite en la nube privada.....	12
Áreas funcionales de la consola de administración.....	13
Configurar y administrar clientes delgados.....	13
Wyse Device Agent.....	14
<b>Capítulo 3: Instalar o actualizar Wyse Device Agent.....</b>	<b>16</b>
Instalar Wyse Device Agent manualmente en un dispositivo Windows Embedded.....	16
Actualizar Wyse Device Agent mediante la política de la aplicación de Wyse Management Suite.....	17
Instalar o actualizar Wyse Device Agents en clientes ThinLinux o Linux.....	17
<b>Capítulo 4: Registrar y configurar un nuevo dispositivo mediante Wyse Management Suite.....</b>	<b>19</b>
Registrar y configurar un nuevo dispositivo Windows Embedded Standard mediante Wyse Management Suite.....	19
Registrar y configurar un nuevo dispositivo ThinOS 8.x mediante Wyse Management Suite.....	20
Registrar y configurar un nuevo dispositivo ThinOS 9.x mediante Wyse Management Suite.....	20
Registrar y configurar un nuevo dispositivo Linux o ThinLinux mediante Wyse Management Suite.....	21
Registrar y configurar un nuevo cliente esbelto de Wyse Software mediante Wyse Management Suite.....	22
<b>Capítulo 5: Panel de Wyse Management Suite.....</b>	<b>23</b>
Ver alertas.....	23
Ver la lista de eventos.....	24
Ver el estado del dispositivo.....	24
Activar la validación de certificados.....	24
Cambiar preferencias de usuario.....	25
Acceder a ayuda en línea.....	25
Cambiar la contraseña.....	25
Cerrar sesión desde la consola de administración.....	25
<b>Capítulo 6: Administrar grupos y configuraciones.....</b>	<b>26</b>
Editar un grupo sin administrar.....	27
Crear un grupo de políticas de dispositivo predeterminado.....	28
Crear un grupo de selección de ThinOS.....	28
Crear un grupo predeterminado de políticas de dispositivo.....	29
Editar un grupo de selección de ThinOS.....	29
Eliminar un grupo de selección de ThinOS.....	29
Configurar una política de nivel global.....	30
Crear un grupo de políticas de usuario.....	30
Editar un grupo de políticas de usuario.....	30

Importar un grupo de políticas de usuario.....	31
Importar un grupo de políticas de grupo desde Active Directory.....	31
Eliminar un grupo.....	31
Configurar una política del nivel del dispositivo.....	32
Exportar políticas de grupos.....	32
Importar políticas de grupos.....	32
Importar políticas de grupos desde la página Grupos y configuraciones.....	33
Importar políticas de grupos desde la página Editar políticas.....	33
Editar la configuración de la política de ThinOS.....	34
ThinOS: modo de asistente.....	35
ThinOS: modo avanzado.....	35
Editar la configuración de la política de ThinOS 9.x.....	35
Configuraciones del BIOS para ThinOS 9.x.....	36
Cargar e insertar paquetes de OS.....	37
Cargar e insertar paquetes de BIOS.....	37
Cargar y subir paquetes de aplicaciones de ThinOS 9.x mediante Wyse Management Suite.....	38
Editar la configuración de la política de Windows Embedded Standard.....	38
Editar la configuración de la política de Linux.....	38
Editar la configuración de la política de ThinLinux.....	39
Editar la configuración de la política de Wyse Software Thin Client.....	39
Editar la configuración de la política de Cloud Connect.....	39
<b>Capítulo 7: Administrar dispositivos.....</b>	<b>40</b>
Métodos para registrar los dispositivos en Wyse Management Suite.....	41
Registrar dispositivos ThinOS mediante Wyse Device Agent.....	41
Registrar clientes esbeltos de Windows Embedded Standard para Wyse Management Suite mediante Wyse Device Agent.....	42
Registrar el cliente esbelto de Wyse Software en Wyse Management Suite mediante Wyse Device Agent...	43
Registrar clientes esbeltos de ThinLinux mediante Wyse Device Agent.....	43
Registrar dispositivos ThinOS mediante el método FTP INI.....	44
Registrar dispositivos ThinLinux versión 2.0 mediante el método FTP INI.....	44
Registrar dispositivos ThinLinux versión 1.0 mediante el método FTP INI.....	45
Registrar dispositivos mediante etiquetas de opciones de DHCP.....	46
Registrar dispositivos mediante registro SRV DNS.....	46
Buscar un dispositivo mediante filtros.....	48
Guardar el filtro en la página Dispositivos.....	48
Consultar el estado del dispositivo.....	49
Bloquear los dispositivos.....	49
Reiniciar los dispositivos.....	49
Anular el registro del dispositivo.....	49
Validación de la inscripción.....	50
Validar la inscripción de un dispositivo.....	50
Restablecer el dispositivo a los ajustes predeterminados de fábrica.....	51
Cambiar la asignación de un grupo en la página Dispositivos.....	51
Enviar mensajes a un dispositivo.....	51
Activar el dispositivo.....	52
Ver los detalles del dispositivo.....	52
Administrar el resumen del dispositivo.....	52
Ver información del sistema.....	53
Ver eventos del dispositivo.....	53

Ver las aplicaciones instaladas.....	53
Renombrar el cliente delgado.....	54
Configurar la conexión de seguimiento remoto.....	54
Apagar dispositivos.....	54
Etiquetar un dispositivo.....	55
Estado de cumplimiento de normas del dispositivo.....	55
Obtener la imagen de Windows Embedded Standard o ThinLinux.....	55
Solicitar un archivo de registro.....	56
Solución de problemas del dispositivo.....	57
<b>Capítulo 8: Aplicaciones y datos.....</b>	<b>58</b>
Política de la aplicación.....	59
Configurar el inventario de aplicaciones para clientes esbeltos.....	59
Configurar el inventario de aplicaciones para clientes esbeltos de Wyse Software.....	60
Crear e implementar una política de aplicaciones estándar para clientes esbeltos.....	60
Crear e implementar una política de aplicaciones estándar para clientes esbeltos.....	61
Habilitar el inicio de sesión único para Citrix StoreFront mediante la política de aplicación estándar.....	62
Crear e implementar políticas avanzadas de la aplicación en clientes esbeltos.....	62
Crear e implementar políticas avanzadas de la aplicación en clientes esbeltos de Wyse Software.....	64
Política de imagen.....	65
Agregar las imágenes del sistema operativo Windows Embedded Standard y ThinLinux al repositorio.....	65
Agregar el firmware de ThinOS al repositorio.....	66
Agregar el archivo del BIOS de ThinOS al repositorio.....	66
Agregar el archivo del paquete de ThinOS al repositorio.....	66
Agregar el firmware de ThinOS 9.x al repositorio.....	67
Agregar el archivo del paquete de ThinOS 9.x al repositorio.....	67
Crear políticas de imagen de Windows Embedded Standard y ThinLinux.....	67
Administrar el repositorio de archivos.....	68
<b>Capítulo 9: Administrar reglas.....</b>	<b>70</b>
Editar una regla de registro.....	71
Crear reglas de asignación automática para dispositivos no administrados.....	71
Editar la regla de asignación automática de un dispositivo no administrado.....	72
Deshabilitar y eliminar una regla para la asignación automática de un dispositivo no administrado.....	72
Guardar el orden de las reglas.....	72
Agregar una regla para la notificación de alertas.....	73
Editar una regla de notificación de alertas.....	73
<b>Capítulo 10: Administración de trabajos.....</b>	<b>74</b>
Sincronizar contraseña del BIOS del administrador.....	75
Buscar un trabajo programado utilizando filtros.....	76
Programar un trabajo de comandos del dispositivo.....	77
Programar la política de imágenes.....	77
Programar una política de aplicaciones.....	78
<b>Capítulo 11: Administración de eventos.....</b>	<b>79</b>
Buscar un evento o una alerta utilizando filtros.....	79
Ver el resumen de eventos.....	80
Ver el registro de la auditoría.....	80

<b>Capítulo 12: Administrar usuarios.....</b>	<b>81</b>
Agregar un nuevo perfil de administrador.....	82
Crear reglas de asignación automática para dispositivos no administrados.....	83
Editar un perfil de administrador.....	83
Agregar un usuario final.....	84
Editar un usuario final.....	84
Crear excepciones de usuario final.....	84
Importación masiva de usuarios finales.....	85
Eliminar un usuario final.....	85
Desactivar un perfil de administrador.....	85
Eliminar un perfil de administrador.....	86
Editar un perfil de usuario.....	86
Importación masiva de administradores no asignados o usuarios de Cloud Connect.....	87
<b>Capítulo 13: Administración del portal.....</b>	<b>88</b>
Cómo agregar la información del servidor de Active Directory.....	89
Configurar función de Active Directory Federation Services en nube pública.....	90
Importar usuarios no asignados o grupos de usuarios a la nube pública mediante Active Directory.....	91
Clasificaciones de alerta.....	91
Crear una interfaz de programación de aplicaciones; cuentas API.....	91
Acceder al repositorio de archivos de Wyse Management Suite.....	92
Asignación de la subred.....	93
Configurar otros ajustes.....	94
Administrar las configuraciones de Teradici.....	94
Activar la autenticación de dos factores.....	94
Activar cuentas de varios inquilinos.....	95
Generar informes.....	95
Activar una marca personalizada.....	95
Administrar la configuración del sistema.....	96
<b>Capítulo 14: Administración de dispositivos Teradici.....</b>	<b>98</b>
Detectar dispositivos Teradici.....	98
Situaciones de casos de uso de CIFS.....	100
<b>Capítulo 15: Administrar suscripción a la licencia.....</b>	<b>102</b>
Importar licencias desde la nube pública de Wyse Management Suite.....	102
Exportar licencias a la nube privada de Wyse Management Suite.....	103
Asignación de licencias de clientes delgados.....	103
Pedidos de licencias.....	104
<b>Capítulo 16: Actualización del firmware.....</b>	<b>105</b>
Actualizar ThinLinux 1.x a 2.1 y versiones posteriores.....	105
Preparar la imagen de ThinLinux 2.x.....	105
Actualizar ThinLinux 1.x a 2.x.....	106
Actualizar ThinOS 8.x a 9.0.....	107
Agregar el firmware de ThinOS al repositorio.....	107
Actualizar ThinOS 8.6 a ThinOS 9.x.....	108
Actualización de ThinOS 9.x a versiones posteriores mediante Wyse Management Suite.....	108

<b>Capítulo 17: Repositorio remoto.....</b>	<b>110</b>
Administración del servicio de repositorio de Wyse Management Suite.....	116
<b>Capítulo 18: Solución de problemas del dispositivo.....</b>	<b>117</b>
Solicitar un archivo de registro mediante Wyse Management Suite.....	117
Ver registros de auditoría mediante Wyse Management Suite.....	118
El dispositivo no se puede registrar en Wyse Management Suite cuando el proxy WinHTTP está configurado...	118
La política de redirección de USB RemoteFX no se aplica a dispositivos de almacenamiento masivo USB.....	118
<b>Capítulo 19: Preguntas frecuentes.....</b>	<b>120</b>
¿Qué tiene prioridad entre Wyse Management Suite y la interfaz del usuario de ThinOS cuando se aplica una configuración en conflicto?.....	120
¿Cómo utilizo el repositorio de archivos de Wyse Management Suite?.....	120
¿Cómo importo usuarios desde un archivo .csv?.....	121
Cómo puedo verificar la versión de Wyse Management Suite.....	121
Cómo crear y configurar etiquetas de opción de DHCP.....	122
Cómo crear y configurar registros SRV de DNS.....	123
Cómo cambiar el nombre de host a dirección IP.....	123
Cómo creo una imagen del dispositivo mediante un repositorio remoto autofirmado.....	124

Identifier	GUID-704E0126-A6A7-48E2-90F2-584324EC7604
Version	1
Status	Translation approved

## Introducción a Wyse Management Suite

Wyse Management Suite es la solución de administración de última generación que le permite configurar a nivel central, controlar, administrar y optimizar sus Thin clients Dell Wyse. También ofrece opciones de funciones avanzadas como la implementación desde la nube y en las instalaciones, la opción para administrar desde cualquier lugar usando una aplicación móvil, seguridad mejorada como la configuración del BIOS y el bloqueo de puertos. En otras funciones se incluyen la detección y el registro de dispositivos, la administración de propiedad y de inventario, la administración de configuración, la implementación de sistemas operativos y aplicaciones, comandos en tiempo real, y supervisión, alertas, presentación de informes y solución de problemas de extremos.

### Temas:

- [Ediciones de Wyse Management Suite](#)
- [Matriz de funciones de Wyse Management Suite](#)

Identifier	GUID-6F018A19-43A2-44A9-8C43-BEDC81FC08FC
Version	1
Status	Translation approved

## Ediciones de Wyse Management Suite

Wyse Management Suite se encuentra disponible en las siguientes ediciones:

- **Estándar (gratuita):** la edición estándar de Wyse Management Suite se encuentra disponible solo para una implementación in situ. No necesita una clave de licencia para usar la edición estándar. La edición estándar es apropiada para empresas pequeñas y medianas.
- **Pro (pagada):** la edición Pro de Wyse Management Suite está disponible tanto para implementación in situ como en la nube. Necesita una clave de licencia para usar la edición Pro. Ofrece una licencia por suscripción. Con la solución Pro, las organizaciones pueden adoptar un modelo híbrido y usar licencias entre el equipo en las instalaciones y la nube. La edición in situ Pro es apropiada para empresas pequeñas, medianas y de mayor tamaño. Para una implementación en la nube, la edición Pro se puede administrar en redes no corporativas (oficina en el hogar, terceros, socios, Thin clients móviles, entre otros).

**i** **NOTA: Las licencias se pueden usar fácilmente en la instalación en la nube e in situ.**

La edición Pro de Wyse Management Suite también ofrece:

- Una aplicación móvil para ver alertas críticas, notificaciones y enviar comandos en tiempo real.
- Seguridad mejorada a través de la identificación de dos factores y la autenticación de Active Directory para la administración basada en las funciones
- Política de aplicación y generación de informes avanzadas

**i** **NOTA: Los servicios en la nube se alojan en Estados Unidos y Alemania. Es posible que los clientes en países con restricciones de residencia de datos no puedan utilizar el servicio basado en la nube.**

La consola web de Wyse Management Suite admite la internacionalización. En la esquina inferior derecha de la página, en el menú desplegable, seleccione cualquiera de los siguientes idiomas:

- Inglés
- Francés
- Italiano
- Alemán
- Español
- Chino
- Japonés

# Matriz de funciones de Wyse Management Suite

En la siguiente tabla se entrega información sobre las funciones compatibles para cada tipo de suscripción:

**Tabla 1. Matriz de funciones para cada tipo de suscripción**

Características	Wyse Management Suite Standard	Wyse Management Suite Pro: nube privada	Wyse Management Suite Pro: edición en nube
Solución extremadamente escalable para administrar Thin clients	Gratuito hasta 10.000 dispositivos	50.000 dispositivos y más	1 millón de dispositivos y más
Clave de licencia	No se requiere	Obligatorio	Obligatorio
Administración basada en grupo	✓	✓	✓
Grupos de multinivel y herencia	✓	✓	✓
Administración de política de configuración	✓	✓	✓
Administración de parches e imágenes de sistema operativo	✓	✓	✓
Ver configuración efectiva a nivel del dispositivo después de la herencia	✓	✓	✓
Administración de la política de la aplicación	✓	✓	✓
Administración de propiedad, inventario y sistemas	✓	✓	✓
Detección automática de dispositivos	✓	✓	✓
Comandos en tiempo real	✓	✓	✓
Programación inteligente	✓	✓	✓
Registros de alertas, eventos y auditorías	✓	✓	✓
Comunicación segura (HTTPS)	✓	✓	✓
Administrar dispositivos detrás de firewalls	Limitado*	Limitado*	✓
Aplicación móvil	X	✓	✓
Alertas con correo electrónico y aplicación móvil	X	✓	✓
Compatibilidad con secuencia de comandos para personalizar la instalación de la aplicación	X	✓	✓
Aplicaciones en paquete para simplificar la implementación y minimizar los reinicios	X	✓	✓
Administración delegada	X	✓	✓
Creación y asignación dinámicas de grupos según los atributos del dispositivo	X	✓	✓

**Tabla 1. Matriz de funciones para cada tipo de suscripción (continuación)**

<b>Características</b>	<b>Wyse Management Suite Standard</b>	<b>Wyse Management Suite Pro: nube privada</b>	<b>Wyse Management Suite Pro: edición en nube</b>
Autenticación de dos factores	✓	✓	✓
Autenticación de Active Directory para administración basada en roles	X	✓	✓
Varios inquilinos	X	✓	✓
Informes de categoría empresarial	X	✓	✓
Varios repositorios	X	✓	✓
Activar/desactivar puertos de hardware en plataformas compatibles	X	✓	✓
Configuración del BIOS en plataformas compatibles	X	✓	✓
Configuración de la política de exportación e importación	X	✓	✓
Asignación de repositorios a la política de la aplicación	X	✓	✓
Comandos de apagado para clientes esbeltos	✓	✓	✓
Tiempo de espera de la consola de Wyse Management Suite	X	✓	✓
Orden de políticas	X	✓	✓
Selección de aplicaciones optimizada según el sistema operativo	✓	✓	✓
Opción para configurar el alias	X	✓	✓
Asignación de la subred	✓	✓	✓
Carga por lotes	X	✓	✓
Configuración de esquemas dinámicos	✓	✓	✓
Validación de la inscripción	✓	✓	✓
Seleccionar grupo para ThinOS	X	✓	✓
Repositorio de Wyse Management Suite	X	✓	✓

**NOTA:** \* El asterisco indica que puede administrar los dispositivos con Wyse Management Suite solo en un entorno de trabajo de firewall seguro. No puede administrar Thin clients más allá del alcance de la configuración del firewall.

Identificier	GUID-979C309B-CF08-433D-B985-4034CA00F5DB
Version	1
Status	Translation approved

## Introducción a Wyse Management Suite

Esta sección proporciona información sobre las funciones generales que lo ayudan a comenzar como administrador y a administrar clientes esbeltos mediante Wyse Management Suite.

### Temas:

- [Iniciar sesión en Wyse Management Suite en la nube pública](#)
- [Requisitos previos para implementar Wyse Management Suite en la nube privada](#)
- [Áreas funcionales de la consola de administración](#)
- [Configurar y administrar clientes delgados](#)
- [Wyse Device Agent](#)

Identificier	GUID-D4B86DE9-0D37-4187-A241-F18876EBBE9F
Version	2
Status	Translation in review

## Iniciar sesión en Wyse Management Suite en la nube pública

Para iniciar sesión en la consola de Wyse Management Suite, debe tener un navegador web compatible instalado en el sistema. Para iniciar sesión en la consola de Wyse Management Suite, haga lo siguiente:

1. Acceda a la edición de nube pública (SaaS) de Wyse Management Suite a través de uno de los siguientes enlaces:
  - **Centro de datos de Estados Unidos:** [us1.wysemanagementsuite.com/ccm-web](https://us1.wysemanagementsuite.com/ccm-web)
  - **Centro de datos de la Unión Europea:** [eu1.wysemanagementsuite.com/ccm-web](https://eu1.wysemanagementsuite.com/ccm-web)
2. Ingrese el nombre de usuario y la contraseña.
3. Haga clic en **Iniciar sesión**.

Si inicia sesión en la consola Wyse Management Suite por primera vez, se agrega un nuevo usuario o se renueva una licencia de usuario, aparece la página **Términos y condiciones**. Lea los términos y condiciones, seleccione las casillas de verificación correspondientes y haga clic en **Aceptar**.

**NOTA:** Recibe sus credenciales de inicio de sesión cuando se registra para la prueba de Wyse Management Suite en [www.wysemanagementsuite.com](https://www.wysemanagementsuite.com) o cuando adquiere su suscripción. Puede adquirir la suscripción de Wyse Management Suite a través del equipo de ventas de Dell o de su partner de Dell local. Para obtener más información, ingrese a [www.wysemanagementsuite.com](https://www.wysemanagementsuite.com).

**NOTA:** Debe haber un repositorio accesible de manera externa instalado en un servidor con una DMZ mientras se usa la edición Pro de Wyse Management Suite en nube pública. Además, el nombre de dominio calificado completo (FQDN) del servidor debe estar registrado en el DNS público.

## Cambiar la contraseña

Para cambiar la contraseña de inicio de sesión, haga lo siguiente:

1. Haga clic en el enlace de la cuenta en la esquina superior derecha de la consola de administración.
2. Haga clic en **Cambiar contraseña**.

**NOTA:** Se recomienda cambiar su contraseña después de iniciar sesión por primera vez. El propietario de la cuenta de Wyse Management Suite crea el nombre de usuario y la contraseña predeterminados para los administradores adicionales.

## Cierre de sesión

Para cerrar la sesión en la consola de administración, haga lo siguiente:

1. Haga clic en el enlace de la cuenta en la esquina superior derecha de la consola de administración.
2. Haga clic en **Cerrar sesión**.

Identificador	GUID-4C9EF8A1-783A-4B54-A183-08D9C00B3D70
Version	2
Status	Translation in review

## Requisitos previos para implementar Wyse Management Suite en la nube privada

Tabla 2. Requisitos previos

Descripción	10.000 dispositivos o menos	50.000 dispositivos o menos	120.000 dispositivos o menos	Repositorio de software de Wyse Management Suite
Sistema operativo	Windows Server 2012 R2, Windows Server 2016 o Windows Server 2019 Standard Paquete de idiomas compatibles: inglés, francés, italiano, alemán, español, japonés y chino (versión preliminar)			
Espacio mínimo en el disco	40 GB	120 GB	200 GB	120 GB
Memoria mínima (RAM)	8 GB	16 GB	32 GB	16 GB
Requisitos mínimos de CPU	4	4	16	4
Puertos de comunicación de red	<p>El instalador de Wyse Management Suite agrega puertos de protocolo de control de transmisión (TCP) 443, 8080 y 1883 a la lista de excepciones del firewall. Los puertos se agregan para acceder a la consola de Wyse Management Suite y enviar las notificaciones emergentes a los clientes esbeltos.</p> <ul style="list-style-type: none"> <li>• TCP 443: comunicación HTTPS</li> <li>• TCP 1883: comunicación MQTT</li> <li>• TCP 3306: MariaDB (opcional si es remoto)</li> <li>• TCP 27017: MongoDB (opcional si es remoto)</li> <li>• TCP 11211: Memcached</li> <li>• TCP 5172, 49159; Software Development Kit de administración de usuario final (EMSDK): opcional y se requiere solo para administrar los dispositivos Teradici</li> </ul> <p>Es posible que se cambien los puertos predeterminados que utiliza el instalador por uno alternativo durante la instalación.</p>			<p>El instalador del repositorio de Wyse Management Suite agrega los puertos TCP 443 y 8080 a la lista de excepciones del firewall. Los puertos se agregan para acceder a las imágenes de sistema operativo y de aplicaciones que se administran en Wyse Management Suite.</p>
Navegadores compatibles	<p>Internet Explorer versión 11</p> <p>Google Chrome versión 58.0 y posteriores</p> <p>Mozilla Firefox versión 52.0 y posteriores</p> <p>Navegador Edge en Windows: solo inglés</p>			

- Los scripts de Overlay Optimizer versión 1.0 y de instalación se proporcionan con el instalador de Wyse Management Suite. El administrador debe ejecutar los scripts para permitir que Overlay Optimizer esté disponible en Wyse Management Suite.

- Los scripts de instalación de Dell Secure Client versión 1.0 se proporcionan con el instalador de Wyse Management Suite. El administrador debe ejecutar los scripts para permitir que Dell Secure Client esté disponible en Wyse Management Suite.

**NOTA:** `WMS.exe` y `WMS_Repo.exe` se deben instalar en dos servidores diferentes. Debe instalar el repositorio remoto de Wyse Management Suite para la nube pública. En el caso de la nube privada, debe instalar el repositorio local y el repositorio remoto de Wyse Management Suite. El software se puede instalar en una máquina física o virtual. Además, no es necesario que el repositorio de software y el servidor de Wyse Management Suite tengan el mismo sistema operativo.

Identifier	GUID-9CD9EB68-BDA3-4D20-AF34-A7B10EBA4F76
Version	1
Status	Translation approved

## Áreas funcionales de la consola de administración

La consola de Wyse Management Suite se organiza en las siguientes áreas funcionales:

- En la página **Panel** se proporciona información sobre el estado actual de cada área funcional del sistema.
- En la página **Grupos y configuraciones** se emplea una administración de política de grupos jerárquica para la configuración de dispositivos. De manera opcional, se pueden crear subgrupos de la política de grupos global para categorizar dispositivos según normas corporativas. Por ejemplo, los dispositivos se pueden agrupar según la función del trabajo, el tipo de dispositivo, entre otros.
- La página **Usuarios** permite asignar a los usuarios locales y los usuarios importados de Active Directory funciones de administrador global, administrador de grupo y visualizador para iniciar sesión en Wyse Management Suite. Los usuarios reciben permisos para realizar operaciones según las funciones que se les asignan.
- En la página **Dispositivos** puede ver y administrar dispositivos, tipos de dispositivos y las configuraciones específicas de los dispositivos.
- En la página **Aplicaciones y datos** se permite la administración de aplicaciones de dispositivos, imágenes de sistema operativo, políticas, archivos de certificado, logotipos e imágenes de fondo de pantalla.
- En la página **Reglas** es posible agregar, editar y activar o desactivar reglas como la agrupación automática y las notificaciones de alerta.
- La página **Trabajos** le permite crear trabajos para tareas como el reinicio, activar en LAN y políticas de la aplicación e imagen que se deben implementar en los dispositivos registrados.
- En la página **Eventos** es posible ver y hacer auditorías en eventos y alertas del sistema.
- En la página **Administración del portal** es posible configurar varios ajustes del sistema, como la configuración del repositorio local, la suscripción de licencia, la configuración de Active Directory y la autenticación de dos factores.

Identifier	GUID-CEC2BB8B-0347-40F9-936F-9CE9B5B8ADD3
Version	1
Status	Translation approved

## Configurar y administrar clientes delgados

- **Administración de configuración:** Wyse Management Suite es compatible con una jerarquía de grupos y subgrupos. Los grupos se pueden crear manual o automáticamente según las reglas que define el administrador del sistema. Puede organizar los grupos según la jerarquía funcional; por ejemplo, marketing, ventas e ingeniería, o según la jerarquía de ubicación; por ejemplo, país/región, estado y ciudad.

**NOTA:** En la edición Pro, puede agregar reglas para crear grupos. También puede asignar dispositivos a un grupo existente según los atributos del dispositivo como la subred, la zona horaria y la ubicación.

También puede configurar lo siguiente:

- Ajustes que aplican a todos los dispositivos en la cuenta de un inquilino que se establecen en el grupo de política predeterminada. Estos ajustes son el conjunto global de parámetros que todos los grupos y subgrupos heredan. Los ajustes que están configurados en un grupo de niveles inferiores tienen prioridad sobre los ajustes que estaban configurados en grupos principales o de niveles superiores.

Por ejemplo:

- Configure las políticas según grupo de política predeterminada (grupo primario). Después de configurar las políticas, seleccione las políticas del grupo personalizado (grupo secundario). Algunos conjuntos de políticas también se aplican a los grupos secundarios. La configuración en los ajustes del grupo de políticas predeterminadas es el conjunto global de parámetros que todos los grupos y subgrupos heredan del grupo primario.
- Configure ajustes diferentes para el grupo personalizado. El grupo personalizado recibe las cargas útiles, pero los dispositivos del grupo de políticas predeterminadas no reciben la carga útil que se configura para el grupo de políticas personalizadas.

- Configure ajustes diferentes para el grupo personalizado. Los ajustes que están configurados en un grupo de niveles inferiores tienen prioridad sobre los ajustes que estaban configurados en grupos principales o de niveles superiores.
- Los ajustes específicos de un dispositivo en particular se pueden configurar desde la página **Detalles del dispositivo**. Estas configuraciones, como los grupos de niveles inferiores, tienen prioridad sobre los ajustes que se configuran en los grupos de niveles superiores.

Cuando crea y publica la política, los parámetros de configuración se implementan en todos los dispositivos en ese grupo, incluidos los subgrupos.

Después de publicar y propagar una política en los dispositivos, las configuraciones no se envían nuevamente a los dispositivos hasta que haga algún cambio. Los nuevos dispositivos que se registran reciben la política de configuración que está en efecto para el grupo en el que se registró. Esto incluye los parámetros que se heredan del grupo global y de grupos de nivel intermedio.

Las políticas de configuración se publican de inmediato y no se pueden programar para más tarde. Algunos cambios de la política, por ejemplo, los ajustes de pantalla, pueden requerir un reinicio.

- **Implementación de la imagen de la aplicación y del sistema operativo:** las actualizaciones de imagen de aplicaciones y de sistemas operativos se pueden implementar desde la pestaña **Aplicaciones y datos**. Las aplicaciones se implementan según los grupos de políticas.

**NOTA:** La política de la aplicación avanzada le permite implementar una aplicación en todos los grupos, incluso los actuales, según sus requisitos. Las imágenes de sistema operativo se pueden implementar solo en el grupo actual.

Wyse Management Suite es compatible con políticas de la aplicación estándar y avanzadas. Una política de aplicación estándar le permite instalar un paquete único de aplicación. El dispositivo se reiniciará durante la instalación de una aplicación. Reinicie el dispositivo antes y después de la instalación de cada aplicación. Con una política de aplicación avanzada, los paquetes de aplicación múltiples se pueden instalar con solo dos reinicios. Esta función está disponible solo en la edición Pro. Las políticas avanzadas de las aplicaciones también son compatibles con la ejecución de los scripts previos y posteriores a la instalación tal vez se necesiten para instalar una aplicación específica.

Puede configurar políticas de aplicaciones estándar y avanzadas para aplicarlas automáticamente cuando el dispositivo está registrado con Wyse Management Suite o cuando un dispositivo se mueve a un grupo nuevo.

La implementación de políticas de aplicaciones y de imágenes de sistema operativo en Thin clients se puede programar de inmediato o posteriormente según la zona horaria del dispositivo o cualquier otra zona horaria especificada.

- **Inventario de dispositivos:** esta opción se puede ubicar haciendo clic en la pestaña **Dispositivos**. De manera predeterminada, la opción muestra una lista paginada de todos los dispositivos en el sistema. Puede optar por ver un subconjunto de dispositivos usando varios criterios de filtro, como grupos o subgrupos, tipo de dispositivo, tipo de sistema operativo, estado, subred y plataforma o zona horaria.

Para ir a la página **Detalles del dispositivo** de ese dispositivo, haga clic en la entrada del dispositivo que se detalla en esta página. Se muestran todos los detalles del dispositivo.

La página **Detalles del dispositivo** también muestra todos los parámetros de configuración que se aplican a ese dispositivo y también el nivel de grupo en el que se aplica cada parámetro.

Esta página también permite establecer parámetros de configuración que son específicos de ese dispositivo mediante la activación del botón **Excepciones de dispositivo**. Los parámetros que se configuran en esta sección anulan cualquier parámetro que se haya configurado en los grupos o a nivel global.

- **Informes:** puede generar y ver informes según los filtros predefinidos. Para generar informes, haga clic en la pestaña **Informes** en la página **Administración del portal**.
- **Aplicación móvil:** puede recibir notificaciones de alerta y administrar dispositivos usando la aplicación móvil **Dell Mobile Agent** disponible para los dispositivos Android. Para descargar la aplicación móvil y la **Guía de inicio de Dell Mobile Agent**, haga clic en la pestaña **Alertas y clasificación** en la página **Administrador del portal**.

Identificador	GUID-2AB47C8C-2E5B-40E8-8E95-E584540F2265
Version	1
Status	Translation approved

## Wyse Device Agent

Wyse Device Agent (WDA) es un agente unificado para todas las soluciones de administración de cliente esbelto. Si instala WDA, puede administrar los clientes esbeltos con Wyse Management Suite.

Wyse Device Agent admite los siguientes tres tipos de entornos de seguridad del cliente:

- **Entornos altamente seguros:** para mitigar el riesgo de un servidor DHCP o DNS no autorizado en la detección de nuevos dispositivos, los administradores deben iniciar sesión en cada dispositivo de manera individual y configurar la URL del servidor de Wyse Management Suite. Puede utilizar certificados firmados por CA o autofirmados. Sin embargo, Dell recomienda utilizar un certificado firmado por CA. En la solución de nube privada de Wyse Management Suite con certificado autofirmado, el certificado se debe

configurar de forma manual en cada dispositivo. Además, el certificado se debe copiar en la carpeta `Agent Configuration` para preservar el certificado y mitigar el riesgo de servidores DHCP o DNS no autorizados, incluso después de volver a crear la imagen del dispositivo.

La carpeta `Agent Configuration` está disponible en la siguiente ubicación:

- o Dispositivos Windows Embedded Standard: `%SYSTEMDRIVE%\Wyse\WCM\ConfigMgmt\Certificates`
- o Dispositivos ThinLinux: `/etc/addons.d/WDA/certs`
- o Dispositivos ThinOS: `wnos/cacerts/`



**NOTA: Debe importar el certificado a un cliente esbelto que ejecute el sistema operativo ThinOS mediante una unidad USB o rutas FTP.**

- **Entornos seguros:** para mitigar el riesgo de un servidor DHCP o DNS no autorizado en la detección de nuevos dispositivos, los administradores deben configurar el servidor de Wyse Management Suite mediante certificados firmados por CA. El dispositivo puede obtener la URL del servidor de Wyse Management Suite de los registros de DHCP/DNS y realizar la validación de CA. La solución de nube privada de Wyse Management Suite con certificado autofirmado requiere que el certificado se envíe al dispositivo después del primer registro si el dispositivo no tiene el certificado antes del registro. Este certificado se conserva incluso después de volver a crear una imagen o reiniciar el dispositivo para mitigar el riesgo de un servidor DHCP o DNS no autorizado.
- **Entornos normales:** el dispositivo obtiene la URL del servidor de Wyse Management Suite de los registros de DHCP/DNS para la nube privada de Wyse Management Suite que está configurada con un certificado autofirmado o firmado por CA. Si la opción de validación de CA está desactivada en el dispositivo, se notifica al administrador de Wyse Management Suite después de registrar el dispositivo por primera vez. En este escenario, Dell recomienda que los administradores envíen el certificado al dispositivo en el que el servidor está configurado con un certificado autofirmado. Este entorno no está disponible para la nube pública.

Identifíer	GUID-C73B0488-EA87-42B7-91E6-99C3B0311AF4
Version	1
Status	Translation approved

## Instalar o actualizar Wyse Device Agent

Esta sección proporciona información sobre cómo instalar o actualizar Wyse Device Agent en los clientes esbeltos, como dispositivos Windows Embedded Standard, Linux y ThinLinux, mediante Wyse Management Suite.

- **Dispositivos Windows Embedded:** Wyse Device Agent versión 1.4.x se puede descargar desde [support.dell.com](https://support.dell.com). Puede instalar o actualizar Wyse Device Agent en dispositivos Windows Embedded Standard mediante cualquier de los siguientes métodos:
  - [Instalar Wyse Device Agent manualmente](#)
  - [Actualizar Wyse Device Agent mediante la política de la aplicación de Wyse Management Suite](#)

**NOTA:** También puede actualizar manualmente Wyse Device Agent haciendo doble clic en el archivo .exe de Wyse Device Agent.

**NOTA:** Wyse Device Agent se puede instalar en el sistema operativo Windows Embedded Standard 7 solo si KB3033929 está disponible.

- **Dispositivos Linux y ThinLinux:** Wyse Device Agent se puede instalar o actualizar en dispositivos Linux y ThinLinux mediante Wyse Management Suite. Para obtener más información, consulte [Instalar o actualizar Wyse Device Agents en clientes ThinLinux o Linux](#).

### Temas:

- [Instalar Wyse Device Agent manualmente en un dispositivo Windows Embedded](#)
- [Actualizar Wyse Device Agent mediante la política de la aplicación de Wyse Management Suite](#)
- [Instalar o actualizar Wyse Device Agents en clientes ThinLinux o Linux](#)

Identifíer	GUID-A38C59C1-07BF-4BEE-AF9A-BD3DA3F98FA3
Version	3
Status	Translation in review

## Instalar Wyse Device Agent manualmente en un dispositivo Windows Embedded

### Pasos

1. Copie el archivo WDA.exe al Thin client.
2. Haga doble clic en el archivo WDA.exe.
3. Haga clic en **Sí**.

**NOTA:** Se muestra un mensaje de aviso cuando hay una versión anterior de Wyse Device Agent o HAgent está instalada en el dispositivo.

4. En el campo **Token de grupo**, ingrese un token de grupo. Este campo es opcional. Para omitir este paso, haga clic en **Siguiente**. Puede ingresar los detalles del token de grupo posteriormente en la interfaz de usuario de Wyse Device Agent.
5. En la lista desplegable **Región**, seleccione la región del servidor de nube pública Wyse Management Suite. Después de instalar correctamente, el servidor de nube pública Wyse Management Suite registra automáticamente el dispositivo en la consola de Wyse Management Suite.

Identifíer	GUID-5BFD09F9-A29A-4E36-8C96-81EDC900D537
Version	4
Status	Translation approved

## Actualizar Wyse Device Agent mediante la política de la aplicación de Wyse Management Suite

### Requisitos previos

Se recomienda usar la aplicación Wyse Management Suite para actualizar Wyse Device Agent. En la configuración de la nube privada de Wyse Management Suite, los paquetes más recientes de Wyse Device Agent para Windows Embedded Standard están disponibles en el repositorio local. Si está usando una nube pública o un repositorio remoto en una nube privada, copie el archivo `WDA.exe` a la carpeta `thinClientApps` en el repositorio.

### Pasos

- Después de copiar el archivo `WDA.exe` en el repositorio, vaya a **Aplicaciones y datos** y cree una política de aplicación estándar con este paquete; consulte [Crear e implementar una política de aplicaciones estándar para clientes esbeltos](#).

**NOTA:** La política de aplicación avanzada es compatible solo desde la versión 14.x de Wyse Device Agent en adelante. Se recomienda que use la política de aplicación estándar para actualizar Wyse Device Agent desde la versión 14.x. También puede usar la política de aplicación avanzada para actualizar Wyse Device Agent desde la versión 14.x en adelante.

- Vaya a la página **Trabajos** y programe un trabajo para actualizar Wyse Device Agent.

**NOTA:** Para actualizar Wyse Device Agent de Windows Embedded Standard desde la versión 13.x a la versión 14.x, se recomienda usar HTTP como protocolo del repositorio.

Después de una instalación correcta, el estado se envía al servidor.

Identifíer	GUID-EBEA716B-1C0A-4327-8A11-DF836C5ADC78
Version	4
Status	Translation approved

## Instalar o actualizar Wyse Device Agents en clientes ThinLinux o Linux

### Requisitos previos

- Para instalar Wyse Device Agents en clientes esbeltos Dell Wyse 3040 con ThinLinux versión 2.0, versión de imagen 2.0.14 y Wyse Device Agent versión 3.0.7, debe instalar el archivo `wda3040_3.0.10-01_amd64.deb` y luego instalar el archivo `wda_3.2.12-01_amd64.tar`.
- Debe instalar el complemento de la utilidad de la plataforma y el complemento de Wyse Device Agent para clientes esbeltos Linux. Puede instalar el archivo `wda_x.x.x.tar` para clientes delgados ThinLinux.

### Sobre esta tarea

Puede instalar o actualizar complementos por medio de cualquiera de las siguientes opciones:

- Usando parámetros INI
- Administrador de complementos
- Comandos de RPM

### Pasos

- Si está usando una nube pública o un repositorio remoto en una nube privada, copie los archivos RPM a la carpeta `thinClientApps` en el repositorio. De manera predeterminada, los Wyse Device Agents más recientes y los RPM de la utilidad de la plataforma para clientes Linux y ThinLinux están disponibles en el repositorio local.
- Vaya a la página **Trabajos** y programe un trabajo para actualizar el complemento de la utilidad de la plataforma. Debe esperar a que el complemento de utilidad de la plataforma se instale correctamente en su Thin client.

**i** **NOTA:** Instale primero un complemento de utilidad de la plataforma y luego instale un complemento de Wyse Device Agent. No se pueden instalar los Wyse Device Agents más recientes antes de instalar el complemento de utilidad de la plataforma más reciente.

3. En la página **Trabajos**, programe un trabajo para actualizar Wyse Device Agent en el cliente.

**i** **NOTA:** El cliente Linux se reinicia después de instalar el complemento de Wyse Device Agent versión 2.0.11.

Identifíer	GUID-93F67936-A986-46EF-B19F-952B87D6087C
Version	1
Status	Translation approved

## Registrar y configurar un nuevo dispositivo mediante Wyse Management Suite

### Temas:

- Registrar y configurar un nuevo dispositivo Windows Embedded Standard mediante Wyse Management Suite
- Registrar y configurar un nuevo dispositivo ThinOS 8.x mediante Wyse Management Suite
- Registrar y configurar un nuevo dispositivo ThinOS 9.x mediante Wyse Management Suite
- Registrar y configurar un nuevo dispositivo Linux o ThinLinux mediante Wyse Management Suite
- Registrar y configurar un nuevo cliente esbelto de Wyse Software mediante Wyse Management Suite

Identifíer	GUID-3697A14F-3884-4781-B12C-BDC9AD63C93E
Version	1
Status	Translation approved

## Registrar y configurar un nuevo dispositivo Windows Embedded Standard mediante Wyse Management Suite

### Pasos

1. Instalar Wyse Device Agent en el cliente esbelto; consulte [Instalar o actualizar Wyse Device Agent](#).
2. Registrar el cliente esbelto en Wyse Management Suite; consulte [Registrar clientes esbeltos de Windows Embedded Standard en Wyse Management Suite mediante Wyse Device Agent](#).



**NOTA:** También puede registrar los dispositivos mediante cualquiera de los siguientes métodos:

- Con etiquetas de opciones de DHCP; consulte [Registrar dispositivos mediante etiquetas de opciones de DHCP](#).
- Mediante el registro SRV de DNS; consulte [Registrar dispositivos mediante el registro SRV de DNS](#).





**NOTA:** Cuando la opción Validación de la inscripción está activada, los dispositivos detectados manual o automáticamente se encuentran en estado de Validación de inscripción pendiente en la página Dispositivos. El usuario puede seleccionar un solo dispositivo o varios dispositivos en la página Dispositivos y validar la inscripción. Los dispositivos se mueven al grupo deseado después de que se validan. Para obtener más información sobre cómo validar los dispositivos, consulte [Validación de la inscripción](#).

3. Agregue el dispositivo al grupo que desea (opcional); consulte [Administración de grupos y configuraciones](#).
4. Configure el cliente esbelto mediante cualquiera de las siguientes opciones:
  - En la página **Grupos y configuraciones**; consulte [Editar la configuración de la política de Windows Embedded Standard](#).
  - En la **página Dispositivos**; consulte [Administración de dispositivos](#).

Identifíer	GUID-C6FDE6C7-04C2-41D3-B1E0-81AC8252EF35
Version	1
Status	Translation approved

# Registrar y configurar un nuevo dispositivo ThinOS 8.x mediante Wyse Management Suite

## Pasos

1. Desde el menú del escritorio del cliente esbelto, vaya a **Configuración del sistema** > **Configuración central**. Aparecerá la ventana **Configuración central**.
  2. Ingrese la **Clave de registro del grupo** según lo que configuró el administrador para el grupo deseado.
  3. Seleccione la casilla de verificación **Habilitar configuración avanzada de WMS**.
  4. En el campo **Servidor WMS**, ingrese la URL de Wyse Management Server.
  5. Active o desactive la validación de CA según su tipo de licencia. Para la nube pública, seleccione la casilla de verificación **Activar validación de CA**. Para la nube privada, seleccione la casilla de verificación **Activar validación de CA** si importó certificados desde una autoridad de certificación reconocida hacia el servidor de Wyse Management Suite.  
  
Para activar la opción de validación de CA en la nube privada, también debe instalar el mismo certificado autofirmado en el dispositivo de ThinOS. Si no ha instalado el certificado autofirmado en el dispositivo ThinOS, no seleccione la casilla de verificación **Activar validación de CA**. Puede instalar el certificado en el dispositivo utilizando Wyse Management Suite después de registrarse y luego activar la opción de validación de CA.
  6. Para verificar la configuración, haga clic en **Validar clave**.  
 **NOTA:** Si la clave no se valida, verifique la clave de grupo y el URL del servidor WMS que proporcionó. Asegúrese de que los puertos mencionados no estén bloqueados por la red. Los puertos predeterminados son 443 y 1883.
  7. Haga clic en **Aceptar**.  
 **NOTA:** Cuando la opción **Validación de la inscripción** está activada, los dispositivos detectados manual o automáticamente se encuentran en estado de **Validación de inscripción pendiente** en la página **Dispositivos**. El usuario puede seleccionar un solo dispositivo o varios dispositivos en la página **Dispositivos** y validar la inscripción. Los dispositivos se mueven al grupo deseado después de que se validan. Para obtener más información sobre cómo validar los dispositivos, consulte [Validación de la inscripción](#).
- El dispositivo está registrado en Wyse Management Suite.
8. Inicie sesión en Wyse Management Suite.
  9. Agregue el dispositivo al grupo que desea (opcional): consulte [Administración de grupos y configuraciones](#).
  10. Configure el cliente esbelto mediante cualquiera de las siguientes opciones:
    - En la página **Grupos y configuraciones**; consulte [Editar la configuración de la política de ThinOS](#).
    - En la **página Dispositivos**; consulte [Administración de dispositivos](#).

Identifíer	GUID-BF833AD8-5BE7-4133-92D9-ADB4435A5717
Version	1
Status	Translation approved

# Registrar y configurar un nuevo dispositivo ThinOS 9.x mediante Wyse Management Suite

## Pasos

1. Desde el menú del escritorio del cliente esbelto, vaya a **Configuración del sistema** > **Configuración central**. Aparecerá la ventana **Configuración central**.
2. Ingrese la **Clave de registro del grupo** según lo que configuró el administrador para el grupo deseado.
3. Seleccione la casilla de verificación **Habilitar configuración avanzada de WMS**.
4. En el campo **Servidor WMS**, ingrese la URL de Wyse Management Server.

5. Active o desactive la validación de CA según su tipo de licencia. Para la nube pública, marque la casilla de verificación **Activar validación de CA** y, para la nube privada, marque la casilla de verificación **Activar validación de CA** si importó certificados de una autoridad de certificación reconocida al servidor la Wyse Management Suite.

Para activar la opción de validación de CA en la nube privada, también debe instalar el mismo certificado autofirmado en el dispositivo de ThinOS. Si no ha instalado el certificado autofirmado en el dispositivo ThinOS, no seleccione la casilla de verificación **Activar validación de CA**. Puede instalar el certificado en el dispositivo utilizando Wyse Management Suite después de registrarse y luego activar la opción de validación de CA.

6. Para verificar la configuración, haga clic en **Validar clave**.

**NOTA:** Si la clave no se valida, verifique la clave de grupo y el URL del servidor WMS que proporcionó. Asegúrese de que los puertos mencionados no estén bloqueados por la red. Los puertos predeterminados son 443 y 1883.

Se muestra una ventana de alerta.

7. Haga clic en **Aceptar**.

8. Haga clic en **OK** en la ventana **Configuración central**.

**NOTA:** También puede registrar los dispositivos mediante cualquiera de los siguientes métodos:

- Con etiquetas de opciones de DHCP; consulte [Registrar dispositivos mediante etiquetas de opciones de DHCP](#).
- Mediante el registro SRV de DNS; consulte [Registrar dispositivos mediante el registro SRV de DNS](#).

**NOTA:** Cuando la opción Validación de la inscripción está activada, los dispositivos detectados manual o automáticamente se encuentran en estado de Validación de inscripción pendiente en la página Dispositivos. El usuario puede seleccionar un solo dispositivo o varios dispositivos en la página Dispositivos y validar la inscripción. Los dispositivos se mueven al grupo deseado después de que se validan. Para obtener más información sobre cómo validar los dispositivos, consulte [Validación de la inscripción](#).

El dispositivo está registrado en Wyse Management Suite.

9. Inicie sesión en Wyse Management Suite.

10. Agregue el dispositivo al grupo que desea (opcional): consulte [Administración de grupos y configuraciones](#).

11. Configure el cliente esbelto mediante cualquiera de las siguientes opciones:

- En la página **Grupos y configuraciones**; consulte [Editar la configuración de la política de ThinOS 9.x](#).
- En la **página Dispositivos**; consulte [Administración de dispositivos](#).

Identifier	GUID-C2E18382-6533-4C7D-8F3E-FCB9FFD98E70
Version	1
Status	Translation approved

## Registrar y configurar un nuevo dispositivo Linux o ThinLinux mediante Wyse Management Suite

### Pasos

1. Instalar Wyse Device Agent en el cliente esbelto; consulte [Instalar o actualizar Wyse Device Agent](#).
2. Registrar el cliente esbelto en Wyse Management Suite: consulte [Registrar clientes esbeltos de Linux/ThinLinux en Wyse Management Suite mediante Wyse Device Agent](#).

**NOTA:** También puede registrar los dispositivos mediante cualquiera de los siguientes métodos:

- Con etiquetas de opciones de DHCP; consulte [Registrar dispositivos mediante etiquetas de opciones de DHCP](#).
- Mediante el registro SRV de DNS; consulte [Registrar dispositivos mediante el registro SRV de DNS](#).

**NOTA:** Cuando la opción Validación de la inscripción está activada, los dispositivos detectados manual o automáticamente se encuentran en estado de Validación de inscripción pendiente en la página Dispositivos. El usuario puede seleccionar un solo dispositivo o varios dispositivos en la página Dispositivos y validar la inscripción. Los dispositivos se mueven al grupo deseado después de que se validan. Para obtener más información sobre cómo validar los dispositivos, consulte [Validación de la inscripción](#).

3. Agregue el dispositivo al grupo que desea (opcional): consulte [Administración de grupos y configuraciones](#).

4. Configure el cliente esbelto mediante cualquiera de las siguientes opciones:

- En la página **Grupos y configuraciones**; consulte [Editar la configuración de la política de ThinLinux](#) o [Editar la configuración de la política de Linux](#).
- En la **página Dispositivos**; consulte [Administración de dispositivos](#).

Identifier	GUID-4C730068-F549-49BE-ADF4-F260FCF8302A
Version	1
Status	Translation approved

# Registrar y configurar un nuevo cliente esbelto de Wyse Software mediante Wyse Management Suite

## Pasos

1. Instalar Wyse Device Agent en el cliente esbelto; consulte [Instalar o actualizar Wyse Device Agent](#).
2. Registrar el cliente esbelto en Wyse Management Suite; consulte [Registrar clientes esbeltos de Wyse Software en Wyse Management Suite mediante Wyse Device Agent](#).

**NOTA:** También puede registrar los dispositivos mediante cualquiera de los siguientes métodos:

- Con etiquetas de opciones de DHCP; consulte [Registrar dispositivos mediante etiquetas de opciones de DHCP](#).
- Mediante el registro SRV de DNS; consulte [Registrar dispositivos mediante el registro SRV de DNS](#).

**NOTA:** Cuando la opción Validación de la inscripción está activada, los dispositivos detectados manual o automáticamente se encuentran en estado de Validación de inscripción pendiente en la página Dispositivos. El usuario puede seleccionar un solo dispositivo o varios dispositivos en la página Dispositivos y validar la inscripción. Los dispositivos se mueven al grupo deseado después de que se validan. Para obtener más información sobre cómo validar los dispositivos, consulte [Validación de la inscripción](#).

3. Agregue el dispositivo al grupo que desea (opcional); consulte [Administración de grupos y configuraciones](#).
4. Configure el cliente esbelto mediante cualquiera de las siguientes opciones:
  - En la página **Grupos y configuraciones**; consulte [Editar la configuración de la política de clientes esbeltos de Wyse Software](#).
  - En la **página Dispositivos**; consulte [Administración de dispositivos](#).

Identifier	GUID-0D124429-9F2A-41B0-AAA4-01D36ECCC4F9
Version	1
Status	Translation approved

## Panel de Wyse Management Suite

En la página **Panel** puede ver el estado de un sistema y las tareas recientes que se realizan dentro del sistema. Para ver una alerta específica, haga clic en el enlace en la sección **Alertas**. La página **Panel** también le permite ver el resumen del dispositivo.

The screenshot displays the Wyse Management Suite interface. At the top, there is a navigation bar with the Dell logo and the text 'Wyse Management Suite'. Below the navigation bar, there are several sections:

- Alerts:** Shows 0 alerts. There are three sub-sections: 'Devices Not Checked In' (0), 'App Compliance' (0), and 'Other Device Alerts' (0). A 'View All Alerts' link is present.
- Enrollment Validation:** Shows 'On'.
- Devices:** Shows 0 devices. A 'View All' link is present.
- Events:** Shows 'No Events'. A 'View All Events' link is present.
- Summary:** Shows 'No Devices By Categories'. A legend indicates the following counts: Compliant (0), Pending (0), Unmanaged (0), Non-Compliant (0), and Enrollment Pending (0).
- Bottom Summary:** Shows 'No device added in last 30 days'.

Ilustración 1. Panel

### Temas:

- [Ver alertas](#)
- [Ver la lista de eventos](#)
- [Ver el estado del dispositivo](#)
- [Activar la validación de certificados](#)
- [Cambiar preferencias de usuario](#)
- [Acceder a ayuda en línea](#)
- [Cambiar la contraseña](#)
- [Cerrar sesión desde la consola de administración](#)

Identifier	GUID-16E7CF66-D5C0-4D9A-9C1E-DA626895048D
Version	1
Status	Translation approved

## Ver alertas

La sección de **Alertas** muestra el resumen de todas las alertas.

## Pasos

1. Haga clic en **Tablero**.  
Se muestra el resumen de alertas.
2. Haga clic en **Ver todas las alertas**.  
Se muestran los siguientes atributos en la página **Eventos**:
  - **Dispositivos no registrados**
  - **Cumplimiento de la aplicación**
  - **Otras alertas del dispositivo**

Identifier	GUID-957F4AFA-7599-4954-BB4E-640085258241
Version	1
Status	Translation approved

## Ver la lista de eventos

La sección **Eventos** muestra el resumen de los eventos que han ocurrido en los últimos días.

## Pasos

1. Haga clic en **Tablero**.  
Aparece el resumen de eventos.
2. Haga clic en **Ver todos los eventos**.  
Aparece la página **Eventos** con una lista de todos los eventos.

Identifier	GUID-F115FDE3-94D3-4BDA-BA06-FE7629ECE2AF
Version	1
Status	Translation approved

## Ver el estado del dispositivo

La sección **Pantalla** proporciona el resumen del estado del dispositivo.

## Pasos

1. Haga clic en **Tablero**.  
Se muestra el resumen de dispositivos.
2. Haga clic en **Ver todos**.  
Aparece la página **Dispositivos** con una lista de todos los dispositivos registrados. La sección **Resumen** muestra el recuento de dispositivos según las siguientes categorías de estado del dispositivo:
  - **Conforme**
  - **Pendiente**
  - **Sin administrar**
  - **No conforme**
  - **Inscripción pendiente**

Identifier	GUID-4C455A93-75DE-4F3F-8F94-CA47D419F0B5
Version	1
Status	Translation approved

## Activar la validación de certificados

Puede habilitar la **Validación de la inscripción** para permitir que los administradores controlen el registro manual y automático de los clientes esbeltos en un grupo.

## Pasos

1. Haga clic en **Tablero**.
2. Haga clic en el botón **ACTIVAR/DESACTIVAR** junto a la opción **Validación de la inscripción**.  
Es redirigido a la opción **Otras configuraciones** en la página **Administración del portal**.
3. Active o desactive la opción **Validación de la inscripción**.

Identifíer	GUID-33F6F7DA-92D4-44C6-BF29-688C0310654A
Version	1
Status	Translation approved

## Cambiar preferencias de usuario

Puede cambiar las preferencias de usuario, como la notificación de alertas, la configuración de políticas y el tamaño de la página.

### Pasos

1. En la esquina superior derecha de la página **Tablero**, haga clic en el menú desplegable de inicio de sesión.
2. Haga clic en **Preferencias del usuario**.  
Aparece la ventana **Preferencias del usuario**.
3. Haga clic en **Alertas** y seleccione las casillas de verificación correspondientes para asignar un tipo de alerta, Crítico, Advertencia o Aviso, para las notificaciones de sus correos electrónicos y aplicaciones móviles.
4. Haga clic en **Políticas** y seleccione la casilla de verificación **Pregúnteme si deseo utilizar el modo de asistente ThinOS** para ver la ventana **Seleccionar modo de configuración de ThinOS** cada vez que configure los ajustes de política de ThinOS.
5. Haga clic en **Tamaño de página** e ingrese un número entre 10 a 100 en el cuadro de texto **Número de elementos por página**. Esta opción permite configurar la cantidad de elementos que se muestran en cada página.

Identifíer	GUID-AA80F2E8-9CC5-48FE-8468-D141E7996E6F
Version	1
Status	Translation approved

## Acceder a ayuda en línea

### Pasos

1. En la esquina superior derecha de la página **Tablero**, haga clic en el menú desplegable de inicio de sesión.
2. Haga clic en **Ayuda de WMS**.  
Aparece la página **Compatibilidad para Wyse Management Suite**.

Identifíer	GUID-B47AF88F-2EED-4997-B0E6-48183ADC921B
Version	1
Status	Translation approved

## Cambiar la contraseña

### Pasos

1. En la esquina superior derecha de la página **Tablero**, haga clic en el menú desplegable de inicio de sesión.
2. Haga clic en **Cambiar contraseña**.  
Se abrirá la ventana **Cambiar contraseña**.
3. Ingrese la contraseña actual.
4. Introduzca la contraseña nueva.
5. Vuelva a ingresar la nueva contraseña para confirmar.
6. Haga clic en **Cambiar contraseña**.

Identifíer	GUID-1E2136F7-767E-494E-B55C-038CE296507E
Version	1
Status	Translation approved

## Cerrar sesión desde la consola de administración

### Pasos

1. En la esquina superior derecha de la página **Tablero**, haga clic en el menú desplegable de inicio de sesión.
2. Haga clic en **Cerrar sesión**.

Identifíer	GUID-42A135B1-223F-4285-9492-56CC92DDB127
Version	4
Status	Translation in review

## Administrar grupos y configuraciones

En la página **Grupos y configuraciones**, puede definir las políticas necesarias para configurar sus dispositivos. Puede crear subgrupos de las políticas de grupos globales y categorizar dispositivos según sus requisitos. Por ejemplo, los dispositivos se pueden agrupar según las funciones del trabajo, el tipo de dispositivo, entre otros.

En cada grupo, puede definir las políticas de los siguientes tipos de sistemas operativos:

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

Los dispositivos heredan políticas según el orden en que son creadas. La configuración que se ajusta en un grupo de política predeterminada se aplica como configuración predeterminada en todas las políticas detalladas en el grupo de políticas predeterminadas. En un grupo, todos los dispositivos de ese grupo tienen un grupo de políticas predeterminadas como configuración predeterminada.

En la página **Detalles del dispositivo**, puede crear una excepción para un dispositivo en el grupo para tener un subconjunto de políticas que son diferentes de las políticas predeterminadas del grupo.

En la página se muestra la configuración para una propiedad particular con detalles de dónde está establecida la configuración (nivel global, de grupo o de dispositivo). La opción para crear excepciones está disponible en la página. La configuración de **Excepción** se aplica solo para esos dispositivos seleccionados.

### **NOTA:**

**Cuando modifica las políticas de niveles inferiores, aparece un símbolo de viñeta al lado de la política. Este símbolo indica que la política es una anulación de una política de nivel superior. Por ejemplo, personalización del sistema, red, seguridad, entre otros. Cuando modifica políticas, se muestra un asterisco (\*) al lado de la política. Este símbolo indica que hay cambios sin guardar y sin publicar. Para revisar estos cambios antes de publicarlos, haga clic en el enlace Ver cambios pendientes.**

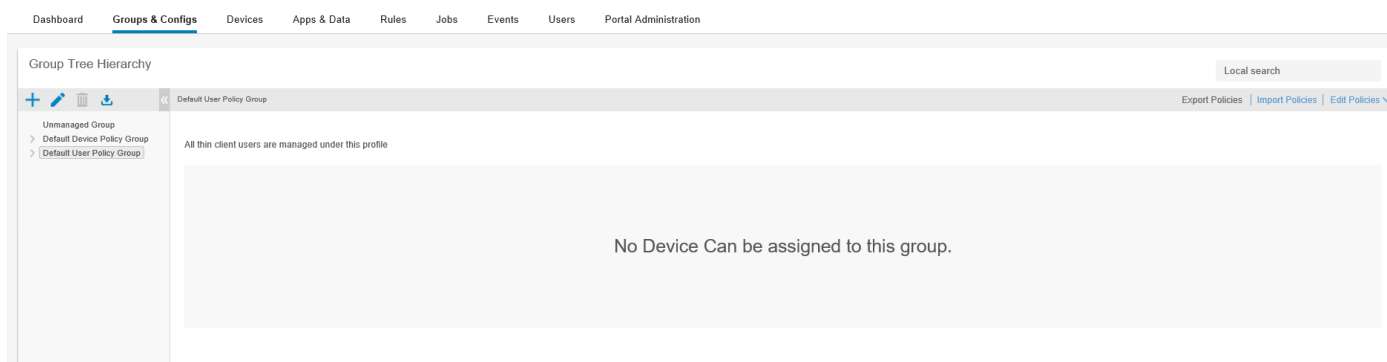
Si una configuración de política se debe priorizar entre diferentes niveles, la política de menor nivel tiene la preferencia.

Después de configurar los ajustes de política, se notifica a los Thin clients de los cambios. Los cambios se aplican inmediatamente después de configurar los Thin clients.

### **NOTA:** Ciertas configuraciones, como la configuración del BIOS para Windows Embedded Standard, requieren un reinicio para que los cambios se apliquen. Sin embargo, para la mayoría de las configuraciones en ThinOS, debe reiniciar el dispositivo para que se apliquen los cambios.

Las políticas se aplican con la siguiente prioridad:

- Global
- Grupo
- Dispositivo



**Ilustración 2. Grupos y configuraciones**

**Temas:**


- Editar un grupo sin administrar
- Crear un grupo de políticas de dispositivo predeterminado
- Eliminar un grupo de selección de ThinOS
- Configurar una política de nivel global
- Crear un grupo de políticas de usuario
- Editar un grupo de políticas de usuario
- Importar un grupo de políticas de usuario
- Importar un grupo de políticas de grupo desde Active Directory
- Eliminar un grupo
- Configurar una política del nivel del dispositivo
- Exportar políticas de grupos
- Importar políticas de grupos
- Editar la configuración de la política de ThinOS
- Editar la configuración de la política de ThinOS 9.x
- Editar la configuración de la política de Windows Embedded Standard
- Editar la configuración de la política de Linux
- Editar la configuración de la política de ThinLinux
- Editar la configuración de la política de Wyse Software Thin Client
- Editar la configuración de la política de Cloud Connect

Identifier	GUID-FFC489B7-6F43-4A6D-B722-5A1CAEE9F021
Version	2
Status	Translation approved

## Editar un grupo sin administrar

Los dispositivos que pertenecen al grupo no administrado no usan licencias ni reciben configuración o políticas según la aplicación. Para agregar dispositivos a un grupo no administrado, use una clave de registro del dispositivo del grupo no administrado como parte de un registro automático o un registro manual de dispositivo.

**Pasos**

1. En la página **Grupos y configuraciones**, seleccione **Grupo no administrado**.
2. Haga clic en . Se muestra la página **Editar grupo no administrado**. En el **Nombre de grupo**, se muestra el nombre del grupo.
3. Edite los siguientes detalles:
  - **Descripción:** se muestra una breve descripción del grupo.
  - **Token de grupo:** seleccione esta opción para activar el token de grupo.
4. Haga clic en **Guardar**.

**NOTA:** Para una nube pública, el token de grupo para un grupo no administrado se debe activar para registrar los dispositivos. Para una nube privada, el token de grupo para un grupo no administrado se activa automáticamente.

Identifíer	GUID-67B60182-B167-4A00-BA8F-C2585E4D47AE
Version	3
Status	Translation in review

# Crear un grupo de políticas de dispositivo predeterminado

Puede crear grupos para las políticas de grupos de dispositivos globales y categorizar los dispositivos según sus requisitos.

## Pasos

1. En la página **Grupos y configuraciones**, haga clic en la opción **Grupo de políticas de grupo predeterminadas**.
2. Haga clic en **+**.
3. En el cuadro de diálogo **Agregar nuevos grupos**, ingrese el **Nombre del grupo**, la **Descripción**, el **Dominio** y el **Nombre de atributo de AD**.

**NOTA:** Seleccione la opción **Este es un elemento primario del grupo de selección de ThinOS** para crear un grupo de selección primario para los dispositivos ThinOS. Para obtener más información, consulte [Crear un grupo de selección de ThinOS](#).

4. En la pestaña **Registro**, seleccione la casilla de verificación **Activada** en el token del grupo.
5. Ingrese el token de grupo.
6. En la pestaña **Administración**, puede seleccionar el nombre de los administradores del grupo que tienen la tarea de administrar este grupo. En la casilla **Administradores de grupos disponibles**, seleccione el grupo en particular y haga clic en la flecha derecha para moverlo a la casilla **Administradores de grupos asignados**. Para mover un grupo desde **Administradores de grupos asignados** a **Administradores de grupos disponibles**, haga lo inverso. Este paso es opcional.
7. Haga clic en **Guardar**.

El grupo se agrega a la lista de grupos disponibles en la página **Grupos y configuraciones**.

**NOTA:** Los dispositivos se pueden registrar en un grupo ingresando el token de grupo que está disponible en la página **Grupos y configuraciones** para el grupo correspondiente.

Identifíer	GUID-AFFEBA1C-12F6-4BCB-BC5C-C04B1E79A950
Version	3
Status	Translation in review

# Crear un grupo de selección de ThinOS

## Pasos

1. En la página **Grupos y configuraciones**, haga clic en la opción **Grupo de políticas de grupo predeterminadas**.
2. Haga clic en **+**.
3. En el cuadro de diálogo **Agregar grupo nuevo**, ingrese el **Nombre del grupo** y la **Descripción**.
4. Seleccione la opción **Este es un elemento primario del grupo de selección de ThinOS**.
5. Seleccione el nombre de los administradores del grupo que tienen la tarea de administración de este grupo. En la casilla **Administradores de grupos disponibles**, seleccione el grupo en particular y haga clic en la flecha derecha para moverlo a la casilla **Administradores de grupos asignados**. Para mover un grupo desde **Administradores de grupos asignados** a **Administradores de grupos disponibles**, haga lo inverso. Este paso es opcional.
6. Haga clic en **Guardar**.

El grupo se agrega a la lista de grupos disponibles en la página **Grupos y configuraciones**.

Para agregar subgrupos al grupo principal que creó, haga clic en el grupo principal en la página **Grupos y configuraciones** y siga los pasos que se mencionan en [Crear grupo de políticas del dispositivo](#).

**NOTA:** El grupo de selección principal puede tener 10 grupos de selección secundarios y puede registrar los dispositivos en el grupo de selección secundario.

**NOTA:** Los perfiles se pueden configurar para otros sistemas operativos. Los perfiles creados son los mismos que los de otros grupos personalizados.

Identifíer	GUID-81F85AD9-B6F4-466F-86EF-B7C169BEC781
Version	1
Status	Translation in review

## Crear un grupo predeterminado de políticas de dispositivo


### Pasos

1. Vaya a la página **Grupos y configuraciones** y seleccione el **grupo predeterminado de políticas de dispositivo**.
2. En el cuadro de diálogo **Editar grupo predeterminado de políticas de dispositivo**, edite la información del grupo requerido.
3. Haga clic en **Guardar**.

Identifíer	GUID-39C6ADBC-6741-48B7-8858-E5B58BC7BA68
Version	2
Status	Translation approved

## Editar un grupo de selección de ThinOS

### Pasos


1. Vaya a la página **Grupos y configuraciones** y haga clic en el grupo de selección de Thin OS que desea editar.
2. Haga clic en .
3. En el cuadro de diálogo **Editando grupo de política predeterminada**, edite la información del grupo como el **Nombre del grupo** y la **Descripción**.
4. En la pestaña **Administración**, puede seleccionar el nombre de los administradores del grupo que tienen la tarea de administrar este grupo. En la casilla **Administradores de grupos disponibles**, seleccione el grupo en particular y haga clic en la flecha derecha para moverlo a la casilla **Administradores de grupos asignados**. Para mover un grupo desde **Administradores de grupos asignados** a **Administradores de grupos disponibles**, haga lo inverso. Este paso es opcional.
5. Haga clic en **Guardar**.

Identifíer	GUID-B38863AF-7848-4B4D-963F-DD29E0618A20
Version	1
Status	Translation approved

## Eliminar un grupo de selección de ThinOS

Como administrador, puede eliminar un grupo de la jerarquía de grupos.

### Pasos

1. En la página **Grupos y configuraciones**, seleccione el grupo de selección de ThinOS que desea eliminar.
2. Haga clic en .
3. En la lista desplegable, seleccione un nuevo grupo para los usuarios y los dispositivos que hay en el grupo actual.
4. Haga clic en **Borrar grupo**.

**NOTA:** Cuando elimina un grupo de la jerarquía de grupos, todos los usuarios y los dispositivos que pertenecen al grupo eliminado se mueven al grupo personalizado, de forma predeterminada, o al grupo no administrado.

**NOTA:** Cuando elimina el grupo de selección, los dispositivos del grupo eliminado no se pueden mover a otro grupo de selección.

Identifíer	GUID-0AF78464-3DE6-484A-B3B5-DA518CDF724E
Version	1
Status	Translation approved

## Configurar una política de nivel global

### Pasos


1. En la página **Grupos y configuraciones**, en el menú desplegable **Editar políticas**, seleccione un tipo de dispositivo.  
Aparecen los ajustes de la política del tipo de dispositivo respectivo.
2. Seleccione el ajuste de política que desee configurar y haga clic en **Configurar este elemento**.
3. Después de configurar las opciones, haga clic en **Guardar y publicar**.

Identifíer	GUID-5A40FEC9-B02F-4071-A0A6-58BAB8BD4FC5
Version	4
Status	Translation in review


## Crear un grupo de políticas de usuario

Puede crear grupos para las políticas globales de grupos de usuario y categorizar los usuarios y dispositivos según sus grupos de usuario.

### Pasos

1. En la página **Grupos y configuraciones**, haga clic en la opción **Grupo predeterminado de políticas de usuario**.
2. Haga clic en .
3. En el cuadro de diálogo **Agregar nuevo grupo**, ingrese el **nombre del grupo**, la **descripción**, el **dominio**, el **atributo de AD** y el **nombre del atributo de AD**.
4. Seleccione el nombre de los administradores del grupo que tienen la tarea de administración de este grupo.
5. En la casilla **Administradores de grupos disponibles**, seleccione el grupo en particular y haga clic en la flecha derecha para moverlo a la casilla **Administradores de grupos asignados**.  
Para mover un grupo desde **Administradores de grupos asignados** a **Administradores de grupos disponibles**, haga lo inverso.
6. Haga clic en **Guardar**.

El grupo se agrega a la lista de grupos disponibles en la página **Grupos y configuraciones**.

 **NOTA:** Un grupo de políticas de usuario se debe asignar a un grupo de AD o a una unidad organizacional, pero no a ambos.


7. Seleccione la opción **Mapeo de grupos de dispositivos** para importar grupos de usuarios con mapeo de dispositivos, a fin de controlar las configuraciones que se aplican a todos los grupos de dispositivos de forma predeterminada.

 **NOTA:** Esta función solo está disponible en la licencia Wyse Management Suite Pro. Puede importar 100 grupos de usuarios a Wyse Management Suite.

Identifíer	GUID-AAE516AD-47A3-4643-B86F-CE4B5E4B83E8
Version	4
Status	Translation in review

## Editar un grupo de políticas de usuario


### Pasos

1. Vaya a la página **Grupos y configuraciones** y seleccione el grupo predeterminado de políticas de usuario.
2. Haga clic en .
3. En el cuadro de diálogo **Editar grupo predeterminado de políticas de usuario**, edite la información del grupo requerido.
4. Haga clic en **Guardar**.

Identifíer	GUID-5FEC3630-2D90-41FF-949D-E218CDC7CDB7
Version	2
Status	Translation in review

## Importar un grupo de políticas de usuario



### Pasos

1. En la página **Grupos y configuraciones**, haga clic en la opción **Grupo predeterminado de políticas de usuario**.
2. Haga clic en .
3. En el cuadro de diálogo **Importación masiva**, busque el archivo .csv.  
El archivo .csv debe contener los detalles en el siguiente orden:
  - Nombre de grupo
  - Descripción
  - Dominio
  - Atributo de AD
  - Nombre de atributo de AD
4. Haga clic en **Importar**.

Identifíer	GUID-B508242A-CF8A-42FE-8B79-D15D78C220F3
Version	1
Status	Translation in review

## Importar un grupo de políticas de grupo desde Active Directory

### Pasos


1. Inicie sesión en la nube privada de Wyse Management Suite.
  2. Vaya a **Administrador del portal > Configuración de la consola > Active Directory**.
  3. Haga clic en la pestaña **Información de AD**.
  4. Haga clic en .
  5. Seleccione **Grupo de usuarios de AD** en **Autenticación de AD e importación única** y haga clic en **Importar grupo**.  
Puede ver los grupos de políticas de usuarios que se crean en la pestaña **Grupo predeterminado de políticas de usuario** en la página **Grupos y configuración**.
-  **NOTA:** Debe usar la interfaz del usuario del repositorio remoto para importar grupos de políticas de usuarios desde Active Directory en la nube pública.

Identifíer	GUID-7C1295CA-762B-43CC-AB32-AF303C8FF9C7
Version	3
Status	Translation in review

## Eliminar un grupo

Como administrador, puede eliminar un grupo de la jerarquía de grupos.

### Pasos

1. En la página **Grupos y configuraciones**, seleccione el grupo que desea eliminar.
2. Haga clic en .
3. En la lista desplegable, seleccione un nuevo grupo para los usuarios y los dispositivos que hay en el grupo actual.
4. Haga clic en **Borrar grupo**.



**NOTA:** Cuando elimina un grupo de la jerarquía de grupos, todos los usuarios y dispositivos que pertenecen a ese grupo eliminado se mueven a un grupo seleccionado.

Identifier	GUID-9DB1E3EF-0664-4BC8-922C-499D35023294
Version	1
Status	Translation approved

## Configurar una política del nivel del dispositivo

### Pasos

1. En la página **Dispositivos**, haga clic en el dispositivo que desee configurar.  
Se muestra la página **Detalles del dispositivo**.
2. En la sección **Configuración del dispositivo**, haga clic en **Crear/Editar excepciones**.

Identifier	GUID-AA9D50DB-55D3-42D6-9185-C11F76601A3C
Version	1
Status	Translation approved

## Exportar políticas de grupos

La opción **Exportar políticas** le permite exportar las políticas desde el grupo actual. Esta opción está disponible para usuarios de la licencia PRO de Wyse Management Suite.

### Pasos

1. En la página **Grupos y configuraciones**, seleccione el grupo desde el cual desea exportar las políticas. El grupo debe tener políticas configuradas.
2. Haga clic en **Exportar políticas**.  
Aparece la pantalla **Exportar políticas**.
3. Seleccione las políticas de tipo de dispositivo que desea exportar.  
Las siguientes opciones se encuentran disponibles:
  - Todas las políticas de tipo de dispositivo: se exportan todas las políticas de tipo de dispositivo.
  - Políticas específicas de tipo de dispositivo: seleccione uno o más tipos de dispositivo de la lista desplegable. Solo se exportan las políticas de tipo de dispositivo seleccionadas.
4. Haga clic en el botón **Sí** para exportar las políticas de tipo de dispositivo seleccionadas.  
Las políticas del grupo primario no se exportan. Solo se exportan las políticas que están configuradas en el nivel de grupo seleccionado o de destino.
5. Haga clic en el enlace de descarga o haga clic con el botón secundario en el archivo, y luego haga clic en **Guardar como** para guardar el archivo JSON .



**NOTA:** Las contraseñas están encriptadas en el archivo exportado. El nombre del archivo está en formato [Group Name]-[ALL]-[Exported Date & Time]UTC.json.

Identifier	GUID-83E5F344-4569-4125-8985-574B5D45FC58
Version	1
Status	Translation approved

## Importar políticas de grupos

La opción **Importar políticas** le permite importar las políticas. Esta opción está disponible para usuarios de la licencia PRO de Wyse Management Suite. Puede importar las políticas de grupos desde la página **Grupos y configuraciones** o desde la página **Editar políticas**.

Identifíer	GUID-916F3496-4848-4B68-A09A-FF39DD57A3B5
Version	1
Status	Translation approved

## Importar políticas de grupos desde la página Grupos y configuraciones

### Pasos

- En la página **Grupos y configuraciones**, seleccione el grupo que prefiera.  
Si el grupo de destino contiene políticas del mismo tipo de dispositivo que las importadas, se eliminan y se agregan otras nuevas.
- Haga clic en **Importar políticas**.  
Aparece la pantalla **Asistente de importación de políticas**.
- Seleccione el modo en que se importan las políticas de grupos del grupo seleccionado.  
Las siguientes opciones se encuentran disponibles:
  - Desde un grupo existente: seleccione un grupo de la lista desplegable. Las políticas de ese grupo se copian en el grupo actual.
  - Desde un archivo exportado: busque el archivo `.json`. Las políticas de ese archivo se copian en el grupo actual.
- Haga clic en **Siguiente**.
- Seleccione las configuraciones de tipo de dispositivo que desea importar.  
Las siguientes opciones se encuentran disponibles:
  - Todas las políticas de tipo de dispositivo: todas las políticas de tipo de dispositivo configuradas se importan al grupo actual.
  - Políticas específicas de tipo de dispositivo: seleccione uno o más tipos de dispositivo de la lista desplegable. Solo las políticas de tipo de dispositivo seleccionadas se importan al grupo actual.
- Haga clic en **Siguiente**.  
Se muestra una vista previa de las políticas en el grupo seleccionado.
- Haga clic en **Siguiente**.  
Se muestra el resumen del proceso de importación. Se pueden mostrar los siguientes tipos de advertencia:
  - Las políticas de <tipo de sistema operativo> importadas se aplican al grupo <nombre del grupo>**: cuando se importan las configuraciones del sistema operativo a un grupo que no contiene ninguna de las configuraciones.
  - Las políticas de <tipo de sistema operativo> ya existen para el grupo <nombre del grupo>. Se aplican o eliminan las políticas de <tipo de sistema operativo> existentes**: cuando importa nuevas configuraciones de tipo de sistema operativo a un grupo que contiene las configuraciones de tipo de sistema operativo.
  - La importación de políticas de un archivo que contiene dependencias a los archivos de inventario va a fallar. Para permitir esta importación, use la opción de importación de la ventana "Editar políticas"**: cuando importe las configuraciones de tipo de dispositivo de un archivo que contiene referencias a archivos de inventario.
- Haga clic en **Importar**.
  - NOTA:** Solo se pueden importar las configuraciones de tipo de dispositivo seleccionadas y las políticas que están definidas en el grupo de destino para el tipo de dispositivo seleccionado se eliminan antes de aplicar las políticas nuevas del mismo tipo de dispositivo.
  - NOTA:** Mientras importa las políticas de grupo, las contraseñas no se importan. El administrador debe volver a ingresar la contraseña en todos los campos de contraseña.

Identifíer	GUID-0C05BB8F-B011-47F5-81D9-BEC97E40B994
Version	1
Status	Translation approved

## Importar políticas de grupos desde la página Editar políticas

### Pasos

- En la página **Grupos y configuraciones**, seleccione el grupo que prefiera.
- Haga clic en **Editar políticas** y seleccione la opción que prefiera.

3. Haga clic en **Importar**.  
Aparece la pantalla **Asistente de importación de políticas**.
4. Seleccione el modo en que se importan las políticas de grupos del grupo seleccionado. Las siguientes opciones se encuentran disponibles:
  - Desde un grupo existente: seleccione un grupo de la lista desplegable. Las políticas de ese grupo se copian en el grupo actual.
  - Desde un archivo exportado: busque el archivo .JSON. Las políticas de ese archivo se copian en el grupo actual.
5. Haga clic en **Siguiente**.  
Se muestra una vista previa de las políticas en el grupo seleccionado.
6. Haga clic en **Siguiente**. Se muestra el resumen del proceso de importación. Se pueden mostrar los siguientes tipos de advertencia:
  - **Las políticas de <tipo de dispositivo> importadas se aplican al grupo <nombre del grupo>**: cuando se importan las configuraciones de tipo de dispositivo a un grupo que no contiene ninguna de estas configuraciones de tipo de dispositivo.
  - **Las políticas de <tipo de dispositivo> ya existen para el grupo <nombre del grupo>. Se eliminan las políticas existentes de <tipo de dispositivo> y se aplican las políticas importadas**: cuando se importan las configuraciones de tipo de dispositivo a un grupo que contiene las configuraciones de tipo de dispositivo.
  - **La importación de políticas de un archivo que contiene dependencias a los archivos de inventario va a fallar. Para permitir esta importación, use la opción de importación de la ventana “Editar políticas”**: cuando importe las configuraciones de tipo de dispositivo de un archivo que contiene referencias a archivos de inventario.
7. Haga clic en **Importar**.
 

**NOTA:** Cuando importa una política desde un archivo y si hay referencias o dependencias no válidas, la importación falla y aparece un mensaje de error. Además, si el archivo que va a importar tiene un archivo de referencia o de dependencia, consulte la página Editar política del tipo de dispositivo correspondiente y luego importe las políticas de grupo.

## Resultados

Si el grupo de destino contiene políticas del mismo tipo de dispositivo que las importadas, se eliminan y se agregan otras nuevas.

- NOTA:** Mientras importa las políticas de grupo, las contraseñas no se importan. El administrador debe volver a ingresar la contraseña en todos los campos de contraseña.

Identifier	GUID-8F1868D6-7F12-4544-9654-ED94F2B46F1D
Version	1
Status	Translation approved

# Editar la configuración de la política de ThinOS

## Pasos

1. Haga clic en **Grupos y configuración**.  
Se muestra la página **Grupos y configuración**.
2. Haga clic en el menú desplegable **Editar políticas**.
3. Haga clic en **ThinOS**.  
Se muestra la ventana **Seleccionar modo de configuración de ThinOS**.
4. Seleccione el modo preferido para configurar los ajustes de la política. Los modos disponibles son:
  - Modo de asistente
  - Modo de configuración avanzada

**NOTA:** Para establecer la Configuración avanzada de ThinOS como el modo predeterminado, seleccione la casilla de verificación.
5. Después de configurar los ajustes de la política, haga clic en **Guardar y publicar**.
 

**NOTA:** El cliente esbelto se reinicia si realiza cambios en la siguiente configuración:

  - Configuración del BIOS
  - Audio DP
  - Menú emergente de conexión
  - Nombre del terminal

- **Velocidad de Ethernet**
- **Cambio de pantalla: resolución, rotación, actualización, pantalla doble y pantalla múltiple**
- **Modo de sistema: VDI, StoreFront y clásico**
- **Enlace de puerto LPT**

Identifier	GUID-B8188852-C2EB-4890-8E89-99D7C3BB249B
Version	1
Status	Translation approved

## ThinOS: modo de asistente

Use esta página para configurar los parámetros usados con más frecuencia para los dispositivos ThinOS.

### Pasos

1. Seleccione **Asistente** como el modo de configuración.
2. Configure las opciones necesarias.
3. Haga clic en **Siguiente** para ir a la próxima configuración de política.
4. Haga clic en **Guardar y publicar** después de configurar las opciones.

 **NOTA:** Para ir al modo de configuración avanzada de ThinOS, haga clic en Continuar.

Identifier	GUID-586ABF73-7DB8-46CA-9805-4CE0FEED77E9
Version	1
Status	Translation approved

## ThinOS: modo avanzado

Use esta página para configurar los ajustes de política avanzados para los dispositivos ThinOS.

### Pasos

1. Seleccione **Configuración avanzada** como el modo de configuración.
2. Configure las opciones según sea necesario.
3. Haga clic en **Guardar y publicar** para guardar y publicar la configuración.

 **NOTA:** Para regresar a la página de ThinOS, haga clic en Eliminar política.

Identifier	GUID-77A99DA8-83B1-4A11-AE12-7541A6675B97
Version	3
Status	Translation in review

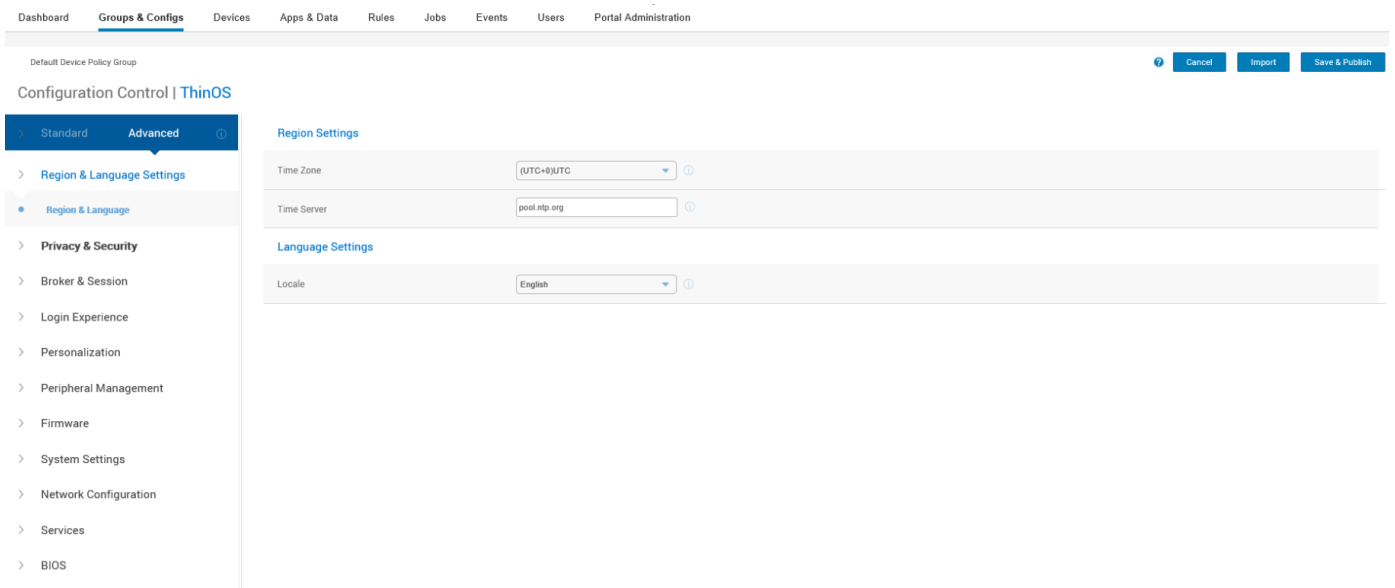
## Editar la configuración de la política de ThinOS 9.x

### Requisitos previos

- Cree un grupo con un token de grupo para los dispositivos en los que desea insertar el paquete de aplicaciones.
- Registre el cliente esbelto en Wyse Management Suite.

### Pasos

1. Vaya a la página **Grupos y configuraciones** y seleccione un grupo.
2. En el menú desplegable **Editar políticas**, haga clic en **ThinOS 9.x**. Aparece la ventana **Control de configuración | ThinOS**.
3. Haga clic en la opción **Avanzado**.



### Ilustración 3. Opción avanzada

4. Seleccione las opciones que desea configurar.

**NOTA:** Se agregó soporte de configuración del BIOS en Wyse Management Suite 2.1.

5. En los campos correspondientes, haga clic en la opción que desea configurar.
6. Configure las opciones según sea necesario.
7. Haga clic en **Guardar y publicar**.

**NOTA:** Después de hacer clic en Guardar y publicar, los ajustes configurados también aparecen en la pestaña **Estándar**.

Identifier	GUID-B69647C0-CCBB-4151-8766-A6B831077AD8
Version	1
Status	Translation in review

## Configuraciones del BIOS para ThinOS 9.x

### Sobre esta tarea

Los ajustes de configuración del BIOS pueden configurarse para dispositivos ThinOS 9.x mediante Wyse Management Suite 2.1. Puede implementar los paquetes del BIOS mediante la página **Grupos y configuraciones** o mediante la opción de asignación de subred.

**NOTA:** Esta función solo está disponible con la licencia Wyse Management Suite Pro.

### Pasos

1. Vaya a la página **Grupos y configuraciones** y seleccione un grupo.  
Aparece la ventana Control de configuración | ThinOS.
2. En el menú desplegable **Editar políticas**, haga clic en **ThinOS 9.x**.
3. Haga clic en **Opciones avanzadas**.
4. En el campo **BIOS**, haga clic en **Seleccione la plataforma** para elegir la plataforma en la que desea configurar los ajustes del BIOS.

Identifíer	GUID-1E359EA4-6F74-48B1-86B5-07254C6C50F0
Version	1
Status	Translation in review

## Cargar e insertar paquetes de OS

### Requisitos previos

- Cree un grupo en Wyse Management Suite con un token de grupo. Utilice este token de grupo para registrar los dispositivos ThinOS 9.x.
- Registre el cliente esbelto en Wyse Management Suite.

### Pasos

1. Vaya a la página **Grupos y configuraciones** y seleccione un grupo.
2. En el menú desplegable **Editar políticas**, haga clic en **ThinOS 9.x**. Aparece la ventana **Control de configuración || ThinOS**.
3. Haga clic en **Opciones avanzadas**
4. En el campo **Firmware**, seleccione **Actualizaciones de firmware del SO**.
5. Haga clic en el menú desplegable **Seleccione el firmware de ThinOS que desea implementar** y, luego, seleccione y cargue el paquete del BIOS.

**NOTA:** Puede cargar e implementar varios paquetes de firmware desde el repositorio remoto, el repositorio de nube de grupos de usuarios o el repositorio de nube del operador.

6. Haga clic en **Guardar y publicar**. El cliente delgado se reinicia y se instala el paquete del BIOS.

Identifíer	GUID-60CDA435-3340-42A2-BCDE-CF9B7206A846
Version	1
Status	Translation in review

## Cargar e insertar paquetes de BIOS

### Requisitos previos

- Cree un grupo en Wyse Management Suite con un token de grupo. Utilice este token de grupo para registrar los dispositivos ThinOS 9.x.
- Registre el cliente esbelto en Wyse Management Suite.

### Pasos

1. Vaya a la página **Grupos y configuraciones** y seleccione un grupo.
2. En el menú desplegable **Editar políticas**, haga clic en **ThinOS 9.x**. Aparece la ventana Control de configuración | ThinOS.
3. Haga clic en **Opciones avanzadas**.
4. En el campo **Firmware**, haga clic en **Actualizaciones de firmware del SO**.
5. En el menú desplegable **Seleccionar el BIOS de ThinOS que desea implementar**, seleccione el paquete.

**NOTA:** Puede cargar e implementar varios paquetes de firmware desde el repositorio remoto, el repositorio de nube de grupos de usuarios o el repositorio de nube del operador. Puede cargar 10 paquetes desde el repositorio de nube de grupos de usuarios.

6. Haga clic en **Guardar y publicar**. El cliente esbelto se reinicia y se instala el paquete de aplicaciones.

También puede cargar el firmware del BIOS desde **Aplicaciones y datos** en Wyse Management Suite 2.1, como se indica en los siguientes pasos:

- a. Vaya a la página **Aplicaciones y datos**.
- b. Haga clic en **Repositorio de imágenes del SO** y seleccione **ThinOS 9.x**.
- c. Haga clic en **Agregar archivo de BIOS** para examinar y agregar el archivo que desea agregar al repositorio.

 **NOTA:** Esta función solo está disponible en la licencia Wyse Management Suite Pro.

Identifier	GUID-4A6360E5-5E34-49A1-8655-395EC1ECF3FE
Version	3
Status	Translation in review

## Cargar y subir paquetes de aplicaciones de ThinOS 9.x mediante Wyse Management Suite

### Requisitos previos

- Cree un grupo en Wyse Management Suite con un token de grupo. Utilice este token de grupo para registrar los dispositivos ThinOS 9.x.
- Registre el cliente esbelto en Wyse Management Suite.

### Pasos

1. Vaya a la página **Grupos y configuraciones** y seleccione un grupo.
2. En el menú desplegable **Editar políticas**, haga clic en **ThinOS 9.x**. Aparece la ventana **Control de configuración | ThinOS**.
3. Haga clic en **Opciones avanzadas**.
4. En el campo **Firmware**, haga clic en **Actualizaciones de paquete de aplicaciones**.
5. En el menú desplegable **Seleccionar los paquetes de ThinOS que desea implementar**, seleccione el paquete.

 **NOTA:** Puede cargar e implementar varios paquetes de firmware desde el repositorio remoto, el repositorio de nube de grupos de usuarios o el repositorio de nube del operador.

6. Haga clic en **Guardar y publicar**. El cliente esbelto se reinicia y se instala el paquete de aplicaciones.

Identifier	GUID-F9D352D7-E2B2-4C14-8B4D-6B1843BF062A
Version	1
Status	Translation approved

## Editar la configuración de la política de Windows Embedded Standard

### Pasos

1. Haga clic en **Grupos y configuración**. Se muestra la página **Grupos y configuración**.
2. Haga clic en el menú desplegable **Editar políticas**.
3. Haga clic en **WES**. Aparece la página **WES**.
4. Después de configurar los ajustes de la política, haga clic en **Guardar y publicar**.

Identifier	GUID-EC3A1168-3401-496D-B580-A7D9D71556C5
Version	1
Status	Translation approved

## Editar la configuración de la política de Linux

### Pasos

1. Haga clic en **Grupos y configuración**. Se muestra la página **Grupos y configuración**.
2. Haga clic en el menú desplegable **Editar políticas**.
3. Haga clic en **Linux**.

- Después de configurar los ajustes de la política, haga clic en **Guardar y publicar**.

Identifíer	GUID-3D9FF68E-E3BF-4362-AA8F-C1DC59B152F8
Version	1
Status	Translation approved

## Editar la configuración de la política de ThinLinux

### Pasos

- Haga clic en **Grupos y configuración**.  
Se muestra la página **Grupos y configuración**.
- Haga clic en el menú desplegable **Editar políticas**.
- Haga clic en **ThinLinux**.
- Después de configurar los ajustes de la política, haga clic en **Guardar y publicar**.

Identifíer	GUID-89C76C87-EB31-45C4-823D-E1D7F330ACB7
Version	1
Status	Translation approved

## Editar la configuración de la política de Wyse Software Thin Client

### Pasos

- Haga clic en **Grupos y configuración**.  
Se muestra la página **Grupos y configuración**.
- Haga clic en el menú desplegable **Editar políticas**.
- Haga clic en **Ciente delgado Wyse Software**.  
Aparece la página **Ciente delgado del software Wyse**.
- Después de configurar los ajustes de la política, haga clic en **Guardar y publicar**.

Identifíer	GUID-0B7EB956-112A-44E5-AC7B-6F63F5CF134C
Version	1
Status	Translation approved

## Editar la configuración de la política de Cloud Connect

### Pasos

- Haga clic en **Grupos y configuración**.  
Se muestra la página **Grupos y configuración**.
- Haga clic en el menú desplegable **Editar políticas**.
- Haga clic en **Cloud Connect**.
- Después de configurar los ajustes de la política, haga clic en **Guardar y publicar**.

Identifier	GUID-EA69AEA1-B7FE-4243-9A1C-02E1F0B5BEDF
Version	1
Status	Translation approved

## Administrar dispositivos

En esta sección se describe cómo realizar una tarea de rutina de administración de dispositivos usando la consola de administración. Para localizar el inventario de los dispositivos, haga clic en la pestaña **Dispositivos**. Puede ver un subconjunto de los dispositivos usando varios criterios de filtro, como grupos o subgrupos, tipo de dispositivo, tipo de sistema operativo, estado, subred, plataforma o zona horaria.

Puede ordenar la lista de dispositivos según los siguientes aspectos:

- Tipo
- Plataforma
- Versión del sistema operativo
- Número de serie
- Dirección IP
- Detalles del usuario más reciente
- Detalles del grupo
- Hora del último registro
- Estado del registro
- Estado del filtro de escritura

Para ver la página **Detalles del dispositivo** de un dispositivo en particular, haga clic en la entrada del dispositivo indicada en la página. Todos los parámetros de configuración del dispositivo y el nivel del grupo en el que se aplica cada parámetro se muestran en la página **Detalles del dispositivo**.

Puede establecer el parámetro de configuración específico de ese dispositivo. En esta sección, los parámetros configurados anulan cualquier parámetro que se haya configurado en los niveles globales o de grupo.

Ilustración 4. Página Dispositivos

## Temas:

- Métodos para registrar los dispositivos en Wyse Management Suite
- Buscar un dispositivo mediante filtros
- Guardar el filtro en la página Dispositivos
- Consultar el estado del dispositivo
- Bloquear los dispositivos
- Reiniciar los dispositivos
- Anular el registro del dispositivo
- Validación de la inscripción
- Restablecer el dispositivo a los ajustes predeterminados de fábrica
- Cambiar la asignación de un grupo en la página Dispositivos
- Enviar mensajes a un dispositivo
- Activar el dispositivo
- Ver los detalles del dispositivo
- Administrar el resumen del dispositivo
- Ver información del sistema
- Ver eventos del dispositivo
- Ver las aplicaciones instaladas
- Renombrar el cliente delgado
- Configurar la conexión de seguimiento remoto
- Apagar dispositivos
- Etiquetar un dispositivo
- Estado de cumplimiento de normas del dispositivo
- Obtener la imagen de Windows Embedded Standard o ThinLinux
- Solicitar un archivo de registro
- Solución de problemas del dispositivo

Identifíer	GUID-2A406116-3EF8-4399-BBF5-E045C11E1190
Version	1
Status	Translation approved

## Métodos para registrar los dispositivos en Wyse Management Suite

Puede registrar un cliente delgado para Wyse Management Suite por medio de cualquiera de los siguientes métodos:

- Registre manualmente a través de la interfaz de usuario ofrecida por Wyse Device Agent (WDA) en el dispositivo.
- Registre automáticamente configurando las etiquetas de opciones adecuadas en el servidor de DHCP.
- Registre automáticamente configurando los registros DNS SRV adecuados en el servidor de DNS.

### **NOTA:**

- Para una nube pública, registre un Thin client indicando la URL de Wyse Management Suite y el token de grupo para el grupo en el que desea registrar el dispositivo.
- Para una nube privada, registre un cliente esbelto indicando la URL de Wyse Management Suite y el token de grupo; opcional para el grupo en el que desea registrar este dispositivo. Los dispositivos se registran en el grupo no administrado si no se indica el token de grupo.

Identifíer	GUID-E8C5E6E0-1F67-4899-B0A7-99C4F088D067
Version	1
Status	Translation approved

## Registrar dispositivos ThinOS mediante Wyse Device Agent

Para registrar dispositivos ThinOS manualmente, haga lo siguiente:

## Pasos

1. Desde el menú del escritorio del cliente esbelto, vaya a **Configuración del sistema > Configuración central**. Aparecerá la ventana **Configuración central**.
2. Haga clic en la pestaña **WDA**. El servicio WDA se ejecuta automáticamente después de que el proceso de arranque del cliente se completa.

**WMS** aparece seleccionado de manera predeterminada.

3. Seleccione la casilla de verificación **Activar Wyse Management Suite** para activar Wyse Management Suite.
4. Ingrese la **Clave de registro del grupo** según lo que configuró el administrador para el grupo deseado.
5. Seleccione la opción **Activar configuración avanzada de WMS** e ingrese los detalles del servidor WMS o del servidor MQTT.
6. Active o desactive la validación de CA según su tipo de licencia. Para la nube pública, marque la casilla de verificación **Activar validación de CA** y, para la nube privada, marque la casilla de verificación **Activar validación de CA** si importó certificados de una autoridad de certificación reconocida al servidor la Wyse Management Suite.

Para activar la opción de validación de CA en la nube privada, también debe instalar el mismo certificado autofirmado en el dispositivo de ThinOS. Si no ha instalado el certificado autofirmado en el dispositivo ThinOS, no marque la casilla de verificación **Activar validación de CA**. Puede instalar el certificado en el dispositivo utilizando Wyse Management Suite después de registrarse y luego activar la opción de validación de CA.

### **i** NOTA:

- Aparecerá un mensaje de aviso si deshabilita la validación de CA. Debe hacer clic en **Aceptar para confirmar**.
- En el caso de la versión de nube pública de Wyse Management Suite en los centros de datos en EE. UU., no cambie los detalles predeterminados de los servidores WMS y MQTT. En el caso de la versión de nube pública de Wyse Management Suite en los centros de datos en Europa, utilice lo siguiente:
  - Servidor CCM: [eu1.wysemanagementsuite.com](http://eu1.wysemanagementsuite.com)
  - Servidor MQTT: [eu1-pns.wysemanagementsuite.com:1883](http://eu1-pns.wysemanagementsuite.com:1883)
- Aparecerá un mensaje de aviso si la dirección del servidor contiene http. Debe hacer clic en **Aceptar para confirmar**.

7. Para verificar la configuración, haga clic en **Validar clave**. El dispositivo se reinicia automáticamente después de validar la clave.

### **i** NOTA: Si la clave no se valida, verifique la clave de grupo y el URL del servidor WMS que proporcionó. Asegúrese de que los puertos 443 y 1883 no estén bloqueados por la red.

8. Haga clic en **Aceptar**. El dispositivo está registrado en Wyse Management Suite.

Identifíer	GUID-456F5EF6-8F94-4A2A-A4D7-11934698AA5C
Version	1
Status	Translation approved

# Registrar clientes esbeltos de Windows Embedded Standard para Wyse Management Suite mediante Wyse Device Agent

## Requisitos previos

Cree un grupo en Wyse Management Suite para registrar un dispositivo.

## Pasos

1. Abra la aplicación Wyse Device Agent. Aparecerá la ventana Wyse Device Agent.
2. En la lista desplegable **Servidor de administración**, seleccione **Wyse Management Suite**.
3. Ingrese la dirección del servidor y el número de puerto en los campos correspondientes.

### **i** NOTA: Si la dirección del servidor contiene http, aparece un mensaje de advertencia. Haga clic en **Aceptar para confirmar**.

4. Ingrese el token de grupo. Para un inquilino único, el token de grupo es un paso opcional.

**i** **NOTA:** El token de grupo que se ingresa en el campo Token de grupo no se muestra en texto no cifrado.

5. Active o desactive la validación de CA que se basa en el tipo de licencia.

**i** **NOTA:** Si desactiva la validación de CA, aparece un mensaje de advertencia. Haga clic en Aceptar para confirmar.

6. Haga clic **Registrar**.

Identifier	GUID-EE8C5BD5-C478-4C20-BD59-EFC861ABB8B0
Version	1
Status	Translation approved

## Registrar el cliente esbelto de Wyse Software en Wyse Management Suite mediante Wyse Device Agent

### Requisitos previos

Cree un grupo para registrar un dispositivo para Wyse Management Suite.

### Pasos

1. Abra la aplicación **Wyse Device Agent**.

Se muestra la ventana de **Wyse Device Agent**.

2. Ingrese los detalles de registro del dispositivo.

3. En la lista desplegable **Servidor de administración**, seleccione **Wyse Management Suite**.

4. Ingrese la dirección del servidor y el número de puerto en los campos correspondientes.

**i** **NOTA:** Si la dirección del servidor contiene http, aparece un mensaje de advertencia. Haga clic en Aceptar para confirmar.

5. Ingrese el token de grupo. Para un inquilino único, el token de grupo es un paso opcional.

6. Active o desactive la validación de CA que se basa en el tipo de licencia.

**i** **NOTA:** Si desactiva la validación de CA, aparece un mensaje de advertencia. Haga clic en Aceptar para confirmar.

7. Haga clic **Registrar**.

Una vez finalizado el proceso de registro, aparece el mensaje **Wyse Management Suite se registró**.

Identifier	GUID-7649FF26-0BA4-4037-8637-92808E7611CA
Version	1
Status	Translation approved

## Registrar clientes esbeltos de ThinLinux mediante Wyse Device Agent

### Requisitos previos

Cree un grupo en Wyse Management Suite para registrar un dispositivo.

### Pasos

1. Abra la aplicación Wyse Device Agent.

Aparecerá la ventana Wyse Device Agent.

2. Ingrese los detalles de registro del dispositivo.

3. En la pestaña Wyse Management Suite, ingrese los detalles del servidor Wyse Management Suite.

4. Ingrese el token de grupo.

Para un inquilino único, el token de grupo es un paso opcional.

- Haga clic **Registrar**.  
Una vez finalizado el registro, se mostrará el mensaje de confirmación.

Identifier	GUID-16BFD811-8B57-45C2-991C-D901E5E22266
Version	1
Status	Translation approved

## Registrar dispositivos ThinOS mediante el método FTP INI

### Requisitos previos

Cree un grupo y regístrelo en Wyse Management Suite.

### Pasos

1. Cree un archivo `wnos.ini`. Ingrese el siguiente parámetro:

**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

Por ejemplo, para registrar el dispositivo ThinOS en Wyse Management Suite (el nombre de dominio completamente calificado del servidor corresponde a `ServerFQDN.domain.com`), con el grupo de token `defa-defadefa` y con la opción de validación de CA activada, ingrese el siguiente parámetro de INI:

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

2. Coloque el archivo `wnos.ini` dentro de la carpeta `wnos` de cualquier ruta de FTP.
3. Vaya a **Configuración central** en el dispositivo ThinOS.
4. En la pestaña **General**, proporcione la ruta FTP en los servidores de archivos o la ruta hasta la carpeta principal.
5. Ingrese las credenciales de FTP si es necesario. Si no se requieren credenciales para acceder a FTP, el nombre de usuario y la contraseña pueden ser anónimos.
6. Haga clic en **Aceptary**, a continuación, reinicie el cliente delgado.
7. Vaya a **Configuración central** en el dispositivo ThinOS.  
 En la pestaña **Wyse Device Agent**, tenga en cuenta que los detalles del servidor de Wyse Management están disponibles en el campo correspondiente y que la entrada del cliente se puede ver en la página Servidor de Wyse Management > Dispositivos.

Identifier	GUID-DC1CA306-5084-4AE1-9F26-614AA29271D1
Version	1
Status	Translation approved

## Registrar dispositivos ThinLinux versión 2.0 mediante el método FTP INI

### Requisitos previos

Cree un grupo y regístrelo en Wyse Management Suite.

### Pasos

1. Cree un archivo `wlx.ini`. Ingrese el siguiente parámetro:

**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

Por ejemplo, para registrar el dispositivo ThinLinux versión 2.0 en Wyse Management Suite (el nombre de dominio completamente calificado del servidor corresponde a `ServerFQDN.domain.com`), con el grupo de token `defa-defadefa` y con la opción de validación de CA activada, ingrese el siguiente parámetro de INI:

**WMSEnable**=yes

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

**GroupRegistrationKey**=defa-defadefa

**CAValidation**=True

2. Ubique el archivo wlx ini en la carpeta wyse\wlx2.
3. Vaya a **Configuración** y cambie a admin en el cliente delgado de ThinLinux.
4. Vaya a **Administración > INI**.
5. Ingrese la URL del servidor FTP.
6. Haga clic en **Guardar** y luego reinicie el cliente esbelto.
7. Vaya a **Administración > Wyse Device Agent**.  
En la pestaña Wyse Device Agent, tenga en cuenta que los detalles del servidor de Wyse Management están disponibles en el campo correspondiente y que la entrada del cliente se puede ver en la página Servidor de Wyse Management > Dispositivos.

Identifier	GUID-87186E57-AF0E-4C3A-A7D4-4121AF68E187
Version	1
Status	Translation approved

## Registrar dispositivos ThinLinux versión 1.0 mediante el método FTP INI

### Requisitos previos

Cree un grupo y regístrelo en Wyse Management Suite.

### Pasos

1. Cree un archivo wlx.ini e ingrese el siguiente parámetro:

**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

Por ejemplo, para registrar la versión ThinLinux 1.0 en Wyse Management Suite (el nombre de dominio completamente calificado del servidor corresponde a ServerFQDN.domain.com), con el grupo de token defa-defadefa y con la opción de validación de CA activada, ingrese el siguiente parámetro de INI:

**WMSEnable**=yes

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

**GroupRegistrationKey**=defa-defadefa

**CAValidation**=True

2. Ponga el archivo wlx ini en la carpeta wyse\wlx.
3. Vaya a **Configuración** y cambie a admin en el cliente delgado de ThinLinux.
4. Vaya a **Administración > INI**.
5. Ingrese la URL del servidor FTP.
6. Haga clic en **Guardar** y luego reinicie el cliente esbelto.
7. Vaya a **Administración > Wyse Device Agent**.  
En la pestaña Wyse Device Agent, tenga en cuenta que los detalles del servidor de Wyse Management están disponibles en el campo correspondiente y que la entrada del cliente se puede ver en la página Servidor de Wyse Management > Dispositivos.

Identifíer	GUID-D27C9C48-FB23-4D8C-8371-4608649304C9
Version	1
Status	Translation approved

## Registrar dispositivos mediante etiquetas de opciones de DHCP

Puede registrar los dispositivos utilizando las etiquetas de opción de DHCP.

**Tabla 3. Registrar un dispositivo mediante etiquetas de opciones de DHCP**

Etiqueta de opciones	Descripción
<p><b>Nombre:</b> WMS</p> <p><b>Tipo de dato:</b> cadena</p> <p><b>Código:</b> 165</p> <p><b>Descripción:</b> FQDN de servidor de WMS</p>	<p>Esta etiqueta señala la URL del servidor de Wyse Management Suite. Por ejemplo, <code>wmserver.acme.com:443</code>, donde <code>wmserver.acme.com</code> es el nombre de dominio completo del servidor donde Wyse Management Suite se encuentra instalado.</p>
<p><b>Nombre:</b> MQTT</p> <p><b>Tipo de dato:</b> cadena</p> <p><b>Código:</b> 166</p> <p><b>Descripción:</b> servidor de MQTT</p>	<p>Esta etiqueta dirige el dispositivo al servidor de notificación push de Wyse Management Suite (PNS). Para una instalación de nube privada, el dispositivo se dirige al servicio de MQTT en el servidor de Wyse Management Suite. Por ejemplo, <code>wmservername.domain.com:1883</code>.</p> <p>Para registrar sus dispositivos en la nube pública de Wyse Management Suite, el dispositivo debe señalar los servidores de PNS (MQTT) en la nube pública. Por ejemplo:</p> <p>EE. UU.1:<a href="https://us1-pns.wysemanagementsuite.com">us1-pns.wysemanagementsuite.com</a></p> <p>UE1:<a href="https://eu1-pns.wysemanagementsuite.com">eu1-pns.wysemanagementsuite.com</a></p>
<p><b>Nombre:</b> Validación de CA</p> <p><b>Tipo de dato:</b> cadena</p> <p><b>Código:</b> 167</p> <p><b>Descripción:</b> Validación de la entidad emisora de certificados</p>	<p>Puede activar o desactivar la opción de validación de CA si registra sus dispositivos con Wyse Management Suite en la nube privada. De manera predeterminada, la validación de CA está activada en la nube pública. También puede desactivar la validación de CA en la nube pública.</p> <p>Ingrese <b>Verdadero</b> si importó los certificados de SSL desde una entidad emisora conocida para la comunicación https entre el cliente y servidor de Wyse Management Suite.</p> <p>Ingrese <b>Falso</b> si no importó los certificados de SSL desde una entidad emisora reconocida para la comunicación https entre el cliente y servidor de Wyse Management Suite.</p>
<p><b>Nombre:</b> token de grupo</p> <p><b>Tipo de dato:</b> cadena</p> <p><b>Código:</b> 199</p> <p><b>Descripción:</b> token de grupo</p>	<p>Esta etiqueta es necesaria para registrar los dispositivos ThinOS con Wyse Management Suite en una nube privada o pública.</p> <p>Esta etiqueta es opcional para registrar los dispositivos Windows Embedded Standard o ThinLinux con Wyse Management Suite en una nube privada. Si la etiqueta no está disponible, los dispositivos se registran automáticamente en el grupo no administrado en el curso de instalación in situ.</p>

**NOTA:** Para obtener instrucciones detalladas sobre cómo agregar etiquetas de opción de DHCP en el servidor Windows, consulte [Cómo creo y configuro etiquetas de opción de DHCP](#).

Identifíer	GUID-0073BF93-E5DC-4687-8CF1-F2D61BDB3098
Version	1
Status	Translation approved

## Registrar dispositivos mediante registro SRV DNS

El registro de dispositivos basado en DNC es compatible con las siguientes versiones de Wyse Device Agent:

- Sistemas Windows Embedded: 13.0 o versiones posteriores
- Thin Linux: 2.0.24 o versiones posteriores

- ThinOS: firmware 8.4 o versiones posteriores

Puede registrar los dispositivos en el servidor de Wyse Management Suite si los campos de registros SRV de DNS se establecen con los valores válidos.

**NOTA:** Para obtener instrucciones detalladas sobre cómo agregar registros SRV de DNS en el servidor Windows, consulte [Cómo creo y configuro un registro SRV de DNS](#).

En la siguiente tabla se indican los valores válidos para los registros SRV de DNS:

**Tabla 4. Configurar el dispositivo mediante un registro SRV de DNS**

URL/etiqueta	Descripción
<p><b>Nombre de registro:</b> _WMS_MGMT</p> <p><b>FQDN de registro:</b> _WMS_MGMT._tcp.&lt;Domainname&gt;</p> <p><b>Tipo de registro:</b> SRV</p>	<p>Este registro señala la URL del servidor de Wyse Management Suite. Por ejemplo, <code>wmserver.acme.com:443</code>, donde <code>wmserver.acme.com</code> es el nombre de dominio completo del servidor donde Wyse Management Suite se encuentra instalado.</p> <p><b>NOTA:</b> No utilice <code>https://</code> en la URL del servidor, o el cliente delgado no se registrará en Wyse Management Suite.</p>
<p><b>Nombre de registro:</b> _WMS_MQTT</p> <p><b>FQDN de registro:</b> _WMS_MQTT._tcp.&lt;Domainname&gt;</p> <p><b>Tipo de registro:</b> SRV</p>	<p>Este registro dirige el dispositivo al servidor de notificación push de Wyse Management Suite (PNS). Para una instalación de nube privada, el dispositivo se dirige al servicio de MQTT en el servidor de Wyse Management Suite. Por ejemplo, <code>wmservername.domain.com:1883</code>.</p> <p><b>NOTA:</b> MQTT es opcional para la versión más reciente de Wyse Management Suite.</p> <p>Para registrar sus dispositivos en la nube pública de Wyse Management Suite, el dispositivo debe señalar los servidores de PNS (MQTT) en la nube pública. Por ejemplo:</p> <p>EE. UU.1: <a href="https://us1-pns.wysemanagementsuite.com">us1-pns.wysemanagementsuite.com</a></p> <p>UE1: <a href="https://eu1-pns.wysemanagementsuite.com">eu1-pns.wysemanagementsuite.com</a></p>
<p><b>Nombre de registro:</b> _WMS_GROUPTOKEN</p> <p><b>FQDN de registro:</b> _WMS_GROUPTOKEN._tcp.&lt;Domainname&gt;</p> <p><b>Tipo de registro:</b> TEXTO</p>	<p>Este registro es necesario para registrar los dispositivos ThinOS con Wyse Management Suite en una nube privada o pública.</p> <p>Este registro es opcional para registrar los dispositivos Windows Embedded Standard o ThinLinux con Wyse Management Suite en una nube privada. Si el registro no está disponible, los dispositivos se registran automáticamente para el grupo no administrado durante la instalación in situ.</p> <p><b>NOTA:</b> El token de grupo es opcional para la versión más reciente de Wyse Management Suite en nube privada.</p>
<p><b>Nombre de registro:</b> _WMS_CAVVALIDATION</p> <p><b>FQDN de registro:</b> _WMS_CAVVALIDATION._tcp.&lt;Domainname&gt;</p> <p><b>Tipo de registro:</b> TEXTO</p>	<p>Puede activar o desactivar la opción de validación de CA si registra sus dispositivos con Wyse Management Suite en la nube privada. De manera predeterminada, la validación de CA está activada en la nube pública. También puede desactivar la validación de CA en la nube pública.</p> <p>Ingrese <b>Verdadero</b> si importó los certificados de SSL desde una entidad emisora conocida para la comunicación https entre el cliente y servidor de Wyse Management Suite.</p> <p>Ingrese <b>Falso</b> si no importó los certificados de SSL desde una entidad emisora reconocida para la comunicación https entre el cliente y servidor de Wyse Management Suite.</p> <p><b>NOTA:</b> Validación de CA es opcional para la versión más reciente de Wyse Management Suite.</p>

Identifíer	GUID-C507B253-E9C7-44E8-A9C7-AE0B8AE54247
Version	1
Status	Translation approved

## Buscar un dispositivo mediante filtros

### Pasos

1. En la lista desplegable **Grupos de configuración**, seleccione el grupo de política predeterminada o los grupos agregados por un administrador.
2. En la lista desplegable **Estado**, seleccione cualquiera de las siguientes opciones:
  - **Registro**
    - Registrado
    - Registrado previamente
    - No registrado
    - Conforme
    - Validación de inscripción pendiente
    - Pendiente
    - No conforme
  - **Estado en línea**
    - En línea
    - Sin conexión
    - Desconocido
  - **Otros**
    - Agregado recientemente
3. En la lista desplegable **Tipo de SO**, seleccione cualquiera de los siguientes sistemas operativos:
  - **Thin client**
    - Linux
    - ThinLinux
    - ThinOS
    - WES
    - Teradici (nube privada)
    - Wyse Software Thin Client
4. En la lista desplegable **Subtipo de SO**, seleccione un subtipo para su sistema operativo.
5. En la lista desplegable **Plataforma**, seleccione una plataforma.
6. En la lista desplegable **Versión del SO**, seleccione una versión del SO.
7. En la lista desplegable **Versión del agente**, seleccione una versión del agente.
8. En la lista desplegable **Subred**, seleccione una subred.
9. En la lista desplegable **Zona horaria**, seleccione la zona horaria.
10. En la lista desplegable **Etiqueta del dispositivo**, seleccione la etiqueta del dispositivo.

Identifíer	GUID-A7CB037C-92D6-4808-87B0-E58E15C6CC91
Version	2
Status	Translation in review

## Guardar el filtro en la página Dispositivos

Puede guardar el filtro actual como un grupo configurando las opciones de filtro requeridas.

### Pasos

1. Ingrese el **Nombre** del filtro.
2. Ingrese una descripción para el filtro en el cuadro de texto **Descripción**.
3. Seleccione la casilla de verificación para establecer el filtro actual como la opción predeterminada.
4. Haga clic en **Guardar filtro**.

Identifíer	GUID-5164A78D-DC08-4795-B143-6CBA5DE81FC1
Version	1
Status	Translation approved

## Consultar el estado del dispositivo

Puede enviar un comando para actualizar la información y el estado del dispositivo en el sistema.

### Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivo**.
2. Aplicar los filtros para encontrar el dispositivo preferido.
3. Seleccione la casilla de verificación del dispositivo.
4. Haga clic en **Consulta**.  
Se muestra la ventana **Alerta**.
5. Haga clic en **Enviar comando** para enviar el comando de consulta.

Identifíer	GUID-9D99AB86-F043-4B09-8DBC-513FFC6FD964
Version	1
Status	Translation approved

## Bloquear los dispositivos

Puede enviar un comando para desbloquear el dispositivo registrado.

### Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivo**.
2. Aplicar los filtros para encontrar el dispositivo preferido.
3. Seleccione la casilla de verificación del dispositivo.
4. Haga clic en **Bloqueo**.  
Se muestra la ventana **Alerta**.
5. Haga clic en **Enviar comando** para enviar el comando de bloqueo.

Identifíer	GUID-0D8C7A2B-5957-444D-AB63-C6985075D108
Version	1
Status	Translation approved

## Reiniciar los dispositivos

Puede enviar un comando para reiniciar un dispositivo registrado.

### Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivo**.
2. Aplicar los filtros para encontrar el dispositivo preferido.
3. Seleccione la casilla de verificación del dispositivo.
4. Haga clic en **Reiniciar**.  
Se muestra la ventana **Alerta**.
5. Haga clic en **Enviar comando** para enviar el comando de reinicio.

Identifíer	GUID-B494EA82-3CD1-45B5-9DED-06467003EF5E
Version	1
Status	Translation approved

## Anular el registro del dispositivo

Puede enviar un comando para anular el registro de un dispositivo desde Wyse Management Suite.

## Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivo**.
2. Aplicar los filtros para encontrar el dispositivo preferido.
3. Seleccione la casilla de verificación del dispositivo.
4. Haga clic en **Cancelar registro**.  
Se muestra la ventana **Alerta**.
5. Seleccione la casilla de verificación **Forzar anulación de registro**.
6. Haga clic en **Enviar comando** para enviar el comando para cancelar el registro.

**NOTA:** La opción **Forzar anulación del registro** se puede utilizar para eliminar el dispositivo cuando no exista comunicación entre el servidor y el cliente. El dispositivo cambia al estado **no administrado** y se puede eliminar de la entrada del servidor. En la IU de WES WDA también se pueden realizar las acciones de **Anular el registro** y **Forzar anulación del registro**.

Identifíer	GUID-F56E2ED4-4869-4A31-B40D-CF3688371301
Version	1
Status	Translation approved

## Validación de la inscripción

Cuando registra un dispositivo de forma manual o mediante el método de detección automática de DHCP/DNS, el dispositivo se registra en un grupo específico si se define el token de grupo. Si no se define el token de grupo, el dispositivo se registra en el grupo no administrado.

En Wyse Management Suite, se introduce la opción de **Validación de la inscripción** donde el grupo de usuarios se debe aprobar manualmente antes de que el dispositivo se registre en un grupo.

Cuando la opción **Validación de la inscripción** está activada, los dispositivos detectados automáticamente se encuentran en estado de **Validación pendiente** en la página **dispositivos**. El usuario puede seleccionar un solo dispositivo o varios dispositivos en la página **Dispositivos** y validar la inscripción. Los dispositivos se mueven al grupo deseado después de que se validan. Para obtener más información sobre cómo validar los dispositivos, consulte [Validación de la inscripción](#).

**NOTA:** La opción de **Validación de la inscripción** está deshabilitada para los grupos de usuarios existentes en la nube pública o cuando se actualizan los grupos de usuarios en las instalaciones.

El estado de validación de los dispositivos también aparece en la sección **Dispositivos** en la página **Panel**.

Identifíer	GUID-470EA1B5-8319-4BC4-8CFD-1B2CB3F93B9D
Version	1
Status	Translation approved

## Validar la inscripción de un dispositivo

Puede habilitar la **Validación de la inscripción** para permitir que los administradores controlen el registro manual y automático de los clientes esbeltos en un grupo. Puede filtrar los dispositivos con estado de **Validación pendiente** haciendo clic en el conteo **Pendiente** en la página **Panel** o seleccionando **Validación de inscripción pendiente** en la lista desplegable **Estado** en la página **Dispositivos**.

### Requisitos previos

- Debe habilitar la opción **Validación de la inscripción** cuando instale Wyse Management Suite o en la página **Administración del portal**.
- El dispositivo debe estar en el estado de inscripción pendiente.

### Pasos

1. Seleccione la casilla de verificación del dispositivo que desea validar.
2. Haga clic en la opción **Validar la inscripción**.  
Se muestra la ventana **Alerta**.
3. Haga clic en **Enviar comando**.  
El dispositivo se mueve al grupo deseado y el dispositivo está registrado.

Identifíer	GUID-BB75E8B1-09A3-45C7-95E1-EA1FCF47CC8C
Version	2
Status	Translation in review

## Restablecer el dispositivo a los ajustes predeterminados de fábrica

Puede enviar un comando para restablecer el dispositivo a los ajustes predeterminados de fábrica.

### Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivo**.
2. Aplicar los filtros para encontrar el dispositivo preferido.
3. Seleccione la casilla de verificación del dispositivo.
4. En el menú desplegable **Más acciones**, haga clic en **Restablecimiento de fábrica**.  
Se muestra la ventana **Alerta**.
5. Ingrese el motivo para restablecer el cliente.
6. Haga clic en **Enviar comando**.

Identifíer	GUID-2429D1C3-F880-45F5-B19B-102BFA163295
Version	1
Status	Translation approved

## Cambiar la asignación de un grupo en la página Dispositivos

Puede cambiar la asignación de grupo de un dispositivo mediante la página **Dispositivos**.

### Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivo**.
2. Aplicar los filtros para encontrar el dispositivo preferido.
3. Seleccione la casilla de verificación del dispositivo.
4. En el menú desplegable **Más acciones**, haga clic en **Cambiar grupo**.  
Aparece la ventana **Cambiar asignación de grupo**.
5. En el menú desplegable, seleccione un nuevo grupo para el dispositivo.
6. Haga clic en **Guardar**.

Identifíer	GUID-87D5E340-F8B9-4DAB-A17A-EACE2EFDDE7A
Version	1
Status	Translation approved

## Enviar mensajes a un dispositivo

Puede enviar un mensaje a un dispositivo registrado mediante la página **Dispositivos**.

### Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivos**.
2. Aplicar los filtros para encontrar el dispositivo preferido.
3. Seleccione la casilla de verificación del dispositivo.
4. En el menú desplegable **Más acciones**, haga clic en **Enviar mensaje**.  
Aparece la ventana **Enviar mensaje**.
5. Ingrese el mensaje.
6. Haga clic en **Enviar**.

Identifíer	GUID-DDFF4F2A-8A75-43D7-9FA7-7D727D846C28
Version	1
Status	Translation approved

## Activar el dispositivo

Puede enviar un comando para activar un dispositivo si está apagado o en modo de reposo.

### Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivo**.
2. Aplicar los filtros para encontrar el dispositivo preferido.
3. Seleccione la casilla de verificación del dispositivo.
4. En el menú desplegable **Más acciones**, haga clic en **Wake on LAN**.  
Se muestra la ventana **Alerta**.
5. Haga clic en **Enviar comando**.

Identifíer	GUID-7373184A-F298-4D54-B806-9E403D48DE09
Version	1
Status	Translation approved

## Ver los detalles del dispositivo

### Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivo**.
2. Aplicar los filtros para encontrar el dispositivo preferido.  
Se muestra la lista de dispositivos preferidos.
3. Haga clic en cualquiera de los dispositivos que se muestran.  
Se muestra la página **Detalles del dispositivo**.

Identifíer	GUID-56C359AA-9E3D-4BDF-951C-36D8F13011A1
Version	1
Status	Translation approved

## Administrar el resumen del dispositivo

Para ver y administrar información sobre las notas, asignación del grupo, alertas y configuración del dispositivo mediante la página **Dispositivos**.

### Pasos

1. Haga clic en **Dispositivos**.
2. En la página **Detalles de los dispositivos**, haga clic en la pestaña **Resumen**.  
Aparece el resumen de los dispositivos.
3. En el panel derecho, haga clic en **Agregar nota**.  
Aparece la ventana **Agregar nota**.
4. Digite el mensaje en el campo correspondiente y haga clic en **Guardar**.
5. En el panel derecho, haga clic en **Cambiar asignación de grupo**.  
Aparece la ventana **Cambiar asignación de grupo**.
6. En el menú desplegable, seleccione un nuevo grupo para el dispositivo.
7. Haga clic en **Guardar**.
8. Haga clic en **Crear/Editar excepciones** para crear o editar una excepción a nivel de dispositivos y configurar una política de un dispositivo en particular en la página **Dispositivos**.

Identifíer	GUID-5D5DFED7-1BA8-463F-9836-141B6DACD8EA
Version	1
Status	Translation approved

## Ver información del sistema

### Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivo**.
2. Aplicar los filtros para encontrar el dispositivo preferido.  
Se muestra la lista de dispositivos preferidos.
3. Haga clic en cualquiera de los dispositivos que se muestran.  
Se muestra la página **Detalles del dispositivo**.
4. Haga clic en **Información del sistema**.  
Aparece la página Información del sistema.

Identifíer	GUID-F8575F61-50BA-430A-AEBC-46BB10FEF146
Version	1
Status	Translation approved

## Ver eventos del dispositivo

Puede ver y administrar información acerca de los eventos del sistema que corresponden a un dispositivo.

### Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivo**.
2. Aplicar los filtros para encontrar el dispositivo preferido.  
Se muestra la lista de dispositivos preferidos.
3. Haga clic en cualquiera de los dispositivos que se muestran.  
Se muestra la página **Detalles del dispositivo**.
4. En la página **Detalles de los dispositivos**, haga clic en la pestaña **Eventos**.  
Se muestran los eventos del dispositivo.

Identifíer	GUID-A26BA4DE-BFAA-4DB2-A24D-7BD899A05905
Version	1
Status	Translation approved

## Ver las aplicaciones instaladas

### Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivo**.
2. Aplicar los filtros para encontrar el dispositivo preferido.  
Se muestra la lista de dispositivos preferidos.
3. Haga clic en cualquiera de los dispositivos que se muestran.  
Se muestra la página **Detalles del dispositivo**.
4. Haga clic en la pestaña **Aplicaciones instaladas**.  
Se muestra la lista de las aplicaciones instaladas en el dispositivo.

Esta opción está disponible para dispositivos Windows Embedded Standard, Linux y ThinLinux. Los siguientes son los atributos que se muestran en la página:

- Nombre
- Editor
- Versión
- Instalado el



El conteo de aplicaciones instaladas aumenta o disminuye en función de la instalación o desinstalación de las aplicaciones. La lista se actualiza cuando el dispositivo se registra o se consulta a continuación.

Identifier	GUID-26F6ABCF-D5D4-4867-A368-D7F9E2FF3695
Version	1
Status	Translation approved

## Renombrar el cliente delgado

Puede usar esta página para cambiar el nombre de host de clientes esbeltos que se ejecutan en los sistemas operativos Windows Embedded Standard, ThinLinux y ThinOS.

### Pasos

1. En la página **Dispositivos**, haga clic en el dispositivo.
2. En la lista desplegable **Más opciones**, seleccione la opción **Cambiar nombre de host**.
3. Ingrese el nuevo nombre de host cuando se le indique.

**NOTA:** El nombre de host solo puede contener caracteres alfanuméricos y un guion.

4. Para dispositivos Windows Embedded Standard, la lista desplegable **Reiniciar** está en la ventana **Alerta**. Para reiniciar el sistema, seleccione la opción **Reiniciar**. Si se selecciona la opción **Reiniciar más tarde**, el dispositivo se reinicia a la hora configurada y luego se actualiza el nombre de host.

**NOTA:** No es necesario reiniciar un dispositivo ThinLinux para actualizar el nombre de host.

5. Haga clic en **Enviar comando**.  
Aparece un mensaje de confirmación.

Identifier	GUID-EB0B1DFD-FB5B-424D-9B1E-243F72787B9E
Version	1
Status	Translation approved

## Configurar la conexión de seguimiento remoto

Use esta página para permitir que los administradores globales y de grupo accedan de manera remota a las sesiones del cliente esbelto de Windows Embedded Standard, ThinLinux y ThinOS. Esta función se aplica solo a la nube privada y está disponible tanto para licencias estándar como Pro.

### Pasos

1. En la página **Dispositivos**, haga clic en el dispositivo.
2. En la lista desplegable **Más opciones**, seleccione la opción **Vigilancia remota (VNC)**.  
La dirección IP y el número de puerto del Thin client de destino se muestran en el cuadro de diálogo **Vigilancia remota (VNC)**.

**NOTA:** El número de puerto predeterminado es 5900.

3. Cambie el número de puerto del cliente esbelto de destino; opcional.
4. Haga clic en **Conectar** para iniciar una sesión remota en el Thin client de destino.

**NOTA:** El portal de Wyse Management Suite admite un máximo de cinco sesiones de vigilancia remota por inquilino.

Identifier	GUID-AEBA5841-965C-466B-BCB1-9A9D0D7B98B1
Version	1
Status	Translation approved

## Apagar dispositivos

Wyse Management Suite permite apagar dispositivos como, por ejemplo, Windows Embedded Standard, ThinLinux y clientes esbeltos de ThinOS.

### Pasos

1. Haga clic en **Dispositivos**.

Se muestra la página **Dispositivo**.

2. Aplicar los filtros para localizar el dispositivo preferido.  
Se muestra la lista de dispositivos preferidos.
3. En la lista desplegable **Más opciones**, haga clic en **Apagar ahora**.  
El comando remoto para apagar el dispositivo se envía al dispositivo seleccionado. El dispositivo responde al servidor y el comando se aplica de manera correcta.

**NOTA:** La opción **Apagar ahora** no está activada para los clientes esbeltos que se ejecutan en el sistema operativo Linux.

Identifier	GUID-9D798A7E-0810-444F-A7C3-BFD9BC0218A0
Version	1
Status	Translation approved

## Etiquetar un dispositivo

Wyse Management Suite le permite identificar un dispositivo o grupo de dispositivos mediante la opción **Dispositivo con etiqueta**.

### Pasos

1. Haga clic en **Dispositivos**.  
Se muestra la página **Dispositivo**.
2. Aplicar los filtros para localizar el dispositivo preferido.  
Se muestra la lista de dispositivos preferidos.
3. Seleccione uno o varios dispositivos. En la lista desplegable **Más opciones**, haga clic en **Dispositivo con etiqueta**.  
Se muestra la ventana de **Establecer etiqueta de dispositivo**.
4. Ingrese el nombre preferido de la etiqueta.
5. Haga clic en **Establecer etiqueta**.

Identifier	GUID-EB83F36C-AB39-4F4A-86ED-B9A8E34CBCC8
Version	1
Status	Translation approved

## Estado de cumplimiento de normas del dispositivo

De manera predeterminada, los siguientes colores se muestran como el estado del dispositivo:

- Rojo: cuando el dispositivos registrado no se ha revisado durante más de siete días.
- Gris: cuando aplica cualquier política de configuración en el dispositivo.
- Verde: cuando aplica todas las políticas de configuración en el dispositivo.

Se puede cambiar el valor predeterminado de 1 día a 99 días.

La opción **Estado en línea** se encuentra ubicada junto al nombre del dispositivo. Se muestran los siguientes colores en los estados en línea:

- Rojo: cuando el dispositivo no ha enviado su latido durante más de tres intentos.
- Gris: cuando el dispositivo no ha enviado su latido más de dos intentos, pero menos de tres intentos.
- Verde: cuando el dispositivo envía su latido con regularidad.

Identifier	GUID-77BAE5C5-F380-427B-A232-843084A7DF4F
Version	5
Status	Translation approved

## Obtener la imagen de Windows Embedded Standard o ThinLinux

### Requisitos previos

- Si utiliza el repositorio remoto de Wyse Management Suite 1.3, entonces la plantilla de extracción de recuperación/recuperación + SO no va a estar disponible en el repositorio. Debe actualizar Wyse Management Suite a la versión 1.4 o una versión posterior para acceder a las plantillas.

- Para realizar la operación de extracción de imágenes de ThinLinux, debe cerrar la ventana **Configuración** en el dispositivo ThinLinux. Debe realizar esta operación antes de extraer una imagen de SO/SO + recuperación del dispositivo ThinLinux.
- Para actualizar de ThinLinux 1.x a 2.x, el administrador debe actualizar el dispositivo con la última versión de WDA y Merlin, y luego extraer la imagen. Esta imagen extraída debe usarse para actualizar de ThinLinux 1.x a 2.x.

## Pasos

1. Vaya a la página del dispositivo **Wyse Management Suite** o **ThinLinux**.
2. Seleccione la opción **Extracción de la imagen del sistema operativo**, en la lista desplegable **Más acciones**.
3. Ingrese o seleccione los siguientes detalles:
  - **Nombre de imagen:** proporciona un nombre para la imagen. Para cambiar la imagen con un nombre similar y archivos de imagen que no están completados correctamente, haga clic en **Invaldar nombre**.
  - **Repositorio de archivos:** en la lista desplegable, seleccione el repositorio de archivos en el que está cargada la imagen. Hay dos tipos de repositorio de archivos:
    - Repositorio local
    - Repositorio de Wyse Management Suite remoto
  - **Tipo de extracción:** seleccione **Predeterminada** o **Avanzada** según sus requisitos del tipo de extracción.
    - Cuando se selecciona el tipo de extracción **Predeterminada**, se muestran las siguientes opciones:
      - Comprimir
      - SO
      - BIOS
      - Recuperación: para ThinLinux 2.x
    - Cuando se selecciona el tipo de extracción **Avanzada**, se muestra una lista desplegable para seleccionar las plantillas. Seleccione cualquier plantilla que esté disponible de manera predeterminada.

**NOTA:** Puede usar las plantillas personalizadas que se crean manualmente editando las plantillas existentes o predeterminadas.
4. Haga clic en **Prepararse para la extracción de la imagen**.

## Resultados

Cuando se envía el comando **Extraer imagen de SO**, el dispositivo del cliente recibe una solicitud para extraer la imagen del servidor. Se muestra un mensaje de solicitud para extraer la imagen en el lado del cliente. Haga clic en una de las siguientes opciones:

- **Extraer después de sysprep:** el dispositivo se reinicia e inicia sesión en el sistema operativo en un estado desactivado. Ejecute el Sysprep personalizado. Después de que se completa el sysprep personalizado, el dispositivo arranca en el sistema operativo Merlin y se realiza la operación de extracción de la imagen.

**NOTA:** Esta opción es válida para dispositivos Windows Embedded Standard.

- **Extraer ahora:** el dispositivo se inicia en el sistema operativo Merlin y se realiza la operación de extracción de la imagen.

Identifíer	GUID-32D92A7E-63F6-4585-BCCE-418331F3943E
Version	1
Status	Translation approved

# Solicitar un archivo de registro

Puede solicitar un archivo de registro de los dispositivos Windows Embedded Standard, ThinOS y ThinLinux. El dispositivo ThinOS carga los registros del sistema. El dispositivo Windows Embedded Standard carga los registros de Wyse Device Agent y los registros del visor de eventos de Windows. Linux o ThinLinux carga los registros de Wyse Device Agent y los registros del sistema.

## Requisitos previos

El dispositivo debe estar activado para extraer el archivo de registro.

## Pasos

1. Vaya a la página **Dispositivos** y haga clic en un dispositivo particular.  
Se muestran los detalles del dispositivo.
2. Haga clic en la pestaña **Registro del dispositivo**.
3. Haga clic en **Solicitar archivo de registro**.

- Después de cargar los archivos de registro en el servidor Wyse Management Suite, haga clic en el enlace **Haga clic aquí** y descargue los registros.



**NOTA:** Linux o ThinLinux cargan el archivo de registro en formato `.tar`. Si está extrayendo los archivos en un sistema Windows o ThinOS 9.x, requiere 7zip o cualquier otro archivo equivalente.

Identifier	GUID-E3FCEFC7-C5FD-461F-8B26-3E898DFC9624
Version	1
Status	Translation approved

## Solución de problemas del dispositivo

Puede ver y administrar la información de solución de problemas mediante la página **Dispositivos**.

### Pasos

- En la página **Detalles de los dispositivos**, haga clic en la pestaña **Solución de problemas**.
- Haga clic en **Solicitar captura de pantalla**.  
Puede obtener una captura de pantalla del cliente esbelto con o sin permiso del cliente. Si selecciona la casilla de verificación **Necesita aceptación del usuario**, entonces aparece un mensaje en el cliente. Esta opción solo es válida para dispositivos Windows Embedded Standard, Linux y ThinLinux.
- Haga clic en **Solicitar lista de procesos** para ver la lista de procesos que se ejecutan en el Thin client.
- Haga clic en **Solicitar lista de servicios** para ver la lista de servicios que se ejecutan en el Thin client.
- Haga clic en **Iniciar la supervisión** para acceder a la consola de métrica de rendimiento. En la consola de **Métrica de rendimiento**, se muestran los siguientes detalles:
  - Último minuto promedio de la CPU
  - Último minuto promedio de uso de la memoria

Identifier	GUID-BFA3F046-A7DC-46F1-A6C4-ECCC6B824DAF
Version	2
Status	Translation in review

## Aplicaciones y datos

En esta sección se describe cómo realizar tareas de aplicación de dispositivos de rutina, la digitalización del sistema operativo y la administración del inventario, además de establecer políticas, mediante la consola de administración de Wyse. Los nombres de los repositorios están codificados por colores para indicar el estado.

Puede configurar los siguientes tipos de políticas mediante la página **Aplicaciones y datos**:

- Política de la aplicación estándar: esta política le permite instalar un paquete de una sola aplicación.
- Política de la aplicación avanzada: esta política le permite instalar paquetes de varias aplicaciones.
- Política de imagen: esta política le permite instalar el sistema operativo.

La implementación de políticas de aplicaciones e imágenes de sistema operativo en los Thin clients se puede programar inmediatamente o para más tarde, según una zona horaria específica o según la zona horaria que está configurada en su dispositivo.

El nombre del repositorio en Wyse Management Suite se muestra como “WMS de nube de operador” para los archivos cargados por el operador en la nube pública. Además, el nombre del repositorio se muestra como “Repositorio de nube de grupos de usuarios” para el repositorio de administrador global de grupos de usuarios.

Sin embargo, para la nube privada, todos los repositorios se muestran como “Repositorio de grupos de usuarios”, el cual es el repositorio local.

The screenshot shows the 'Apps & Data' page in the Wyse Management Suite. The page has a blue header with the Dell logo and 'Wyse Management Suite' text. Below the header is a navigation menu with items: Dashboard, Groups & Configs, Devices, **Apps & Data**, Rules, Jobs, Events, Users, and Portal Administration. The main content area is titled 'Apps & Data - Thin Client App Inventory' and includes a 'Local search' input field. On the left, there are several sections: 'App Inventory' with 'Mobile' and 'Thin Client' options, 'App Policies' with 'Mobile' and 'Thin Client' options, 'OS Image Repository' with 'WES / ThinLinux', 'ThinOS', and 'ThinOS 9.x' options, 'OS Image Policies' with 'WES / ThinLinux' options, and 'File Repository' with 'Inventory' options. The main table area shows a header with columns: Name, Version, Repository Name, Size, Date Added, Notes, and Status. Below the header, it says 'No applications in the inventory.'

Ilustración 5. Página Aplicaciones y datos

### Temas:

- [Política de la aplicación](#)
- [Política de imagen](#)

- Administrar el repositorio de archivos

Identifier	GUID-8CC25343-D74E-487A-90F3-91C12AEB060B
Version	1
Status	Translation approved

## Política de la aplicación

Wyse Management Suite admite los siguientes tipos de políticas inventarios e implementación de aplicaciones:

- Configurar el inventario de aplicaciones para clientes esbeltos
- Configurar el inventario de aplicaciones para clientes esbeltos de Wyse Software
- Crear e implementar una política de aplicaciones estándar para clientes esbeltos
- Crear e implementar políticas avanzadas de la aplicación en clientes esbeltos
- Crear e implementar políticas estándar de la aplicación en clientes esbeltos de Wyse Software
- Crear e implementar políticas avanzadas de la aplicación en clientes esbeltos de Wyse Software

### Notas importantes para dispositivos basados en Windows:

- Admite la instalación de aplicaciones basadas en Windows con extensiones .msi, .exe, .msu, .msp.  
Las aplicaciones con cualquier otra extensión se descargan en %systemdrive%\wyse\WDA" Ex: "C:\wyse\WDA.
- Para implementar las aplicaciones .exe mediante el uso de Wyse Management Suite, siga el método de instalación silenciosa. Debe ingresar los parámetros silenciosos adecuados si es necesario. Por ejemplo, **VMware-Horizon-Client-4.6.1-6748947.exe/silent/install/norestart**.
- Admite implementaciones de secuencias con extensiones de archivo .bat, .cmd, .ps1 y .vbs.  
Las secuencias de comandos con cualquier otra extensión se descargan a %systemdrive%\Wyse\WDA" Ej.: "C:\Wyse\WDA.
- Cualquier script que se inserte mediante el uso de Wyse Management Suite no debe ser interactivo, lo que significa que no se requiere ninguna interacción del usuario durante la instalación.
- En la política de la aplicación avanzada, si existe una secuencia de comandos o un archivo exe que arroje un valor distinto de 0, se considerará como fallo.
- En la política de la aplicación avanzada, si la instalación previa falla, se detendrá la instalación de la aplicación.
- Cualquier archivo exe o secuencia de comandos que se inserte mediante el uso de la aplicación estándar se informará como correcto y su código de error se actualizará en el estado de trabajo.
- En el caso de aplicaciones con extensión msi, msu o msp, se informarán códigos de error estándar. Si la aplicación arroja REBOOT\_REQUIRED, el dispositivo se volverá a reiniciar una vez.

### Notas importantes para dispositivos Linux:

- Admite la instalación de aplicaciones basadas en Linux con extensiones .bin, .deb en el caso de ThinLinux 2.0 y .RPM en el caso de Linux 1.0.
- Admite implementaciones de secuencias de comandos en el caso de dispositivos ThinLinux con extensiones .sh.
- En la política de la aplicación avanzada o estándar, si existe una secuencia de comandos o un archivo deb o rpm que arroje un valor distinto de 0, se considerará como fallo.
- En la política de la aplicación avanzada, si la instalación previa falla, se detendrá la instalación de la aplicación.

Identifier	GUID-D86F754C-1ACA-4405-86B2-624D0597E43F
Version	1
Status	Translation approved

## Configurar el inventario de aplicaciones para clientes esbeltos

### Pasos

1. Haga clic en la pestaña **Aplicaciones y datos**.
2. En el panel izquierdo, vaya a **Inventario de aplicaciones > Thin Client**.  
Los detalles de la aplicación se muestran en la ventana **Inventario de Thin client**.
3. Para agregar una aplicación al inventario, ubique los archivos de la aplicación de los clientes delgados en la carpeta <repo-dir>\repository\thinClientApps.  
El repositorio de Wyse Management Suite envía periódicamente metadatos para todos los archivos al servidor Wyse Management Suite.

4. Para editar la aplicación, realice lo siguiente:
  - a. Seleccione la solución cargada en la lista.
  - b. Haga clic en **Editar aplicación**. Aparecerá la ventana **Editar aplicación**.
  - c. Ingrese la nota.
  - d. Haga clic en **Guardar**.

 **NOTA:** El sufijo global se agrega a las aplicaciones cargadas por el operador.

Las aplicaciones que están presentes en diferentes repositorios se muestran una vez. En la columna **Nombre del repositorio** aparece la cantidad de repositorios en los que está presente la aplicación. Puede colocar el cursor sobre la columna para ver el nombre de los repositorios. Además, el nombre del repositorio está codificado por colores para especificar la disponibilidad.

Identifíer	GUID-43CC8F3D-0E9D-4884-BD5F-F176903A173E
Version	1
Status	Translation approved

## Configurar el inventario de aplicaciones para clientes esbeltos de Wyse Software

### Pasos

1. Haga clic en la pestaña **Aplicaciones y datos**.
2. En el panel izquierdo, vaya a **Inventario de aplicaciones > Wyse Software Thin Client**.
3. Para agregar una aplicación al inventario, ubique los archivos de la aplicación de los clientes ligeros en la carpeta `<repo-dir>\repository\softwareTcApps`.  
El repositorio de Wyse Management Suite envía periódicamente metadatos para todos los archivos al servidor Wyse Management Suite.

Identifíer	GUID-8A9490EA-0CF1-4753-B6EA-A6D4D2D2864E
Version	1
Status	Translation approved

## Crear e implementar una política de aplicaciones estándar para clientes esbeltos

### Pasos

1. En el repositorio local, vaya a **thinClientApps** y copie la aplicación a la carpeta.
2. Vaya a **Aplicaciones y datos > Inventario de aplicaciones > Cliente esbelto** y verifique que la aplicación esté registrada en Wyse Management Suite.

 **NOTA:** La interfaz Inventario de aplicaciones demora aproximadamente dos minutos en llenar cualquier programa recientemente agregado.

3. Vaya a **Aplicaciones y datos > Política de aplicaciones > Cliente esbelto**.
4. Haga clic en **Agregar política**. Aparece la ventana **Agregar política de aplicación estándar**.
5. Ingrese el **nombre de la política**.
6. En la lista desplegable **Grupos**, seleccione el grupo.
7. En la lista desplegable **Tarea**, seleccione la tarea.
8. En el menú desplegable **Tipo de SO**, seleccione el sistema operativo.
9. Seleccione la casilla de verificación **Filtrar archivos según las extensiones** para filtrar las aplicaciones.
10. En la lista desplegable **Aplicación**, seleccione la aplicación.  
Si los archivos de la aplicación están disponibles en varios repositorios, la cantidad de repositorios se muestra junto al nombre de archivo.
11. Para implementar esta política en un sistema operativo o una plataforma en específico, seleccione **Filtro del subtipo de SO** o **Filtro de la plataforma**.

12. En la lista desplegable **Aplicar la política automáticamente**, seleccione cualquiera de las siguientes opciones:
- **No aplicar automáticamente:** esta opción no aplica automáticamente ninguna política a los dispositivos.
  - **Aplicar la política a los dispositivos nuevos:** esta opción aplica automáticamente la política a un dispositivo registrado que pertenezca a un grupo seleccionado o que se traslade a un grupo seleccionado.
  - **Aplicar la política a los dispositivos durante el registro:** esta opción se aplica automáticamente al dispositivo durante el registro.

**NOTA:** En el caso de dispositivos basados en Windows, especifique los parámetros de instalación silenciosa para los archivos .exe para ejecutar la aplicación en el modo silencioso. Por ejemplo, VMware-Horizon-Client-4.6.1-6748947.exe/silent/install/norestart.

13. Para detener el proceso de instalación después de un valor definido, especifique la cantidad de minutos en el campo **Tiempo de espera de la instalación de la aplicación**. El valor predeterminado es 60 minutos.

**NOTA:** La opción **Tiempo de espera de la instalación de la aplicación** solo se aplica a dispositivos Windows Embedded Standard, clientes esbeltos Wyse Software y dispositivos Linux y Thin Linux.

14. Haga clic en **Guardar** para crear una política.

Aparece un mensaje para permitir que el administrador programe esta política en los dispositivos según el grupo.

15. Seleccione **Sí** para programar un trabajo en la misma página.

16. Seleccione cualquiera de las opciones siguientes:

- **Inmediatamente:** el servidor ejecuta el trabajo inmediatamente.
- **En la zona horaria del dispositivo:** el servidor crea un trabajo para la zona horaria de cada dispositivo y programa el trabajo para la fecha u hora seleccionada de la zona horaria del dispositivo.
- **En la zona horaria seleccionada:** el servidor crea un trabajo para que se ejecute en la fecha y hora de la zona horaria designada.

17. Para crear el trabajo, haga clic en **Vista previa**; los programas se mostrarán en la página siguiente.

18. Puede revisar el estado del trabajo en la página **Trabajos**.

Identifíer	GUID-072AF92D-B7EA-40D5-BDB3-5BA36D1A58F9
Version	1
Status	Translation approved

## Crear e implementar una política de aplicaciones estándar para clientes esbeltos

### Pasos

1. En el repositorio local, vaya a **softwareTcApps** y copie la aplicación en la carpeta.
2. Vaya a **Aplicaciones y datos > Inventario de aplicaciones > Cliente esbelto de Wyse Software** y verifique que la aplicación esté registrada en Wyse Management Suite.

**NOTA:** La interfaz **Inventario de aplicaciones** demora aproximadamente dos minutos en llenar cualquier programa recientemente agregado.

3. Haga clic en **Agregar política**.

Aparece la ventana **Agregar política de aplicación estándar**.

4. Ingrese el **nombre de la política**.

5. En la lista desplegable **Grupos**, seleccione el grupo.

6. En la lista desplegable **Tarea**, seleccione la tarea.

7. En el menú desplegable **Tipo de SO**, seleccione el sistema operativo.

8. Seleccione la casilla de verificación **Filtrar archivos según las extensiones** para filtrar las aplicaciones.

9. En la lista desplegable **Aplicación**, seleccione la aplicación.

Si los archivos de la aplicación están disponibles en varios repositorios, la cantidad de repositorios se muestra junto al nombre de archivo.

10. Para implementar esta política en un sistema operativo o una plataforma en específico, seleccione **Filtro del subtipo de SO** o **Filtro de la plataforma**.

11. En la lista desplegable **Aplicar la política automáticamente**, seleccione cualquiera de las siguientes opciones:

- **No aplicar automáticamente:** esta opción no aplica automáticamente ninguna política a los dispositivos.

- **Aplicar la política a los dispositivos nuevos:** esta opción aplica automáticamente la política a un dispositivo registrado que pertenezca a un grupo seleccionado o que se traslade a un grupo seleccionado.
- **Aplicar la política a los dispositivos durante el registro:** esta opción se aplica automáticamente al dispositivo durante el registro.

**NOTA:** En el caso de dispositivos basados en Windows, especifique los parámetros de instalación silenciosa para los archivos .exe para ejecutar la aplicación en el modo silencioso. Por ejemplo, VMware-Horizon-Client-4.6.1-6748947.exe/silent/install/norestart.

12. Para detener el proceso de instalación después de un valor definido, especifique la cantidad de minutos en el campo **Tiempo de espera de la instalación de la aplicación**. El valor predeterminado es 60 minutos.

**NOTA:** La opción **Tiempo de espera de la instalación de la aplicación** es aplicable solo para dispositivos Windows Embedded Standard y Wyse Software Thin Clients.

13. Haga clic en **Guardar** para crear una política.

Aparece un mensaje para permitir que el administrador programe esta política en los dispositivos según el grupo.

14. Seleccione **Sí** para programar un trabajo en la misma página.

15. Seleccione cualquiera de las opciones siguientes:

- **Inmediatamente:** el servidor ejecuta el trabajo inmediatamente.
- **En la zona horaria del dispositivo:** el servidor crea un trabajo para la zona horaria de cada dispositivo y programa el trabajo para la fecha u hora seleccionada de la zona horaria del dispositivo.
- **En la zona horaria seleccionada:** el servidor crea un trabajo para que se ejecute en la fecha y hora de la zona horaria designada.

16. Para crear el trabajo, haga clic en **Vista previa**; los programas se mostrarán en la página siguiente.

17. Puede revisar el estado del trabajo en la página **Trabajos**.

Identificator	GUID-8517ED2A-D3AB-4E5D-9AC9-E815E6ED6373
Version	1
Status	Translation approved

## Habilitar el inicio de sesión único para Citrix StoreFront mediante la política de aplicación estándar

Para habilitar el inicio de sesión único para Citrix StoreFront, realice las siguientes acciones:

- **Escenario 1:** si desea habilitar el inicio de sesión único para StoreFront en la versión actual de Citrix Receiver, realice las siguientes acciones:

1. Crear e implementar una política de aplicación estándar para desinstalar Citrix Receiver con el parámetro **/silent**.
2. Crear e implementar una política de aplicación estándar para volver a instalar Citrix Receiver con el parámetro **/silent / includeSSON /AutoUpdateCheck = Disabled**.

- **Escenario 2:** si desea actualizar Citrix Receiver y habilitar el inicio de sesión único para StoreFront, realice las siguientes acciones:

1. Crear e implementar una política de aplicación estándar para actualizar Citrix Receiver con el parámetro **/silent / includeSSON /AutoUpdateCheck = Disabled**.

- **Escenario 3:** si desea cambiar a una versión anterior de Citrix Receiver y habilitar el inicio de sesión único para StoreFront, realice las siguientes acciones:

1. Crear e implementar una política de aplicación estándar para cambiar a una versión anterior de Citrix Receiver con el parámetro **/silent /includeSSON /AutoUpdateCheck = Disabled**.

Identificator	GUID-570747D0-2B54-4C48-B14A-2D8B9ABC0F96
Version	1
Status	Translation approved

## Crear e implementar políticas avanzadas de la aplicación en clientes esbeltos

### Pasos

1. Copiar la aplicación y los scripts previos/posteriores a la instalación (si fuera necesario) para implementar en los clientes delgados.

2. Guarde la aplicación y la secuencia de comandos previa/posterior a la instalación en la carpeta `thinClientApps` del repositorio local o en el repositorio de Wyse Management Suite.
3. Vaya a **Aplicaciones y datos > Inventario de aplicaciones > Cliente esbelto** y verifique que la aplicación esté registrada.
4. Vaya a **Aplicaciones y datos > Política de aplicaciones > Cliente esbelto**.
5. Haga clic en **Agregar política avanzada**. Aparece la página **Agregar política avanzada de aplicaciones**.
6. Ingrese el **nombre de la política**.
7. En la lista desplegable **Grupos**, seleccione el grupo.
8. Seleccione la casilla de verificación **Subgrupos** para aplicar la política a los subgrupos.
9. En la lista desplegable **Tarea**, seleccione la tarea.
10. En el menú desplegable **Tipo de SO**, seleccione el sistema operativo.
11. Seleccione la casilla de verificación **Filtrar archivos según las extensiones** para filtrar las aplicaciones.
12. Haga clic en **Agregar aplicación** y seleccione una o varias aplicaciones en **Aplicaciones**. Para cada aplicación, puede seleccionar el script previo y posterior a la instalación en **Previo a la instalación**, **Posterior a la instalación** y **Parámetros de instalación**.
13. Si desea que el sistema se reinicie después de instalar la aplicación correctamente, seleccione **Reiniciar**.
14. Haga clic en **Agregar aplicación** y repita el paso para agregar varias aplicaciones.

**NOTA:** Para detener la política de la aplicación en el primer fallo, seleccione **Activar dependencia de aplicación**. Si esta opción no se encuentra seleccionada, el fallo de una aplicación afectará la implementación de la política.

Si los archivos de la aplicación están disponibles en varios repositorios, la cantidad de repositorios se muestra junto al nombre de archivo.

15. Para implementar esta política en un sistema operativo o una plataforma en específico, seleccione **Filtro del subtipo de SO** o **Filtro de la plataforma**.
16. Especifique la cantidad de minutos que se debe mostrar en el cuadro de diálogo del mensaje en el cliente. Un mensaje en el cliente que le da tiempo para guardar el trabajo antes de que comience la instalación.
17. Para permitir un retraso en la implementación de la política, seleccione la casilla de verificación **Permitir retraso en la ejecución de la política**. Si se selecciona esta opción, se activarán los siguientes menús desplegados:
  - En la lista desplegable **Máx. de horas por retraso**, seleccione el máximo de horas (de 1 a 24 horas) que puede retrasar la ejecución de la política.
  - En la lista desplegable **Máx. de retrasos**, seleccione el número de veces (de 1 a 3) que puede retrasar la ejecución de la política.
18. En la lista desplegable **Aplicar la política automáticamente**, seleccione cualquiera de las siguientes opciones:
  - **No aplicar automáticamente:** esta opción no aplica automáticamente ninguna política a los dispositivos.
  - **Aplicar la política a los dispositivos nuevos:** esta opción aplica automáticamente la política a un dispositivo registrado que pertenezca a un grupo seleccionado o que se traslade a un grupo seleccionado.
  - **Aplicar la política a los dispositivos durante el registro:** esta opción se aplica automáticamente al dispositivo durante el registro.

**NOTA:** En el caso de dispositivos basados en Windows, especifique los parámetros de instalación silenciosa para los archivos `.exe` para ejecutar la aplicación en el modo silencioso. Por ejemplo, `VMware-Horizon-Client-4.6.1-6748947.exe/silent/install/norestart`.

19. Seleccione la casilla de verificación **Omitir revisión de filtro de escritura** para omitir los ciclos de filtro de escritura. Esta opción es válida para los dispositivos del sistema operativo Windows Embedded Standard y los dispositivos de clientes delgados de Wyse Software.
20. Para detener el proceso de instalación después de un valor definido, especifique la cantidad de minutos en el campo **Tiempo de espera de la instalación de la aplicación**. El valor predeterminado es 60 minutos.

**NOTA:** La opción **Tiempo de espera de la instalación de la aplicación** es aplicable solo para dispositivos Windows Embedded Standard y Wyse Software Thin Clients.

21. Haga clic en **Guardar** para crear una política. Aparece un mensaje para permitir que el administrador programe esta política en los dispositivos según el grupo.
22. Seleccione **Sí** para programar un trabajo en la misma página.
23. Seleccione cualquiera de las opciones siguientes:
  - **Inmediatamente:** el servidor ejecuta el trabajo inmediatamente.
  - **En la zona horaria del dispositivo:** el servidor crea un trabajo para la zona horaria de cada dispositivo y programa el trabajo para la fecha u hora seleccionada de la zona horaria del dispositivo.

- **En la zona horaria seleccionada:** el servidor crea un trabajo para que se ejecute en la fecha y hora de la zona horaria designada.
24. Para crear el trabajo, haga clic en **Vista previa**; los programas se mostrarán en la página siguiente.
  25. Puede revisar el estado del trabajo en la página **Trabajos**.

Identifier	GUID-A5285B7F-BEE0-4213-A202-483AC516720D
Version	1
Status	Translation approved

## Crear e implementar políticas avanzadas de la aplicación en clientes esbeltos de Wyse Software

### Pasos

1. Copiar la aplicación y los scripts previos/posteriores a la instalación (si fuera necesario) para implementar en los clientes delgados.
2. Guarde la aplicación y los scripts previos/posteriores a la instalación en la carpeta `software\TcApps` del repositorio local o en el repositorio de Wyse Management Suite.
3. Vaya a **Aplicaciones y datos > Inventario de aplicaciones > Cliente esbelto de Wyse Software** y verifique que la aplicación esté registrada.
4. Vaya a **Aplicaciones y datos > Política de aplicaciones > Cliente esbelto de Wyse Software**.
5. Haga clic en **Agregar política avanzada**. Aparece la página **Agregar política avanzada de aplicaciones**.
6. Ingrese el **nombre de la política**.
7. En la lista desplegable **Grupos**, seleccione el grupo.
8. Seleccione la casilla de verificación **Subgrupos** para aplicar la política a los subgrupos.
9. En la lista desplegable **Tarea**, seleccione la tarea.
10. En el menú desplegable **Tipo de SO**, seleccione el sistema operativo.
11. Seleccione la casilla de verificación **Filtrar archivos según las extensiones** para filtrar las aplicaciones.
12. Haga clic en **Agregar aplicación** y seleccione una o varias aplicaciones en **Aplicaciones**. Para cada aplicación, puede seleccionar el script previo y posterior a la instalación en **Previo a la instalación**, **Posterior a la instalación** y **Parámetros de instalación**.
13. Si desea que el sistema se reinicie después de instalar la aplicación correctamente, seleccione **Reiniciar**.
14. Haga clic en **Agregar aplicación** y repita el paso para agregar varias aplicaciones.

**NOTA:** Para detener la política de la aplicación en el primer fallo, seleccione **Activar dependencia de aplicación**. Si esta opción no se encuentra seleccionada, el fallo de una aplicación afectará la implementación de la política.

Si los archivos de la aplicación están disponibles en varios repositorios, la cantidad de repositorios se muestra junto al nombre de archivo.

15. Para implementar esta política en un sistema operativo o una plataforma en específico, seleccione **Filtro del subtipo de SO** o **Filtro de la plataforma**.
16. Especifique la cantidad de minutos que se debe mostrar en el cuadro de diálogo del mensaje en el cliente. Un mensaje en el cliente que le da tiempo para guardar el trabajo antes de que comience la instalación.
17. Para permitir un retraso en la implementación de la política, seleccione la casilla de verificación **Permitir retraso en la ejecución de la política**. Si se selecciona esta opción, se activarán los siguientes menús desplegables:
  - En la lista desplegable **Máx. de horas por retraso**, seleccione el máximo de horas (de 1 a 24 horas) que puede retrasar la ejecución de la política.
  - En la lista desplegable **Máx. de retrasos**, seleccione el número de veces (de 1 a 3) que puede retrasar la ejecución de la política.
18. En la lista desplegable **Aplicar la política automáticamente**, seleccione cualquiera de las siguientes opciones:
  - **No aplicar automáticamente:** esta opción no aplica automáticamente ninguna política a los dispositivos.
  - **Aplicar la política a los dispositivos nuevos:** esta opción aplica automáticamente la política a un dispositivo registrado que pertenezca a un grupo seleccionado o que se traslade a un grupo seleccionado.
  - **Aplicar la política a los dispositivos durante el registro:** esta opción se aplica automáticamente al dispositivo durante el registro.

**NOTA:** En el caso de dispositivos basados en Windows, especifique los parámetros de instalación silenciosa para los archivos `.exe` para ejecutar la aplicación en el modo silencioso. Por ejemplo, `VMware-Horizon-Client-4.6.1-6748947.exe/silent/install/norestart`.

19. Seleccione la casilla de verificación **Omitir revisión de filtro de escritura** para omitir los ciclos de filtro de escritura. Esta opción es válida para los dispositivos del sistema operativo Windows Embedded Standard y los dispositivos de clientes delgados de Wyse Software.
20. Para detener el proceso de instalación después de un valor definido, especifique la cantidad de minutos en el campo **Tiempo de espera de la instalación de la aplicación**. El valor predeterminado es 60 minutos.

**NOTA:** La opción **Tiempo de espera de la instalación de la aplicación** es aplicable solo para dispositivos Windows Embedded Standard y Wyse Software Thin Clients.

21. Haga clic en **Guardar** para crear una política.  
Aparece un mensaje para permitir que el administrador programe esta política en los dispositivos según el grupo.
22. Seleccione **Sí** para programar un trabajo en la misma página.
23. Seleccione cualquiera de las opciones siguientes:
  - **Inmediatamente:** el servidor ejecuta el trabajo inmediatamente.
  - **En la zona horaria del dispositivo:** el servidor crea un trabajo para la zona horaria de cada dispositivo y programa el trabajo para la fecha u hora seleccionada de la zona horaria del dispositivo.
  - **En la zona horaria seleccionada:** el servidor crea un trabajo para que se ejecute en la fecha y hora de la zona horaria designada.
24. Para crear el trabajo, haga clic en **Vista previa**; los programas se mostrarán en la página siguiente.
25. Puede revisar el estado del trabajo en la página **Trabajos**.

Identifíer	GUID-EAC85A84-BC2A-405C-8DDC-9548A2F324C0
Version	1
Status	Translation approved

## Política de imagen

Wyse Management Suite admite los siguientes tipos de políticas de implementación de imágenes del sistema operativo:

- Agregar imágenes del sistema operativo Windows Embedded Standard y de ThinLinux al repositorio
- Agregar el firmware de ThinOS al repositorio
- Agregar el archivo del paquete de ThinOS al repositorio
- Agregar el archivo del BIOS de ThinOS al repositorio
- Agregar el firmware de Teradici al repositorio
- Cree políticas de imagen de Windows Embedded Standard y ThinLinux.

Identifíer	GUID-37EBB456-A447-4A22-A124-7C90277401C8
Version	1
Status	Translation approved

## Agregar las imágenes del sistema operativo Windows Embedded Standard y ThinLinux al repositorio

### Requisitos previos

- Si utiliza Wyse Management Suite con implementación en la nube, vaya a **Administración del portal > Configuración de la consola > Repositorio de archivos**. Haga clic en **Descargar versión 2.0** o **Descargar versión 1.4** para descargar el archivo `WMS_Repo.exe` e instale el instalador del repositorio de Wyse Management Suite.
- Si utiliza Wyse Management Suite con una implementación local, el repositorio local se instala durante el proceso de instalación de Wyse Management Suite.

### Pasos

1. Copie las imágenes del sistema operativo Windows Embedded Standard o de ThinLinux en la carpeta `<Repository Location>\repository\osImages\zipped`.

Wyse Management Suite extrae los archivos de la carpeta comprimida y carga los archivos en la ubicación `<Repository Location>\repository\osImages\valid`. Es posible que la extracción de la imagen demore varios minutos, según sea el tamaño de la imagen.

**NOTA:** Si utiliza el sistema operativo ThinLinux, descargue la imagen de Merlin; por ejemplo, `1.0.7_3030LT_merlin.exe` y cópiela en la carpeta `<Repository Location>\Repository\osImages\zipped`.

La imagen se agregará al repositorio.

2. Vaya a **Aplicaciones y datos** > **Repositorio de imágenes de SO** > **WES/ThinLinux** para ver la imagen registrada.

Identifíer	GUID-8372D57D-B184-4B67-B6D4-4554F994E910
Version	1
Status	Translation approved

## Agregar el firmware de ThinOS al repositorio

### Pasos

1. En la pestaña **Aplicaciones y datos**, en **Repositorio de imágenes del SO**, haga clic en **ThinOS**.
2. Haga clic en **Agregar archivo de firmware**.  
Aparece la pantalla **Agregar archivo**.
3. Para seleccionar un archivo, haga clic en **Buscar** y vaya a la ubicación donde se encuentra el archivo.
4. Ingrese la descripción para el archivo.
5. Seleccione la casilla de verificación si desea invalidar un archivo existente.
6. Haga clic en **Cargar**.

**NOTA:** El archivo se agrega al repositorio cuando selecciona la casilla de verificación, pero no se asigna a ningún grupo o dispositivo. Para implementar el firmware en un dispositivo o un grupo de dispositivos, diríjase a la página de configuración del dispositivo o del grupo correspondiente.

Identifíer	GUID-4200AFC1-1FB4-42CA-957C-B34F6143CF46
Version	1
Status	Translation approved

## Agregar el archivo del BIOS de ThinOS al repositorio

### Pasos

1. En la pestaña **Aplicaciones y datos**, en **Repositorio de imágenes del SO**, haga clic en **ThinOS**.
2. Haga clic en **Agregar archivo de BIOS**.  
Aparece la pantalla **Agregar archivo**.
3. Para seleccionar un archivo, haga clic en **Buscar** y vaya a la ubicación donde se encuentra el archivo.
4. Ingrese la descripción para el archivo.
5. Seleccione la casilla de verificación si desea invalidar un archivo existente.
6. Seleccione la plataforma de la lista desplegable Tipo de plataforma del BIOS.
7. Haga clic en **Cargar**.

**NOTA:** El archivo se agrega al repositorio cuando selecciona la casilla de verificación, pero no se asigna a ningún grupo o dispositivo. Para implementar el archivo de BIOS en un dispositivo o un grupo de dispositivos, diríjase a la página de configuración del dispositivo o grupo correspondiente.

Identifíer	GUID-4BE1194D-2C3B-4471-B126-5D312C41A1FD
Version	1
Status	Translation approved

## Agregar el archivo del paquete de ThinOS al repositorio

### Pasos

1. En la pestaña **Aplicaciones y datos**, en **Repositorio de imágenes del SO**, haga clic en **ThinOS**.
2. Haga clic en **Agregar archivo de paquete**.  
Aparece la pantalla **Agregar archivo**.
3. Para seleccionar un archivo, haga clic en **Buscar** y vaya a la ubicación donde se encuentra el archivo.
4. Ingrese la descripción para el archivo.
5. Haga clic en **Cargar**.

**NOTA:** Si la aplicación ya existe en el repositorio público, la referencia de la aplicación se agrega al inventario. De lo contrario, la aplicación se carga en el repositorio público y la referencia se agrega al inventario. Además, los administradores de grupos de usuarios no pueden eliminar los paquetes de firmware y BIOS de ThinOS cargados por el operador.

Identifíer	GUID-41267E9E-2300-4F22-B014-69059BA22418
Version	1
Status	Translation approved

## Agregar el firmware de ThinOS 9.x al repositorio

### Pasos

1. En la pestaña **Aplicaciones y datos**, en **Repositorio de imágenes del SO**, haga clic en **ThinOS 9.x**.
2. Haga clic en **Agregar archivo de firmware**. Aparece la pantalla **Agregar archivo**.
3. Para seleccionar un archivo, haga clic en **Buscar** y vaya a la ubicación donde se encuentra el archivo.
4. Ingrese la descripción para el archivo.
5. Seleccione la casilla de verificación si desea invalidar un archivo existente.
6. Haga clic en **Cargar**.

**NOTA:** El archivo se agrega al repositorio cuando selecciona la casilla de verificación, pero no se asigna a ningún grupo o dispositivo. Para implementar el firmware en un dispositivo o un grupo de dispositivos, diríjase a la página de configuración del dispositivo o del grupo correspondiente.

Identifíer	GUID-8CB2ACA1-05D1-4E18-9BE9-575CC73436FB
Version	1
Status	Translation approved

## Agregar el archivo del paquete de ThinOS 9.x al repositorio

### Pasos

1. En la pestaña **Aplicaciones y datos**, en **Repositorio de imágenes del SO**, haga clic en **ThinOS 9.x**.
2. Haga clic en **Agregar archivo de paquete**. Aparece la pantalla **Agregar archivo**.
3. Para seleccionar un archivo, haga clic en **Buscar** y vaya a la ubicación donde se encuentra el archivo.
4. Ingrese la descripción para el archivo.
5. Haga clic en **Cargar**.

**NOTA:** Si la aplicación ya existe en el repositorio público, la referencia de la aplicación se agrega al inventario. De lo contrario, la aplicación se carga en el repositorio público y la referencia se agrega al inventario. Además, los administradores de grupos de usuarios no pueden eliminar los paquetes de firmware y BIOS de ThinOS cargados por el operador.

Identifíer	GUID-31C11834-63FA-4A1C-88B9-9B4C59FD196A
Version	1
Status	Translation approved

## Crear políticas de imagen de Windows Embedded Standard y ThinLinux

### Pasos

1. En la pestaña **Aplicaciones y datos**, en **Políticas de imagen del SO**, haga clic en **WES/ThinLinux**.
2. Haga clic en **Agregar política**.

Aparecerá la pantalla **Agregar política WES/ThinLinux**.

3. En la página **Agregar política WES/ThinLinux**, haga lo siguiente:
  - a. Ingrese un **Nombre de la política**.
  - b. En el menú desplegable **Grupo**, seleccione un grupo.
  - c. En el menú desplegable **Tipo de SO**, seleccione el tipo de SO.
  - d. En el menú desplegable **Filtro de subtipo de SO**, seleccione el filtro del subtipo de SO.
  - e. Si desea implementar una imagen en un sistema operativo o en una plataforma en particular, seleccione **Filtro del subtipo de SO** o **Filtro de la plataforma**.
  - f. En el menú desplegable **Imagen del SO**, seleccione un archivo de imagen.
  - g. En el menú desplegable **Regla**, seleccione cualquiera de las siguientes reglas que desee establecer para la política de imagen:
    - Solo actualizar
    - Permitir degradación
    - Forzar esta versión.
  - h. En el menú desplegable **Aplicar política automáticamente**, seleccione una de las siguientes opciones:
    - No aplicar automáticamente: la política de imagen no se aplica automáticamente en un dispositivo registrado con Wyse Management Suite.
    - Aplicar la política a nuevos dispositivos: la política de imagen se aplica en un nuevo dispositivo registrado con Wyse Management Suite.
    - Aplicar la política a los dispositivos durante el registro: la política de imagen se aplica durante el registro en un nuevo dispositivo que está registrado con Wyse Management Suite.
4. Haga clic en **Guardar**.

Identifier	GUID-CFC6D03C-CF81-4B22-A3F0-54DAAB0CD5A8
Version	1
Status	Translation approved

## Administrar el repositorio de archivos

Esta sección le permite ver y administrar los inventarios del repositorio de archivos, como el fondo de pantalla, el logotipo, el archivo de texto del EULA, el perfil inalámbrico de Windows y los archivos de certificado.

### Pasos

1. En la pestaña **Aplicaciones y datos**, en **Repositorio de archivos**, haga clic en **Inventario**.
2. Haga clic en **Agregar archivo**.

Aparece la pantalla **Agregar archivo**.
3. Para seleccionar un archivo, haga clic en **Buscar** y vaya a la ubicación donde se encuentra el archivo.
4. En el menú desplegable **Tipo**, seleccione cualquiera de las siguientes opciones que se ajuste a su tipo de archivo:
  - Certificado
  - Fondo de pantalla
  - Logotipo
  - Archivo de texto de CLUF
  - Perfil inalámbrico de Windows
  - Archivo INI
  - Configuración regional
  - Asignaciones de impresora
  - Fuentes
  - Hosts
  - Reglas

**NOTA:** Para ver el tamaño máximo y el formato compatible de los archivos que puede cargar, haga clic en el ícono de información (i).

5. Seleccione la casilla de verificación si desea invalidar un archivo existente.

**NOTA:** El archivo se agrega al repositorio cuando selecciona la casilla de verificación, pero no se asigna a ningún grupo o dispositivo. Para asignar el archivo, vaya a la página de configuración de dispositivo correspondiente.

6. Haga clic en **Cargar**.

# Cómo cambiar el fondo de pantalla para todos los dispositivos que pertenecen al grupo de publicidad

## Pasos

1. Vaya a la pestaña **Aplicaciones y datos**.
2. En la barra de navegación en el panel izquierdo, seleccione **Inventario**.
3. Haga clic en el botón **Agregar archivo**.
4. Busque y seleccione la imagen que desea usar como fondo de pantalla.
5. Para el tipo, seleccione **Fondo de pantalla**.
6. Ingrese la descripción y haga clic en **Cargar**.

Para cambiar la política de configuración de un grupo asignando un nuevo fondo de pantalla, haga lo siguiente:

1. Vaya a la página **Grupos y configuraciones**.
2. Seleccione un grupo de políticas.
3. Haga clic en **Editar políticas** y seleccione **WES**.
4. Seleccione **Experiencia del escritorio** y haga clic en **Configurar este elemento**.
5. Seleccione **Fondo de escritorio**.
6. En el menú desplegable, seleccione el archivo de fondo de pantalla.
7. Haga clic en **Guardar y publicar**.

Haga clic en **Trabajos** para revisar el estado de la política de configuración. Puede hacer clic en el número al lado de la marca del estado en la columna **Detalles** para revisar los dispositivos con su estado.

Identificier	GUID-9999BDF9-DC4C-4039-9258-D4F545D0F2A0
Version	1
Status	Translation approved

## Administrar reglas

En esta sección se describe cómo agregar y administrar las reglas en la consola Wyse Management Suite. Se indican las siguientes opciones de filtro:

- **Registro**
- **Asignación automática del dispositivo sin administrar**
- **Notificación de alerta**

Rules — Registration

Type

Registration

Unmanaged Device Auto Assignment

Alert Notification

Edit Rule

Enabled	Rule Type	Condition	Auto Resolution	Group	Target	Notification
<input checked="" type="checkbox"/>	Unmanaged Devices	unregister after 30 days	Force Unregister	Unmanaged Group	Group Based Devices	Daily to Global Admin Only

Ilustración 6. Página Reglas

### Temas:



- Editar una regla de registro
- Crear reglas de asignación automática para dispositivos no administrados
- Editar la regla de asignación automática de un dispositivo no administrado
- Deshabilitar y eliminar una regla para la asignación automática de un dispositivo no administrado
- Guardar el orden de las reglas
- Agregar una regla para la notificación de alertas
- Editar una regla de notificación de alertas

Identifíer	GUID-DE31BE6A-5084-4055-9332-2567CC6F5971
Version	1
Status	Translation approved

## Editar una regla de registro

Configure las reglas para dispositivos sin administrar mediante la opción **Registro**.


### Pasos

- Haga clic en **Reglas**.  
Aparece la página **Reglas**.
- Haga clic en **Registro** y seleccione la opción Dispositivos no administrados.
- Haga clic en **Editar regla**.  
Aparece la ventana **Editar regla**.  
Puede ver los siguientes detalles:
  - Regla
  - Descripción
  - Destino del dispositivo
  - Grupo
- En el menú desplegable, seleccione un cliente de destino para aplicar la opción **Destino de notificaciones** y la duración para aplicar la opción **Frecuencia de notificaciones**.  
 **NOTA:** La frecuencia de notificaciones se puede configurar para cada 4 horas, cada 12 horas, diariamente o semanalmente al dispositivo de destino.
- Ingrese el número de días que faltan hasta que desee aplicar la regla en la casilla **Aplicar la regla después (de 1 a 30 días)**.  
 **NOTA:** De manera predeterminada, el registro de los dispositivos no administrados se anula después de 30 días.
- Haga clic en **Guardar**.

Identifíer	GUID-F274FAA7-BFBD-4631-8DD7-0BDE7CEF9C59
Version	1
Status	Translation approved

## Crear reglas de asignación automática para dispositivos no administrados

### Pasos

- Haga clic en la pestaña **Reglas**.
- Seleccione la opción **Asignación automática del dispositivo sin administrar**.
- Haga clic en la pestaña **Agregar reglas**.
- Ingrese el **Nombre** y seleccione el **Grupo de destino**.
- Haga clic en la opción **Agregar condición** y seleccione las condiciones para las reglas asignadas.
- Haga clic en **Guardar**.  
La regla se muestra en la lista de grupos no administrados. Esta regla se aplica automáticamente y el dispositivo se detalla en el grupo de destino.  
 **NOTA:** Las reglas no se aplican a los dispositivos con el estado **Inscripción pendiente**.

Identifíer	GUID-8767529F-B51F-422D-828D-A9C546AA0778
Version	1
Status	Translation approved

## Editar la regla de asignación automática de un dispositivo no administrado

### Pasos

1. Haga clic en la pestaña **Reglas**.
2. Seleccione la opción **Asignación automática del dispositivo sin administrar**.
3. Seleccione la regla y haga clic en la opción **Editar**.
4. Ingrese el **Nombre** y seleccione el **Grupo de destino**.
5. Haga clic en la opción **Agregar condición** y seleccione las condiciones para las reglas asignadas.
6. Haga clic en **Guardar**.

Identifíer	GUID-6BF7895E-4DC1-4C3B-BC34-50A7EFF39608
Version	1
Status	Translation approved

## Deshabilitar y eliminar una regla para la asignación automática de un dispositivo no administrado

### Pasos

1. Haga clic en la pestaña **Reglas**.
2. Seleccione la opción **Asignación automática del dispositivo sin administrar**.
3. Seleccione la regla y haga clic en la opción **Desactivar regla**.  
La regla seleccionada está desactivada.
4. Seleccione la regla desactivada y haga clic en la opción **Eliminar reglas desactivadas**.  
Se eliminó la regla.

Identifíer	GUID-4334C016-2A04-4E3B-8724-FB5F60F2B6E7
Version	1
Status	Translation approved

## Guardar el orden de las reglas

### Requisitos previos

Si hay varias reglas presentes, puede cambiar el orden de una regla que se aplica en los dispositivos.

### Pasos

1. Haga clic en la pestaña **Reglas**.
2. Seleccione la opción **Asignación automática del dispositivo sin administrar**.
3. Seleccione la regla que desee mover y luego muévala al orden superior.
4. Haga clic en **Guardar orden de las reglas**.

 **NOTA:** No puede cambiar el orden de las reglas de prefijo de IPV6.

Identifier	GUID-42E70D67-D8F8-4B02-9D62-A3F3C89B7171
Version	1
Status	Translation approved

## Agregar una regla para la notificación de alertas

### Pasos

1. Haga clic en la pestaña **Reglas**.
2. Seleccione la opción **Notificación de alertas**.
3. Haga clic en **Agregar regla**.  
Aparece la ventana **Agregar regla**.
4. En la lista desplegable **Regla**, seleccione una regla.
5. Ingrese la **Descripción**.
6. En la lista desplegable **Grupo**, seleccione la opción preferida.
7. En el menú desplegable, seleccione un dispositivo de destino para aplicar el **Destino de notificaciones** y la duración para aplicar la **Frecuencia de notificaciones**.
8. Haga clic en **Guardar**.

Identifier	GUID-07395704-FA0A-44A9-840A-45C8475CCEE91
Version	1
Status	Translation approved

## Editar una regla de notificación de alertas

### Pasos

1. Haga clic en la pestaña **Reglas**.
2. Seleccione la opción **Notificación de alertas**.
3. Haga clic en **Editar regla**.  
Aparece una ventana **Editar regla**.
4. En la lista desplegable **Regla**, seleccione una regla.
5. Ingrese la **Descripción**.
6. En la lista desplegable **Grupos**, seleccione un grupo.
7. En la lista desplegable, seleccione un dispositivo de destino para aplicar el **destino de notificaciones** y la duración para aplicar la **frecuencia de notificaciones**.
8. Haga clic en **Guardar**.

Identifier	GUID-83681290-E92B-47E4-B7F1-B2F0FFAFCE1A
Version	1
Status	Translation approved

## Administración de trabajos

En esta sección se describe cómo programar y administrar trabajos en la consola de administración.

En esta página puede ver trabajos según las siguientes opciones de filtros:

- **Grupos de configuración:** en el menú desplegable, seleccione el tipo de grupo de configuración.
- **Programado por:** en el menú desplegable, seleccione un programador que realiza la actividad de programación. Las opciones posibles son:
  - Administrador
    - Política de aplicación
    - Política de imagen
    - Comandos del dispositivo
  - Sistema
    - Publicar configuración de grupo
    - Otros
- **Tipo de SO:** en el menú desplegable, seleccione el sistema operativo. Las opciones posibles son:
  - ThinOS
  - WES
  - Linux
  - Thin Linux
  - Wyse Software Thin Client
- **Estado:** en el menú desplegable, seleccione el estado del trabajo. Las opciones posibles son:
  - Programado
  - En ejecución/en curso
  - Completo
  - Cancelado
  - En error
- **Estado detallado:** en el menú desplegable, seleccione el estado en detalle. Las opciones posibles son:
  - 1 o más con error
  - 1 o más pendientes
  - 1 o más en curso
  - 1 o más cancelados
  - 1 o más completados
- **Más acciones:** en el menú desplegable, seleccione la opción **Sincronizar contraseña del BIOS del administrador**. Se muestra la ventana Trabajo de sincronización de la contraseña del administrador del BIOS.

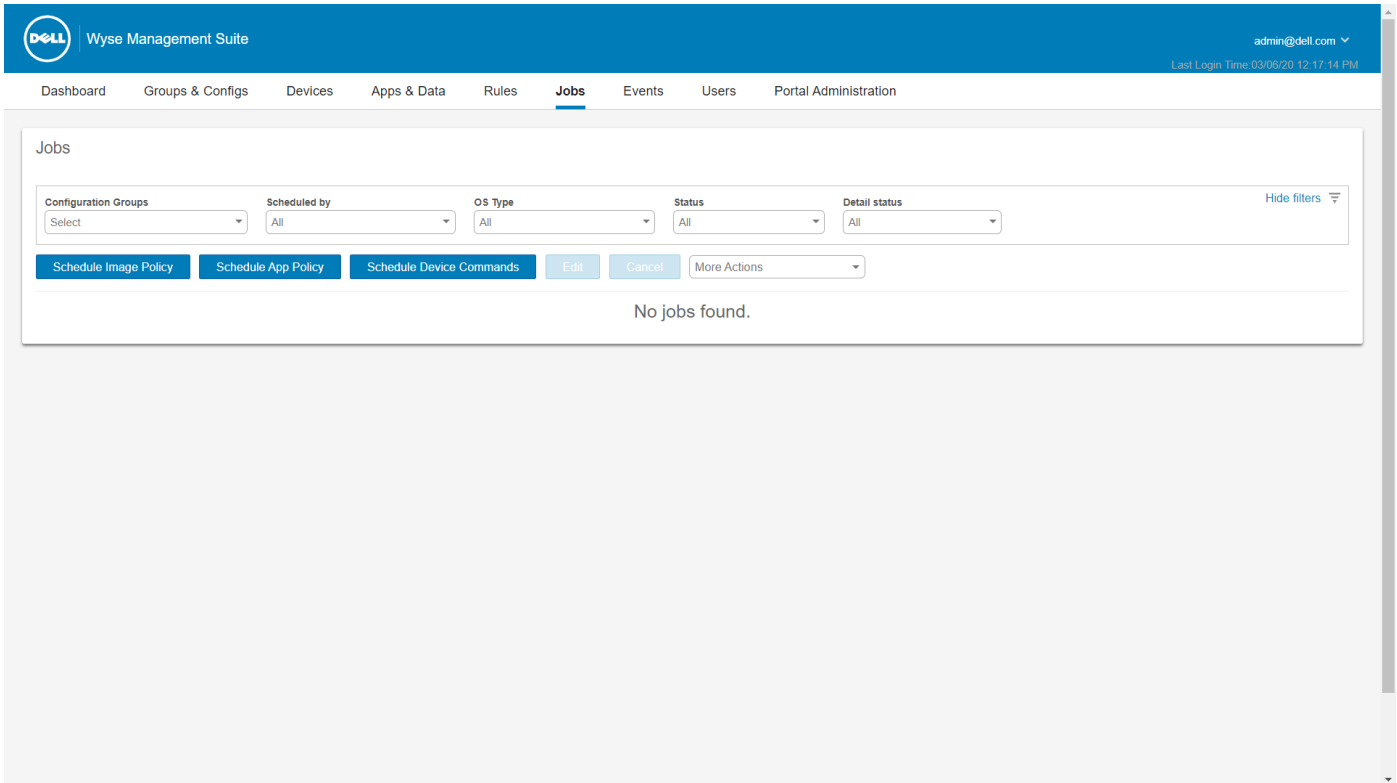


Ilustración 7. Página Trabajos

**Temas:**

- Sincronizar contraseña del BIOS del administrador
- Buscar un trabajo programado utilizando filtros
- Programar un trabajo de comandos del dispositivo
- Programar la política de imágenes
- Programar una política de aplicaciones

Identifier	GUID-92BBB2B9-96C0-4CB4-BCA2-37866E2C0CF8
Version	1
Status	Translation approved

# Sincronizar contraseña del BIOS del administrador

**Pasos**

1. Haga clic en **Trabajos**.  
Aparece la página **Trabajos**.
2. En el menú desplegable **Más acciones**, seleccione la opción **Sincronizar la contraseña del administrador del BIOS**.  
Se muestra la ventana **Trabajo de sincronización de la contraseña del administrador del BIOS**.
3. Introduzca la contraseña. La contraseña debe tener entre 4 y 32 caracteres.
4. Seleccione la casilla de verificación **Mostrar la contraseña** para ver la contraseña.
5. En el menú desplegable **Tipo de SO**, seleccione su opción preferida.
6. En el menú desplegable **Plataforma**, seleccione su opción preferida.
7. Ingrese el nombre del trabajo.
8. En el menú desplegable **Grupo**, seleccione su opción preferida.
9. Seleccione la casilla de verificación **Incluir todos los subgrupos** para incluir los subgrupos.
10. Ingrese la descripción en el cuadro **Descripción**.
11. Haga clic en **Vista previa**.

Identifíer	GUID-401002D9-C486-4560-87C8-8C6BD61207A0
Version	1
Status	Translation approved

# Buscar un trabajo programado utilizando filtros

En esta sección se describe cómo buscar un trabajo programado y administrar trabajos en la consola de administración.

## Pasos

1. Haga clic en **Trabajos**.  
Aparece la página **Trabajos**.
2. En el menú desplegable **Grupos de configuración**, seleccione el grupo de política predeterminada o los grupos que agrega un administrador.
3. En el menú desplegable **Programado por**, seleccione un programador que realiza la actividad de programación.  
Las opciones posibles son:
  - Administrador
    - Política de aplicación
    - Política de imagen
    - Comandos del dispositivo
  - Sistema
    - Publicar configuración de grupo
    - Otros
4. En el menú desplegable **Tipo de SO**, seleccione el sistema operativo.  
Las opciones posibles son:
  - ThinOS
  - WES
  - Linux
  - Thin Linux
  - Wyse Software Thin Client
  - Teradici; nube privada
5. En el menú desplegable **Estado**, seleccione el estado del trabajo.  
Las opciones posibles son:
  - Programado
  - En ejecución/en curso
  - Completo
  - Cancelado
  - En error
6. En el menú desplegable **Estado detallado**, seleccione el estado en detalle.  
Las opciones posibles son:
  - 1 o más con error
  - 1 o más pendientes
  - 1 o más en curso
  - 1 o más cancelados
  - 1 o más completados
7. En el menú desplegable **Más acciones**, seleccione la opción **Sincronizar la contraseña del administrador del BIOS**.  
Se muestra la ventana **Trabajo de sincronización de la contraseña del administrador del BIOS**. Para obtener más información, consulte [Sincronizar la contraseña del administrador del BIOS](#).

Identifíer	GUID-9438DCB8-3834-4E59-B1D7-AA038FCD9C39
Version	2
Status	Translation approved

## Programar un trabajo de comandos del dispositivo

### Pasos

1. En la página **Trabajos**, haga clic en la opción **Programar el trabajo de comandos del dispositivo**. Se muestra la pantalla **Trabajo de comandos del dispositivo**.
2. En la lista desplegable **Comando**, seleccione un comando. Las opciones posibles son:
  - Reiniciar
  - Wake on LAN
  - Apagar
  - Consulta

El comando del dispositivo es un trabajo recurrente. En días de la semana determinados y a una hora específica, los comandos se envían a los dispositivos seleccionados.

3. En la lista desplegable, seleccione el tipo de sistema operativo.
4. Ingrese el nombre del trabajo.
5. En la lista desplegable, seleccione un nombre de grupo.
6. Ingrese la descripción del trabajo.
7. En la lista desplegable, seleccione la hora o la fecha.
8. Especifique/seleccione los siguientes detalles:
  - **Efectivo**: ingrese la fecha de inicio y de término.
  - **Iniciar entre**: ingrese la hora de inicio y de término.
  - **Los días**: seleccione los días de la semana.
9. Haga clic en la opción **Vista previa** para ver los detalles del trabajo programado.
10. En la página siguiente, haga clic en la opción **Programa** para iniciar el trabajo.

Identifíer	GUID-680934DE-869E-4945-A9F1-D266809B465A
Version	1
Status	Translation approved

## Programar la política de imágenes

La política de la imagen no es un trabajo recurrente. Cada comando es específico de un dispositivo.

### Pasos

1. En la página **Trabajos**, haga clic en la opción **Programar política de imagen**. Se muestra la pantalla **Trabajo de actualización de imagen**.
2. En la lista desplegable, seleccione una política.
3. Ingrese la descripción del trabajo.
4. En la lista desplegable, seleccione la hora o la fecha.
5. Especifique/seleccione los siguientes detalles:
  - **Efectivo**: ingrese la fecha de inicio y de término.
  - **Iniciar entre**: ingrese la hora de inicio y de término.
  - **Los días**: seleccione los días de la semana.
6. Haga clic en la opción **Vista previa** para ver los detalles del trabajo programado.
7. Haga clic en la opción **Programar** para iniciar el trabajo.

Identifíer	GUID-0F75B300-954B-4E19-ADD9-F9692746B258
Version	1
Status	Translation approved

# Programar una política de aplicaciones

La política de la aplicación no es un trabajo recurrente. Cada comando es específico de un dispositivo.

## Pasos

1. En la página **Trabajos**, haga clic en la opción **Programar política de la aplicación**.  
Se muestra la pantalla **Trabajo de la política de aplicaciones**.
2. En la lista desplegable, seleccione una política.
3. Ingrese la descripción del trabajo.
4. En la lista desplegable, seleccione la hora o la fecha.
5. Especifique/seleccione los siguientes detalles:
  - **Efectivo**: ingrese la fecha de inicio y de término.
  - **Iniciar entre**: ingrese la hora de inicio y de término.
  - **Los días**: seleccione los días de la semana.
6. Haga clic en la opción **Vista previa** para ver los detalles del trabajo programado.
7. En la página siguiente, haga clic en la opción **Programa** para iniciar el trabajo.

Identifíer	GUID-73D73337-2290-4DD2-A784-D9E381BD250A
Version	1
Status	Translation approved

## Administración de eventos

En la página **Eventos**, puede ver todos los eventos y alertas que hay en el sistema de administración mediante la consola de administración. También se entregan instrucciones sobre cómo ver una auditoría de eventos y alertas para fines de auditorías del sistema.

Se usa un resumen de eventos y alertas para obtener un resumen diario fácil de leer de lo que ha ocurrido en el sistema. La ventana **Auditoría** ordena la información en una vista típica de registros de auditoría. Puede ver la marca de hora, el tipo de evento, la fuente y la descripción de cada evento en orden de hora.

The screenshot shows the 'Events' page in the Wyse Management Suite. The top navigation bar includes 'Dashboard', 'Groups & Confgs', 'Devices', 'Apps & Data', 'Rules', 'Jobs', 'Events', 'Users', and 'Portal Administration'. The 'Events' tab is active. Below the navigation bar, there is a header for 'Events & Alerts' with a '0' indicator. There are two tabs: 'Summary' and 'Audit'. Below the tabs, there are four filter dropdowns: 'Configuration Groups' (Select), 'Events or Alerts' (Events), 'Timeframe' (Select), and 'Event Type' (Select). There is also a 'Hide filters' link. The main content area displays 'No Events'.

Ilustración 8. Página Eventos

### Temas:

- [Buscar un evento o una alerta utilizando filtros](#)
- [Ver el resumen de eventos](#)
- [Ver el registro de la auditoría](#)

Identifíer	GUID-8FFF75BE-778A-4D31-9150-20450FC73757
Version	2
Status	Translation approved

## Buscar un evento o una alerta utilizando filtros

### Pasos

1. Haga clic en **Eventos**.

Se muestra la página **Eventos**.

- En el menú desplegable **Grupos de configuración**, seleccione el grupo de política predeterminada o los grupos que agrega un administrador.
- En el menú desplegable **Eventos o alertas**, seleccione una de las siguientes opciones:
  - Eventos
  - Alertas actuales
  - Historial de alertas
- En la lista desplegable **Período**, seleccione uno de los siguientes sistemas operativos:  
Esta opción le permite ver los eventos que se produjeron en un período determinado. Las opciones disponibles en el menú desplegable son:
  - Hoy
  - Ayer
  - Esta semana
  - Personalizada
- En el menú desplegable **Tipo de evento**, seleccione el sistema operativo.  
Todos los eventos se clasifican en grupos particulares. Las opciones disponibles en el menú desplegable son:
  - Acceso
  - Registro
  - Configuración
  - Comandos remotos
  - Administración
  - Cumplimiento

Identifíer	GUID-EA17162B-CC8E-4932-986F-638C5C2E814A
Version	1
Status	Translation approved

## Ver el resumen de eventos

La ventana **Eventos y alertas** muestra todos los eventos y las alertas que han ocurrido en el sistema. Vaya a **Eventos > Resumen**.

Identifíer	GUID-2BB6AE63-1D96-45CF-A122-FE92D9F71B61
Version	1
Status	Translation approved

## Ver el registro de la auditoría

La ventana **Auditoría** ordena la información en una vista típica de registros de auditoría. Puede ver la marca de hora, el tipo de evento, la fuente y la descripción de cada evento en orden de hora.

### Pasos

- Vaya a **Eventos > Auditoría**.
- En la lista desplegable **Grupos de configuración**, seleccione un grupo para el cual desee ver un registro de auditoría.
- En la lista desplegable **Período**, seleccione el período para ver los eventos que ocurrieron durante ese tiempo.

 **NOTA:** Los archivos de auditoría no están traducidos y están disponibles solo en inglés.

Identifier	GUID-5674BCC4-EF17-4429-A09C-06A10B150082
Version	1
Status	Translation approved

## Administrar usuarios

En esta sección se describe cómo realizar una tarea de rutina de administración de usuarios en la consola de administración. A continuación se indican los dos tipos de usuario:

- **Administradores:** el administrador de Wyse Management Suite puede recibir el rol de administrador global, administrador de grupo o visor.
  - Un administrador global tiene acceso a todas las funciones de Wyse Management Suite.
  - Un administrador de grupo tiene acceso a todas las propiedades y funciones para grupos específicos que estén asignados a él.
  - Un visor tiene solo acceso de lectura a todos los datos y puede recibir permisos para activar comandos en tiempo real específicos, como el apagado o el reinicio.

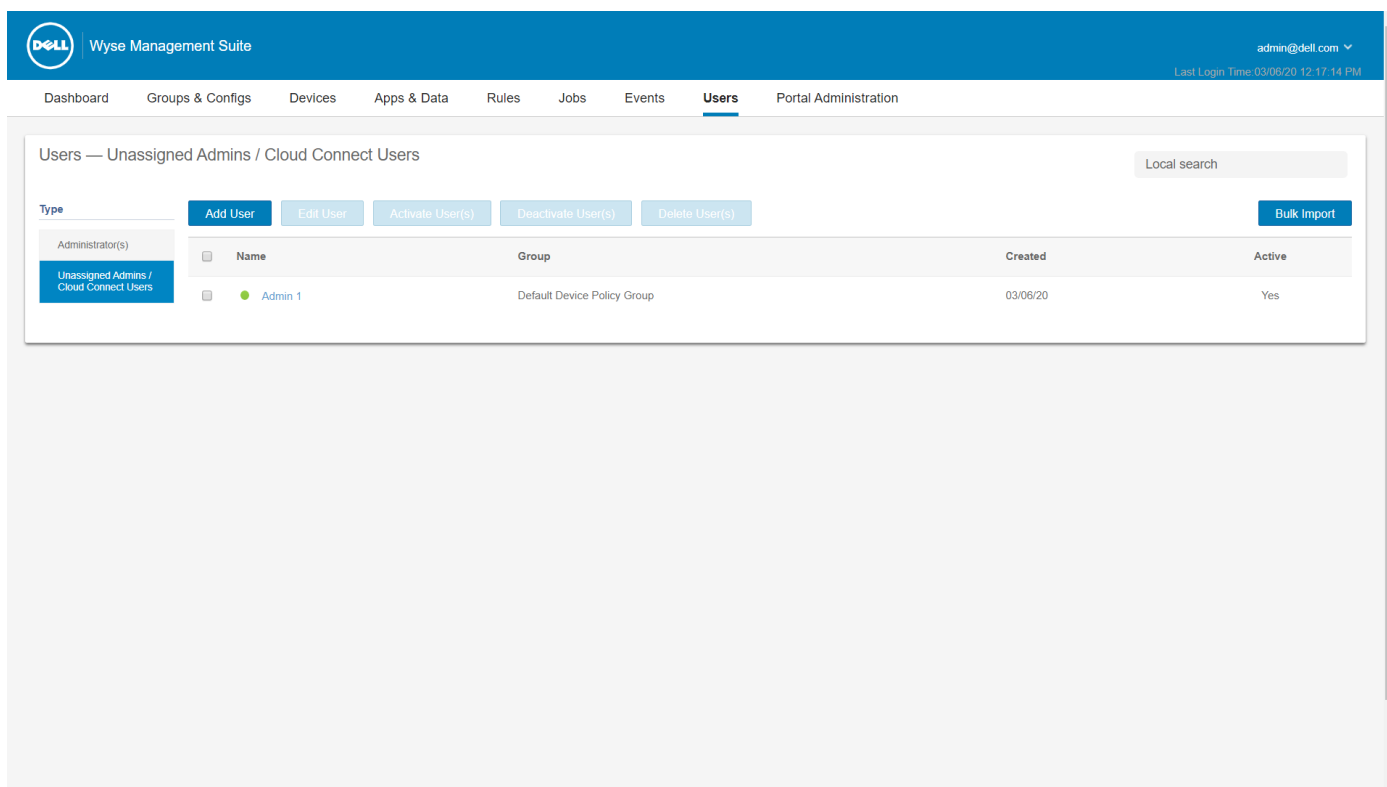
Si selecciona administrador, puede realizar cualquiera de las siguientes acciones:

- Agregar administrador
- Editar administrador
- Activar administradores
- Desactivar administradores
- Eliminar administradores
- Desbloquear administradores
- **Administradores sin asignar:** los usuarios importados del servidor AD se muestran en la página **Administradores sin asignar**. Posteriormente podrá asignar un rol a estos usuarios desde el portal.

Para una mejor y más rápida administración de los usuarios, seleccione los usuarios de su preferencia según las opciones de archivos disponibles. Si selecciona **Usuarios sin administrar**, puede realizar cualquiera de las siguientes acciones:

- Editar usuario
- Activar usuarios
- Desactivar usuarios
- Eliminar usuarios

 **NOTA:** Para importar usuarios desde el archivo .CSV, haga clic en **Importación masiva**.



**Ilustración 9. Página Usuarios**

**Temas:**

- [Agregar un nuevo perfil de administrador](#)
- [Crear reglas de asignación automática para dispositivos no administrados](#)
- [Editar un perfil de administrador](#)
- [Agregar un usuario final](#)
- [Editar un usuario final](#)
- [Crear excepciones de usuario final](#)
- [Importación masiva de usuarios finales](#)
- [Eliminar un usuario final](#)
- [Desactivar un perfil de administrador](#)
- [Eliminar un perfil de administrador](#)
- [Editar un perfil de usuario](#)
- [Importación masiva de administradores no asignados o usuarios de Cloud Connect](#)

Identifier	GUID-5777F5AD-C1B1-49D6-85AE-ACD5BD66ECA2
Version	1
Status	Translation approved

## Agregar un nuevo perfil de administrador

**Pasos**

1. Haga clic en **Usuarios**.
2. Haga clic en **Administradores**.
3. Haga clic en **Agregar administrador**.  
Aparece la ventana **Nuevo usuario administrador**.
4. Escriba su ID de correo electrónico y nombre de usuario en los campos respectivos.
5. Seleccione la casilla de verificación para usar el mismo nombre de usuario que se indica en el correo electrónico.
6. Realice uno de los siguientes pasos:

- Si hace clic en la pestaña **Información personal**, ingrese los siguientes detalles:
  - Nombre
  - Apellido
  - Título
  - Número de teléfono móvil
- Si hace clic en la pestaña **Roles**, ingrese los siguientes detalles:

- a. En la sección **Roles**, en la lista desplegable **Rol**, seleccione el **Rol del administrador**.
  - Administrador global
  - Administrador de grupo
  - Lector

**NOTA:** Si selecciona Función de administrador como Visor, se muestran las siguientes tareas administrativas:

- Consultar dispositivo
- Cancelar registro del dispositivo
- Reiniciar/Apagar dispositivo
- Cambiar asignación de grupo
- Vigilancia remota
- Bloquear dispositivo
- Borrar dispositivo
- Enviar mensaje
- Dispositivo WOL

- b. En la sección **Contraseña**, haga lo siguiente:
  - i. Ingrese la contraseña personalizada.
  - ii. Para generara cualquier contraseña aleatoria, seleccione el botón de selección **Generar contraseña aleatoria**.

7. Haga clic en **Guardar**.

Identifier	GUID-3EDD71BC-E04A-478E-BA14-1C760F11ACD5
Version	1
Status	Translation approved

## Crear reglas de asignación automática para dispositivos no administrados

### Pasos

1. Haga clic en la pestaña **Reglas**.
2. Seleccione la opción **Asignación automática del dispositivo sin administrar**.
3. Haga clic en la pestaña **Agregar reglas**.
4. Ingrese el **Nombre** y seleccione el **Grupo de destino**.
5. Haga clic en la opción **Agregar condición** y seleccione las condiciones para las reglas asignadas.
6. Haga clic en **Guardar**.

La regla se muestra en la lista de grupos no administrados. Esta regla se aplica automáticamente y el dispositivo se agrega a la lista de grupo de destino.

Identifier	GUID-2ECD2887-BD64-435D-8F7B-F395149074A6
Version	1
Status	Translation approved

## Editar un perfil de administrador

### Pasos

1. Haga clic en **Usuarios**.

2. Haga clic en **Administradores**.
3. Haga clic en **Editar administrador**.  
Aparece la ventana **Editar usuario administrador**.
4. Escriba su ID de correo electrónico y nombre de usuario en los campos respectivos.

**NOTA:** Cuando actualiza el nombre de inicio de sesión, está obligado a cerrar sesión en la consola. Inicie sesión en la consola usando el nombre de inicio de sesión actualizado de la cuenta.

5. Realice uno de los siguientes pasos:
  - Si hace clic en la pestaña **Información personal**, ingrese los siguientes detalles:
    - Nombre
    - Apellido
    - Título
    - Número de teléfono móvil
  - Si hace clic en la pestaña **Roles**, ingrese los siguientes detalles:
    - a. En la sección **Roles**, en la lista desplegable **Rol**, seleccione el **Rol del administrador**.
    - b. En la sección **Contraseña**, haga lo siguiente:
      - i. Ingrese la contraseña personalizada.
      - ii. Para generara cualquier contraseña aleatoria, seleccione el botón de selección **Generar contraseña aleatoria**.
6. Haga clic en **Guardar**.

Identifier	GUID-118F2FFF-E002-4AFA-A88A-02808B7D4D34
Version	1
Status	Translation in review

## Agregar un usuario final

### Pasos

1. Haga clic en la ficha **Usuarios**.
2. Haga clic en **Usuarios finales**.
3. Haga clic en **Agregar usuario**.
4. Ingrese el nombre de usuario, el dominio, el nombre, el apellido, la dirección de correo electrónico, el título y el número de teléfono
5. Haga clic en **Guardar**.

Identifier	GUID-C3B567D1-4600-49CB-B69F-601384112963
Version	1
Status	Translation in review

## Editar un usuario final

### Pasos

1. Haga clic en la ficha **Usuarios**.
2. Haga clic en **Usuarios finales**.
3. Haga clic en **Editar usuarios finales**.
4. Escriba su ID de correo electrónico y nombre de usuario en los campos respectivos.
5. Haga clic en **Guardar**.

Identifier	GUID-6F93BD9C-B0D0-4C1D-BE27-69B7512BCDDE
Version	1
Status	Translation in review

## Crear excepciones de usuario final

Puede configurar e implementar ajustes para un usuario individual. La configuración se aplica a la cuenta de usuario y se aplica al cliente delgado cuando el usuario inicia sesión. Esta opción se aplica solo a los clientes delgados que ejecutan el sistema operativo ThinOS 9.x.

## Pasos

1. Haga clic en la ficha **Usuarios**.
2. Haga clic en **Usuarios finales**.
3. Seleccione un usuario.  
Aparece la página **Detalles de usuario final**.
4. Haga clic en el menú desplegable **Editar políticas** y seleccione el sistema operativo.
5. Configure las políticas necesarias y haga clic en **Guardar y publicar**.

**NOTA:** Esta función se aplica solo a los clientes delgados que ejecutan el sistema operativo ThinOS 9.x. No hay límite para la cantidad de usuarios finales en el entorno en las instalaciones. Puede agregar 10 000 usuarios en una nube pública.

Identifier	GUID-60847ABC-5780-4220-BB7B-25FB1A05A0D5
Version	1
Status	Translation in review

# Importación masiva de usuarios finales

## Pasos

1. Haga clic en la ficha **Usuarios**.
2. Haga clic en **Usuarios finales**.
3. Haga clic en **Importación masiva**.
4. Haga clic en **Buscar** y seleccione el archivo .csv.
5. Haga clic en **Importar**.

**NOTA:** Puede agregar hasta 100 usuarios finales a Wyse Management Suite.

Identifier	GUID-FCCC4A95-11BC-4544-8167-218DB8838B53
Version	1
Status	Translation in review

# Eliminar un usuario final

## Pasos

1. Haga clic en la pestaña **Usuarios finales**.
2. Haga clic en **Eliminar usuario final**.  
Se muestra la ventana Alerta. Ingrese el motivo de la eliminación para activar el vínculo Eliminar.
3. Haga clic en **Eliminar**.

Identifier	GUID-D6C25E08-C4EF-43A9-B66F-FDC2AF024C56
Version	1
Status	Translation approved

# Desactivar un perfil de administrador

La desactivación del perfil de administrador evita que inicie sesión en la consola y elimina su cuenta de la lista de dispositivos registrados.

## Pasos

1. Haga clic en **Usuarios**.
2. Haga clic en **Administradores**.
3. En la lista, seleccione un usuario y haga clic en **Desactivar administradores**.  
Se muestra una ventana de alerta.
4. Haga clic en **Aceptar**.

Identifier	GUID-EFB9CB6F-BOC5-476A-8D7D-04361B24A9EC
Version	1
Status	Translation approved

## Eliminar un perfil de administrador

### Sobre esta tarea

Debe desactivar el administrador antes de eliminarlo. Para eliminar un perfil de administrador, haga lo siguiente:


### Pasos

1. Haga clic en **Usuarios**.
2. Haga clic en **Administradores**.
3. Seleccione la casilla de verificación de un administrador o administradores determinados que desee eliminar.
4. Haga clic en **Eliminar administradores**.  
Se muestra la ventana **Alerta**.
5. Ingrese el motivo de la eliminación para activar el vínculo **Eliminar**.
6. Haga clic en **Eliminar**.

Identifier	GUID-CAF0D90C-8F77-4E8D-95DB-FC8E2B618FC7
Version	1
Status	Translation approved

## Editar un perfil de usuario

### Pasos

1. Haga clic en **Usuarios**.
2. Haga clic en **Administrador con asignación cancelada**.
3. Haga clic en **Editar usuario**.  
Aparece la ventana **Editar usuario administrador**.
4. Escriba su ID de correo electrónico y nombre de usuario en los campos respectivos.  
 **NOTA:** Cuando actualiza el nombre de inicio de sesión, está obligado a cerrar sesión en la consola. Inicie sesión en la consola usando el nombre de inicio de sesión actualizado de la cuenta.
5. Realice uno de los siguientes pasos:
  - Si hace clic en la pestaña **Información personal**, ingrese los siguientes detalles:
    - Nombre
    - Apellido
    - Título
    - Número de teléfono móvil
  - Si hace clic en la pestaña **Roles**, ingrese los siguientes detalles:
    - a. En la sección **Roles**, en la lista desplegable **Rol**, seleccione el **Rol del administrador**.
    - b. En la sección **Contraseña**, haga lo siguiente:
      - i. Ingrese la contraseña personalizada.
      - ii. Para generara cualquier contraseña aleatoria, seleccione el botón de selección **Generar contraseña aleatoria**.
6. Haga clic en **Guardar**.

Identifier	GUID-46298852-C2A9-417A-B985-271F6C47432C
Version	2
Status	Translation in review

# Importación masiva de administradores no asignados o usuarios de Cloud Connect

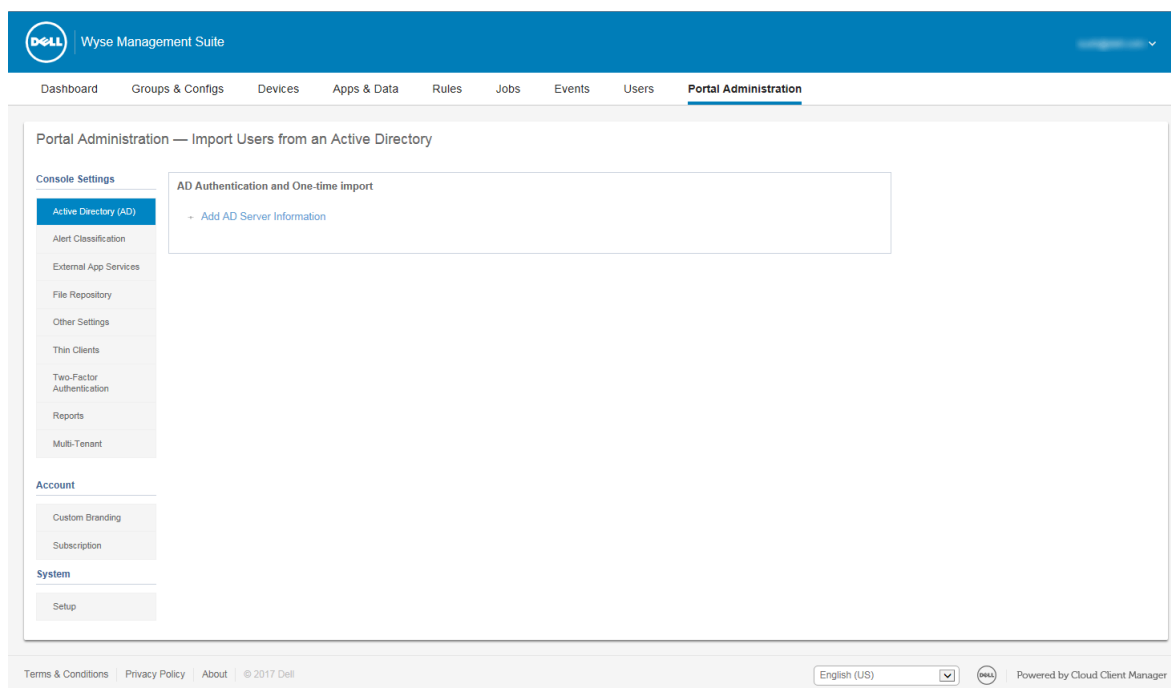
## Pasos

1. Haga clic en **Usuarios**.  
Se muestra la página **Usuarios**.
2. Seleccione la opción **Administrador con asignación cancelada**.
3. Haga clic en **Importación masiva**.  
Aparece la ventana **Importación masiva**.
4. Haga clic en **Navegar** y seleccione el archivo CSV.
5. Seleccione el grupo de usuarios al que se deben asignar los usuarios importados.
6. Haga clic en **Importar**.

Identifier	GUID-EE1CF7C9-FD07-4244-AA26-7D5350E31918
Version	5
Status	Translation approved

## Administración del portal

En esta sección se presenta una breve descripción general de las tareas de administración de su sistema que son necesarias para configurar y mantener su sistema.



**Ilustración 10. Administrador del portal**

### Temas:

- [Cómo agregar la información del servidor de Active Directory](#)
- [Importar usuarios no asignados o grupos de usuarios a la nube pública mediante Active Directory](#)
- [Clasificaciones de alerta](#)
- [Crear una interfaz de programación de aplicaciones; cuentas API](#)
- [Acceder al repositorio de archivos de Wyse Management Suite](#)
- [Configurar otros ajustes](#)
- [Administrar las configuraciones de Teradici](#)
- [Activar la autenticación de dos factores](#)
- [Activar cuentas de varios inquilinos](#)
- [Generar informes](#)
- [Activar una marca personalizada](#)
- [Administrar la configuración del sistema](#)

Identificator	GUID-24002B3A-2B3C-4E05-A86D-E5D3D5088F30
Version	1
Status	Translation in review

# Cómo agregar la información del servidor de Active Directory

Puede importar los usuarios y grupos de usuarios de Active Directory a la nube privada de Wyse Management Suite.

## Pasos

1. Inicie sesión en la nube privada de Wyse Management Suite.
2. Vaya a **Administrador del portal** > **Configuración de la consola** > **Active Directory (AD)**.
3. Haga clic en el enlace **Agregar información del servidor de AD**.
4. Ingrese los detalles del servidor como el **Nombre del servidor de AD**, el **Nombre de dominio**, la **URL del servidor** y el **Puerto**.
5. Haga clic en **Guardar**.
6. Haga clic en **Importar**.
7. Ingrese el nombre de usuario y la contraseña.

**NOTA:** Para buscar grupos y usuarios, puede filtrarlos según las opciones **Base de búsqueda** y **Nombre de grupo** que contiene. Puede ingresar los valores de la siguiente forma:

- OU=<OU Name>, por ejemplo, OU=TestOU
- DC=<Child Domain>, DC=<Parent Domain>, DC=com, por ejemplo, DC=Skynet, DC=Alpha, DC=Com

Puede ingresar un espacio después de una coma, pero no puede usar comillas simples ni dobles.

8. Haga clic en **Inicio de sesión**.
9. En la página **Grupo de usuarios**, haga clic en el **Nombre de grupo** e ingrese el nombre del grupo.
10. En el campo **Buscar**, escriba el nombre del grupo que desea seleccionar.
11. Seleccione un grupo.  
El grupo seleccionado se mueve al panel derecho de la página.
12. En el **campo Contenido de nombre de usuario**, ingrese el nombre de usuario.
13. Haga clic en **Importar usuarios** o **Importar grupos**.

**NOTA:** Si indica un nombre no válido o no indica un apellido, o indica cualquier dirección de correo electrónico como nombre, las anotaciones no se pueden importar en Wyse Management Suite. Estas anotaciones se omiten durante el proceso de importación del usuario.

En el portal de Wyse Management Suite se muestra un mensaje de confirmación con el número de usuarios de Active Directory importados. Los usuarios de Active Directory importados se indican en la pestaña **Usuarios** > **Administradores sin asignar**.

14. Para asignar diferentes roles o permisos, seleccione un usuario y haga clic en **Editar usuario**.

Después de asignar los roles al usuario de Active Directory, se mueven a la pestaña **Administradores** en la página **Usuarios**.

## Siguientes pasos

Los usuarios de Active Directory pueden iniciar sesión en el portal de administración de Wyse Management Suite usando las credenciales de dominio. Para iniciar sesión en el portal de Wyse Management Suite, haga lo siguiente:

1. Inicie el portal de administración de Wyse Management Suite.
2. En la pantalla de inicio de sesión, haga clic en el enlace **Iniciar sesión con sus credenciales de dominio**.
3. Ingrese las credenciales de usuario del dominio y haga clic en **Iniciar sesión**.

Para iniciar sesión en el portal de Wyse Management Suite con credenciales de dominio secundario, realice las siguientes acciones:

1. Inicie el portal de administración de Wyse Management Suite.
2. En la pantalla de inicio de sesión, haga clic en el enlace **Iniciar sesión con sus credenciales de dominio**.
3. Haga clic en **Cambiar el dominio de usuario**.
4. Ingrese la información de identificación y el nombre de dominio completo.
5. Haga clic en **Iniciar sesión**.

Los usuarios de Active Directory importados se pueden activar o desactivar en la página **Usuarios** usando el inicio de sesión de administrador global. Si su cuenta está desactivada, no puede iniciar sesión en el portal de administración de Wyse Management Suite.

**NOTA:** Para importar usuarios mediante el protocolo LDAPS, realice los pasos siguientes:

1. **Importe el certificado raíz del servidor de dominio AD en el almacenamiento de claves de Java en forma manual usando keytool.** Por ejemplo, `<C:\Program Files\DELL\WMS\jdk1.8.0_152\jre\bin>keytool.exe -importcert -alias "WIN-0358EA52H8H" -keystore "<C:\Program Files\DELL\WMS\jdk1.8.0_152\jre\lib\security\cacerts>" -storepass changeit -file "Root Certificate Path"`
2. **Reinicie el servicio Tomcat.**

## Configurar función de Active Directory Federation Services en nube pública

Puede configurar Active Directory Federation Services (ADFS) en una nube pública.

### Pasos

1. En la página **Administrador del portal**, en **Configuración de consola**, haga clic en **Active Directory (AD)**.
2. Ingrese los detalles de Wyse Management Suite en ADFS. Para conocer los detalles de la ubicación en el servidor de ADFS donde debe cargar los archivos xml de Wyse Management Suite, pase el mouse sobre el icono de **información (i)**.

**NOTA:** Para descargar el archivo xml de Wyse Management Suite, haga clic en el enlace de descarga.

3. Establezca los detalles de Wyse Management Suite en ADFS. Para conocer los detalles de las reglas de solicitud personalizada, pase el mouse sobre el icono de **información (i)**.

**NOTA:** Para ver las reglas de Wyse Management Suite, haga clic en el enlace **Mostrar reglas de WMS**. También puede descargar las reglas de Wyse Management Suite haciendo clic en el enlace que se proporciona en la ventana **Reglas de Wyse Management Suite**.

4. Para configurar los detalles de ADFS, haga clic en **Agregar configuración** y haga lo siguiente:

**NOTA:** Para permitir que los inquilinos sigan la configuración de ADFS, cargue el archivo de metadatos de ADFS.

- a. Para cargar el archivo .XML almacenado en el cliente esbelto, haga clic en **Cargar archivo XML**.

El archivo está disponible en <https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml>.

- b. Ingrese los detalles de la ID de la entidad y el certificado de firma X.509 en los cuadros respectivos.
- c. Ingrese la dirección URL de inicio de sesión de ADFS y la URL de cierre de sesión de ADFS en los cuadros respectivos.
- d. Para permitir que los inquilinos configuren un inicio de sesión único usando ADFS, seleccione la casilla de verificación **Activar inicio de sesión SSO utilizando ADFS**. Esta función sigue la especificación estándar de Security Assertion and Markup Language (SAML).
- e. Para validar la información de la configuración, haga clic en **Probar inicio de sesión de ADFS**. Esto permite a los inquilinos probar su configuración antes de guardarla.

**NOTA:** Los inquilinos pueden activar/desactivar el inicio de sesión SSO usando ADFS.

5. Haga clic en **Guardar**.

6. Después de guardar el archivo de metadatos, haga clic en **Actualizar configuración**.

**NOTA:** Los grupos de usuarios pueden iniciar y cerrar sesión con las credenciales de AD que se configuraron desde su ADFS. Debe asegurarse de que los usuarios de AD estén importados al servidor Wyse Management Suite. En la página de inicio de sesión, haga clic en **Iniciar sesión** e ingrese sus credenciales de dominio. Debe indicar la dirección de correo electrónico de su usuario de AD e iniciar sesión. Para importar un usuario a la nube pública, se debe instalar un repositorio remoto. Para obtener más información sobre la documentación de ADFS, vaya a [Technet.microsoft.com](http://Technet.microsoft.com).

## Resultados

Una vez que la conexión de prueba ADFS se realice correctamente, importe los usuarios que usan AD Connector presente en el repositorio remoto.

Identifier	GUID-DCB481F3-3D25-4228-863D-72D4E02D6F81
Version	4
Status	Translation in review

# Importar usuarios no asignados o grupos de usuarios a la nube pública mediante Active Directory


## Pasos

1. Descargue e instale el repositorio de archivos; consulte [Acceder al repositorio de archivos](#). El repositorio debe instalarse mediante la red de la empresa y debe tener acceso al servidor de AD para extraer los usuarios.
2. Registre el repositorio en la nube pública. Una vez registrado, realice las acciones mencionadas en la IU para importar los usuarios a la nube pública de Wyse Management Suite. Puede editar las funciones del usuario de AD después de realizar la importación a la nube pública de Wyse Management Suite.
3. Configurar ADFS en la nube pública.

Identifier	GUID-13685E54-031A-4874-9890-F2C81F9DD734
Version	1
Status	Translation approved

## Clasificaciones de alerta

En la página Alerta se categorizan las siguientes alertas como **Crítica**, **Aviso** o **Información**.

 **NOTA:** Para recibir alertas por correo electrónico, seleccione la opción **Preferencias de alertas de menú de nombre de usuario que se muestra en la esquina superior derecha**.

Seleccione el tipo de notificación preferido como **Crítico**, **Aviso** o **Información** para las siguientes alertas:

- Alerta de condición del dispositivo
- Dispositivo no registrado

Identifier	GUID-0C6DFDD3-89CB-47E9-8A7C-58E5D602FA37
Version	2
Status	Translation approved

# Crear una interfaz de programación de aplicaciones; cuentas API

## Sobre esta tarea

En esta sección puede crear cuentas de interfaz de programación de aplicación (API) seguras. Este servicio ofrece la capacidad de crear cuentas especiales. Para configurar el servicio de aplicaciones externas, haga lo siguiente:

## Pasos

1. Inicie sesión en el portal de Wyse Management Suite y haga clic en la pestaña **Administrador del portal**.
2. Seleccione **Servicios de aplicaciones externas** en **Configuración de consola**.
3. Seleccione la pestaña **Agregar** para agregar un servicio API.  
Aparece el cuadro de diálogo **Agregar servicios de aplicaciones externas**.
4. Ingrese los siguientes detalles para agregar un servicio de aplicación externa.
  - Nombre

- Descripción

5. Seleccione la casilla de verificación **Aprobación automática**.

Si selecciona la casilla de verificación, no se requiere aprobación de los administradores globales.

6. Haga clic en **Guardar**.

Identifier	GUID-382DAAC9-891B-4D03-AE3F-C10B2BDE466A
Version	6
Status	Translation in review

## Acceder al repositorio de archivos de Wyse Management Suite

**Repositorios de archivos** corresponde a lugares en los que se almacenan y organizan los **archivos**. Wyse Management Suite tiene dos tipos de repositorios:

- **Repositorio local:** durante la instalación de la nube privada de Wyse Management Suite, ingrese la ruta del repositorio local en el instalador de Wyse Management Suite. Después de la instalación, vaya a **Administrador del portal > Repositorio de archivos** y seleccione el repositorio local. Haga clic en la opción **Editar** para ver y editar la configuración del repositorio.
- **Repositorio de Wyse Management Suite:** inicie sesión en la nube pública de Wyse Management Suite, vaya a **Administrador del portal > Repositorio de archivos** y descargue el instalador del repositorio de Wyse Management Suite. Después de la instalación, registre el repositorio de Wyse Management Suite en el servidor Wyse Management Suite ingresando la información solicitada.

Puede activar la opción **Replicación automática** para replicar los archivos que se agregan a cualquiera de los repositorios de archivos en otros repositorios. Cuando activa esta opción, se muestra un mensaje de alerta. Puede seleccionar la casilla de verificación **Replicar archivos existentes** para replicar los archivos existentes en los repositorios de archivos.

La opción **Replicar archivo existente** es aplicable si el repositorio ya está registrado. Cuando se registra un nuevo repositorio, todos los archivos se copian en el repositorio nuevo. Puede ver el estado de la replicación de archivos en la página **Eventos**.

Las plantillas `Image Pull` no se replican automáticamente en otros repositorios. Debe copiar estos archivos manualmente.

La función de replicación de archivos solo se admite en repositorios de Wyse Management Suite 2.0 y versiones posteriores.

No puede importar un certificado autofirmado del repositorio remoto al servidor de Wyse Management Suite. Si la validación de CA está activada para el repositorio remoto, la replicación de los archivos del repositorio remoto en el repositorio local va a fallar.

Para usar el repositorio de Wyse Management Suite, haga lo siguiente:

1. Descargue el repositorio de Wyse Management Suite de la consola de la nube pública.
2. Después del proceso de instalación, inicie la aplicación.
3. En la página del repositorio de Wyse Management Suite, ingrese las credenciales para registrar el repositorio de Wyse Management Suite en el servidor Wyse Management Suite.
4. Si activa la opción **Registrar en el portal público de gestión de WMS**, puede registrar el repositorio en la nube pública de Wyse Management Suite.
5. Haga clic en la opción **Sincronizar archivos** para enviar el comando de sincronización de archivos.
6. Haga clic en **Registrar** y luego en **Enviar comando** para enviar el comando de información del dispositivo al dispositivo.
7. Haga clic en la opción **Anular el registro** para anular el registro del servicio in situ.
8. Haga clic en **Editar** para editar los archivos.
9. En la lista desplegable de la opción **Descargas de archivo simultáneas**, seleccione el número de archivos.
10. Active o desactive la opción **Wake on LAN**.
11. Active o desactive la opción **Carga y descarga rápida de archivos (HTTP)**.
  - Cuando HTTP está activado, la carga y la descarga de archivos ocurren por medio de HTTP.
  - Cuando HTTP no está activado, la carga y la descarga de archivos ocurren por medio de HTTPS.
12. Seleccione la casilla de verificación **Validación de certificado** para habilitar la validación de la entidad de certificación (CA) de la nube pública.

**NOTA:** Cuando se habilita la validación de CA del servidor Wyse Management Suite, el certificado debe estar presente en el cliente. Todas las operaciones, como aplicaciones y datos, extracción/inserción de imágenes, se realizan correctamente. Si el certificado no está presente en el cliente, el servidor Wyse Management Suite proporciona un mensaje de evento de auditoría genérico **Se produjo un error al validar la autoridad de certificación en la página Eventos**. Todas las operaciones, como aplicaciones y datos, extracción/inserción de imágenes, no se realizan correctamente. Además, cuando se deshabilita la validación de CA del servidor de Wyse Management Suite, la comunicación del servidor y el cliente se produce en un canal seguro sin la validación de la firma del certificado.

- Agregue una nota en el cuadro disponible.
- Haga clic en **Guardar configuración**.

Identifier	GUID-7D43A4A1-E157-42F4-8E89-8385EED37971
Version	3
Status	Translation in review

## Asignación de la subred

Desde Wyse Management Suite 2.0, puede asignar una subred a un repositorio de archivos. Puede asociar un repositorio de archivos hasta a 25 subredes o rangos. También puede priorizar las subredes asociadas con el repositorio.

Puede implementar los paquetes del BIOS mediante la asignación de subred desde Wyse Management Suite 2.1. Puede cargar e implementar varios paquetes de firmware desde el repositorio remoto, el repositorio de nube de grupos de usuarios o el repositorio de nube del operador. Esta función solo se aplica a la licencia Wyse Management Suite Pro.

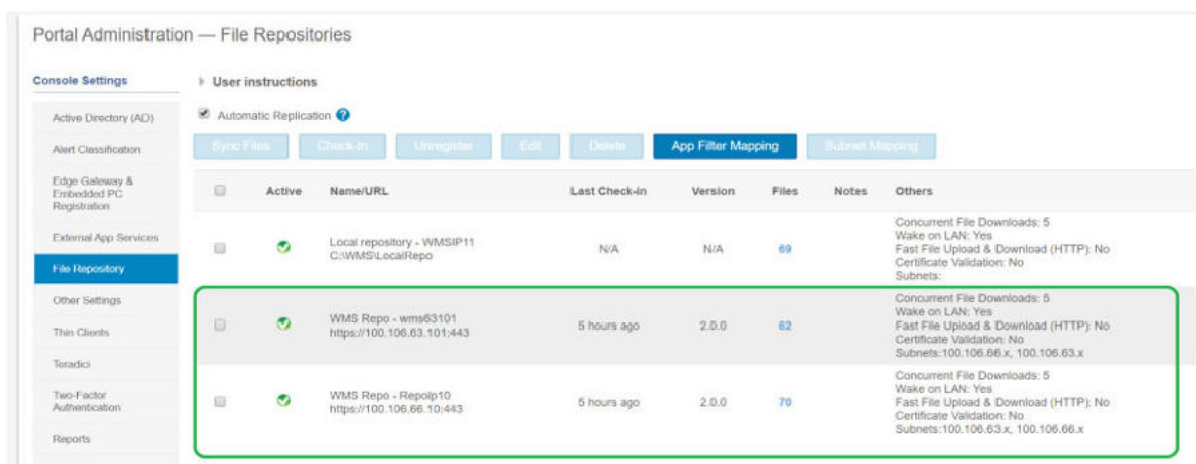
**NOTA: No se admite la proximidad de subred en dispositivos ThinOS 9.x.**

Identifier	GUID-17601EC7-88AC-4531-A8C8-54022F59B6F4
Version	3
Status	Translation in review

## Configurar la asignación de la subred

### Pasos

- Vaya a **Administración del portal > Repositorios de archivos**.



**Ilustración 11. Repositorio de archivos**

- Seleccione un repositorio de archivos.
- Haga clic en la opción **Asignación de la subred**.
- Ingrese las subredes o los rangos, un valor por línea. Debe usar un guión para la separación de rangos.
- De manera opcional, borre la casilla de verificación **Permitir que los dispositivos de las subredes no asignadas a este repositorio de archivos descarguen archivos desde este repositorio como un método de reserva mediante la proximidad de la subred** si desea que se acceda al repositorio de archivos solo a través de las subredes o los rangos configurados.

**NOTA: La opción Permitir que las subredes no asignadas a este repositorio de archivos descarguen archivos desde este repositorio como un método de reserva mediante la proximidad de la subred está seleccionado de forma predeterminada. Esta función no es compatible con dispositivos ThinOS 9.x.**

Identifíer	GUID-497E0790-BA79-4655-996C-3833F3D5F1DE
Version	3
Status	Translation approved

## Configurar otros ajustes

Puede usar los siguientes ajustes para implementar los **Avisos de APNS**, los **Avisos de expiración de la licencia** y otros **Acuerdos legales de autoservicio**.

- **Descartar aviso de caducidad de la licencia en la página Panel:** seleccione esta casilla de verificación para evitar que se muestre el aviso de expiración de la licencia en la página **Panel**.
- **Activar las opciones avanzadas de Dell Wyse Cloud Connect en la página de configuración de políticas de la configuración de Android (nota: Solo Professional Tier):** seleccione esta opción para activar las opciones avanzadas de Dell Wyse Cloud Connect en la página de configuración de políticas de configuración de Android.
- **Intervalo de latido:** ingrese el tiempo. El dispositivo envía una señal de latido cada 60 a 360 minutos.
- **Intervalo de registro:** ingrese el tiempo. El dispositivo envía una señal de registro completo cada 8 a 24 horas.
- **Alerta de cumplimiento no registrada:** ingrese el número de días antes de que el dispositivo active una **alerta de cumplimiento no registrada**. El rango es de 1 a 99.
- **Tiempo de espera de la consola WMS:** ingrese el tiempo de inactividad en minutos después del cual se cierra la sesión del usuario en la consola. Cualquier administrador global puede ajustar esta configuración. El valor predeterminado es 30 minutos.
- **Validación de la inscripción:** cuando la **opción Validación de la inscripción** está activada, los dispositivos detectados automáticamente se encuentran en el estado de **Validación pendiente** en la página **Dispositivos**. El usuario puede seleccionar un solo dispositivo o varios dispositivos en la página **Dispositivos** y validar la inscripción. Los dispositivos se mueven al grupo deseado después de que se validan.

Identifíer	GUID-C61ADC9A-823C-4095-A16A-F4D5293767B0
Version	1
Status	Translation approved

## Administrar las configuraciones de Teradici

Para agregar un servidor Teradici, realice lo siguiente:

### Pasos

1. En la pestaña **Administración del portal**, en **Configuración de la consola**, haga clic en **Teradici**.
2. Haga clic en **Agregar servidor**. Aparecerá la pantalla **Agregar servidor**.
3. Ingrese el **nombre del servidor**. El número de puerto se rellenará automáticamente.
4. Seleccione la casilla de verificación **Validación de CA** para activar la validación de CA.
5. Haga clic en **Prueba**.

Identifíer	GUID-16E12D63-2D05-4DAB-8E1D-51BC03CE7697
Version	3
Status	Translation approved

## Activar la autenticación de dos factores

Debe tener al menos dos usuarios administradores globales activos en el sistema.

### Requisitos previos

Cree dos o más administradores globales antes de continuar con la tarea.

### Sobre esta tarea

1. Inicie sesión en el portal de Wyse Management Suite y haga clic en la pestaña **Administrador del portal**.
2. Haga clic en **Autenticación de doble factor** en **Configuración de la consola**.
3. Debe seleccionar la casilla de verificación para activar la autenticación de dos factores.
  - **NOTA:** Los administradores deben verificar el segundo factor de autenticación usando códigos de acceso de uso único para iniciar sesión en el portal de administración.
4. Recibirá un código de acceso de uso único en su dirección de correo electrónico. Ingrese el código de acceso de uso único.

De manera predeterminada, tiene ocho intentos para verificar el código de acceso de uso único. Si no se puede verificar el código de acceso, la cuenta se bloqueará. Solo los administradores globales pueden desbloquear las cuentas bloqueadas.

Identifier	GUID-49D4E2AD-F40A-4E98-973B-BD6B908742A5
Version	1
Status	Translation approved

## Activar cuentas de varios inquilinos

Esta sección le permite crear cuentas de grupos de usuarios que se pueden administrar de manera independiente entre sí. Puede administrar las organizaciones de manera independiente. Cada cuenta debe tener su propia clave de licencia y puede configurar su propio conjunto de cuentas de administrador, políticas, imágenes de sistema operativo, aplicación, reglas, alertas, entre otros. El operador de alto nivel crea estas organizaciones.

Para activar las cuentas de varios inquilinos, haga lo siguiente:

1. Inicie sesión en el portal de Wyse Management Suite y haga clic en la pestaña **Administrador del portal**.
2. Seleccione **Varios inquilinos** en **Configuración de la consola**.
3. Seleccione esta casilla de verificación para activar la opción de varios inquilinos.
4. Especifique los siguientes detalles.
  - Nombre de usuario
  - Contraseña
  - Confirmar la contraseña
  - Correo electrónico
5. Haga clic en **Guardar la configuración**.

Identifier	GUID-8D4F3506-8668-481C-A4EF-77B283CD0E63
Version	3
Status	Translation approved

## Generar informes

Puede descargar los informes de los trabajos, los dispositivos, los grupos, los eventos, las alertas y las políticas. Los informes se pueden compartir con el administrador si desea solucionar problemas de los puntos finales.

### Pasos

1. Vaya a **Informes del > administrador del portal**.
2. Haga clic en la opción **Generar informe**.  
Se muestra la ventana **Generar informe**.
3. En la lista desplegable **Tipo**, seleccione el tipo de informe.
4. En la lista desplegable **Grupos**, seleccione el grupo.
5. Seleccione el delimitador.
6. Haga clic en **Guardar**.

Identifier	GUID-3BEBF55B-14A1-4FE6-B602-B2D8E47BE5A4
Version	2
Status	Translation approved

## Activar una marca personalizada

### Sobre esta tarea

Esta opción le permite agregar el nombre de su compañía y su logotipo o marca. Puede cargar su propio logotipo del encabezado, favicono, agregar un título de encabezado y cambiar los colores del encabezado para personalizar el portal de Wyse Management Suite. Para acceder a la marca personalizada y especificarla:

### Pasos

1. Vaya a **Administrador del portal > Cuenta > Marca personalizada**.
2. Haga clic en **Activar marca personalizada**.

3. En el **Logotipo del encabezado**, haga clic en **Buscar** y seleccione la imagen del logotipo del encabezado desde la ubicación de la carpeta.

El tamaño máximo del logotipo del encabezado debe ser de 500 \* 50 píxeles.

4. Ingrese el título en la opción **Título**.
5. Seleccione la casilla de verificación **Mostrar título en la ventana/pestaña del navegador** para ver el título en el navegador.
6. Ingrese los códigos de color para el **Color de fondo del encabezado** y el **Color del texto del encabezado**.
7. Haga clic en **Examinar** y seleccione el **Favicono**.

El favicono aparece en la barra de direcciones del navegador al lado de la URL del sitio web.

**NOTA:** Debe guardar las imágenes solo como archivos **.ico**.

8. Haga clic en **Guardar la configuración**.

Identifier	GUID-FD506A7F-45B9-4EB5-B657-EFE39FD73139
Version	5
Status	Translation in review

## Administrar la configuración del sistema

Puede cambiar los detalles de SMTP, los certificados, los detalles de MQTT y los detalles externos de la URL de Wyse Management Suite que se configuraron durante la instalación.

Desde Wyse Management Suite 2.1, se admite la **Configuración de esquema dinámico** para dispositivos ThinOS 9.x que le permite actualizar los ajustes de configuración más recientes sin hacer ningún cambio en el lado del servidor. En la nube pública, el operador de Wyse Management Suite puede actualizar la interfaz del usuario de la configuración 9.x. En la nube privada, solo función pro, el usuario global puede actualizar la interfaz del usuario de la configuración 9.x. Si la función **Varios usuarios** está activada, el operador de Wyse Management Suite puede cargar el esquema más reciente desde la sección **Administración**.

### Pasos

1. Inicie sesión en el portal de Wyse Management Suite y haga clic en la pestaña **Administrador del portal**.
2. Haga clic en **Configuración** en **Sistemas**.
3. Seleccione la casilla de verificación para realizar una validación de certificado del servidor para toda la comunicación del dispositivo al servidor.
4. Ingrese los siguientes detalles en el área **Actualizar SMTP para alertas de correo electrónico**:
  - Servidor SMTP
  - Enviar desde dirección
  - Nombre de usuario
  - Contraseña
  - Dirección de prueba

**Certificado actual:** seleccione la casilla de verificación **Validación del certificado** para activar la validación CA para la nube privada. Todas las comunicaciones desde el servidor y el cliente, incluso la descarga de archivos y la descarga de imágenes del sistema operativo desde el repositorio local usan el certificado.

**NOTA:** Cuando se habilita la validación de CA del servidor Wyse Management Suite, el certificado debe estar presente en el cliente. Todas las operaciones, como aplicaciones y datos, extracción/inserción de imágenes, se realizan correctamente. Si el certificado no está presente en el cliente, el servidor Wyse Management Suite proporciona un mensaje de evento de auditoría genérico **Se produjo un error al validar la autoridad de certificación en la página Eventos**. Todas las operaciones, como aplicaciones y datos, extracción/inserción de imágenes, no se realizan correctamente. Además, cuando se deshabilita la validación de CA del servidor de Wyse Management Suite, la comunicación del servidor y el cliente se produce en un canal seguro sin la validación de la firma del certificado.

5. Seleccione las siguientes opciones e ingrese los detalles:
  - **Clave/certificado:** carga el par de clave HTTPS/archivo de certificado (solo es compatible el formato PEM).
  - **PKCS-12:** cargue PKCS-12 de HTTPS (.pfx, .p12). Se requiere el certificado intermedio de Apache para pfx de IIS.
6. Para actualizar la información de MQTT externo, haga clic en la opción **Cambiar MQTT externo** y configure los detalles.
7. Para actualizar la URL de Wyse Management Suite externo, haga clic en la opción **Cambiar URL de WMS externo** y configure los detalles.

**NOTA:** Para volver a los ajustes anteriores, haga clic en la opción **Revertir últimas URL y luego en Guardar**.

8. Si desea actualizar la interfaz del usuario de la configuración de 9.x, haga clic en **Elegir archivos** en el campo **Configuración del paquete de UI** y navegue hasta el archivo .zip.

 **NOTA:** Esta opción no está disponible si la función Varios usuarios está activada.

9. Haga clic en **Guardar**.

Identifíer	GUID-FD39D3ED-B45B-46D5-A636-FC5C1E0E506F
Version	2
Status	Translation approved

## Administración de dispositivos Teradici

En la sección de administración de dispositivos Teradici se proporciona información sobre la administración y la detección de los dispositivos Teradici. La consola de administración de Teradici utiliza SDK para ser compatible con la administración y configuración de los dispositivos Teradici. Esto es válido solo para la nube privada de Wyse Management Suite con tipo de licencia Pro.

### Temas:

- [Detectar dispositivos Teradici](#)
- [Situaciones de casos de uso de CIFS](#)

Identifíer	GUID-C0D8E20A-336E-4EEB-9492-F85635FBA2E4
Version	3
Status	Translation approved

## Detectar dispositivos Teradici

### Requisitos previos

- Instale la versión más reciente de Wyse Management Suite en Microsoft Windows 2012 Server o versiones posteriores. Los dispositivos ThreadX 5.x y 6.x funcionan con la versión más reciente del sistema operativo.
- Instale y active el componente de **EMSDK**.
- El FQDN del servidor de Wyse Management Suite debe estar disponible para las configuraciones de **DHCP** o **DNS**.
- `Cert.pem` se debe ubicar en la ruta de acceso predeterminada `C:\Program Files\Dell\WMS\Teradici\EMSDK`. Se utiliza para detectar dispositivos Threadx.

## Nivel de seguridad

Según el nivel de seguridad configurado de un terminal es posible que también deba aprovisionar terminales con un certificado de EBM/EM.

Los terminales configurados para un nivel medio o alto de seguridad deben tener un certificado de confianza en su almacén de certificados antes de poder conectarse a un EBM o EM. En el caso de algunos terminales, el proveedor puede cargarlos previamente como valores predeterminados de fábrica. De lo contrario, puede cargar certificados de forma manual utilizando la AWI de un terminal.

Los terminales configurados para un nivel bajo de seguridad no necesitan un certificado de MC en sus almacenes de certificados de confianza si se cumple una de las siguientes condiciones:

- Utilizan el descubrimiento de DHCP o el descubrimiento de DNS, y el servidor DNS o DHCP proporcionó la huella digital del certificado de EBM.
- Se descubren con el método de descubrimiento manual.

**Tabla 5. Requisitos del certificado para terminales**

Método de descubrimiento	Nivel bajo de seguridad	Nivel medio de seguridad	Nivel alto de seguridad
Descubrimiento de DHCP/DNS sin huella digital de EBM	Se requiere certificado	Se requiere certificado	No aplica
Descubrimiento de DHCP/DNS con huella digital de EBM	No se requiere certificado	Se requiere certificado	No aplica
Descubrimiento iniciado por un terminal configurado para un entorno de alta seguridad	No aplica	No aplica	Se requiere certificado

**Tabla 5. Requisitos del certificado para terminales (continuación)**

Método de descubrimiento	Nivel bajo de seguridad	Nivel medio de seguridad	Nivel alto de seguridad
Descubrimiento manual iniciado por el MC	No se requiere certificado	No aplica	No aplica

## DetECCIÓN MANUAL DEL CLIENTE

1. Vaya a `https://<clientIP>`.
2. Acepte el mensaje de advertencia del certificado.
3. Ingrese la contraseña de administrador (la contraseña predeterminada es Administrator) e inicie sesión.
4. Vaya a **cargar certificado**. Seleccione el archivo `Cert.pem` en la ruta de acceso predeterminada y haga clic en **Cargar**.
5. Vaya a **Administración de la configuración**. Haga clic en el botón **borrar estado de administración** para registrar el dispositivo en el nuevo Servidor de administración.
6. Establezca el **modo de detección del administrador** en manual.
7. Ingrese la **dirección URL del Administrador de arranque de terminal** en el siguiente formato **wss:// <Dirección IP del servidor WMS>**

**NOTA:** Si EMSDK se instala con un puerto personalizado, proporciona una dirección URL del Administrador de arranque de terminal en el siguiente formato **wss://<IP Address:Custom port>**.

8. Haga clic en **Aplicar** y, después, en **Continuar**.
9. El **estado de la administración** se mostrará como Conectado al servidor terminal.

## AGREGAR LA CLASE DE PROVEEDOR DEL TERMINAL PCoIP AL SERVIDOR DHCP

1. Inicie sesión en el servidor DHCP.
2. Haga clic con el botón secundario en el servidor DHCP en el panel **SERVIDORES** y seleccione **Administrador de DHCP**.
3. Haga clic con el botón secundario en la opción **IPv4** y, a continuación, seleccione **Definir clases de proveedores**.
4. Haga clic en **Agregar** para agregar una nueva clase de proveedor DHCP.
5. Ingrese el **Terminal PCoIP** en el campo **Nombre de visualización**.
6. Ingrese el **Terminal PCoIP** en la columna **ASCII** como el ID del proveedor.
7. Haga clic en **Aceptar** para guardar la configuración.

## CONFIGURAR OPCIONES DE DHCP

1. Haga clic con el botón secundario en la opción **IPv4** y, a continuación, seleccione **Establecer opciones predefinidas**.
2. Seleccione **Terminal PCoIP** como la clase de **opción** y, a continuación, haga clic en **Agregar**.
3. En el cuadro de diálogo **Tipo de opción**, ingrese el nombre como **EMB URI**, el tipo de datos como **Cadena**, el código como **10** y la descripción como **Administrador de arranque de terminal** y, a continuación, haga clic en **Aceptar**.
4. Haga clic en **Aceptar** para guardar la configuración.
5. Expanda el alcance DHCP al que se desee aplicar las opciones.
6. Haga clic con el botón secundario en **Opciones de alcance** y seleccione **Configurar opciones**.
7. Haga clic en la pestaña **Avanzado** y, a continuación, seleccione la clase **Terminal de PCoIP**.
8. Seleccione la casilla de verificación **010 MBE URI** y, a continuación, ingrese una URI de consola de administración válida en el campo **Cadena**. Haga clic en **Aplicar**. Esta dirección URI requiere un prefijo WebSocket seguro; por ejemplo, `wss://<dirección IP del MC>:[número de puerto].5172` es el puerto de escucha del MC. Ingresar este número de puerto es un paso opcional.
9. Haga clic en **Aceptar** para guardar la configuración.
10. Seleccione **Terminal de PCoIP** como la clase **Opción** y, a continuación, haga clic en **Agregar**.
11. En el cuadro de diálogo **Tipo de opción**, ingrese el nombre como **huella digital EBM X.509 SHA-256**, el tipo de datos como **Cadena**, el código como **11** y la descripción como **huella digital EBM X.509 SHA-256**; a continuación, haga clic en **Aceptar**.
12. Expanda el alcance DHCP al que se desee aplicar las opciones.
13. Haga clic con el botón secundario en **Opciones de alcance** y seleccione **Configurar opciones**.
14. Haga clic en la pestaña **Avanzado** y, a continuación, seleccione la clase **Terminal de PCoIP**.
15. Seleccione la casilla de verificación **huella digital 011 EBM X.509 SHA-256** y pegue la huella digital SHA-256.

16. Haga clic en **Aceptar** para guardar la configuración.
17. Vaya al navegador web del cliente.
18. Vaya a **Configuración > Administración** y establezca el **modo de descubrimiento del gestor** en **automático**
19. El cliente se conectará al servidor mencionado en el servidor DHCP.

## Crear el registro SRV de DNS

1. Inicie sesión en el **servidor DNS**.
2. Haga clic con el botón secundario en el servidor DNS en el panel **SERVIDORES** y, a continuación, seleccione **Administrador de DNS** en el menú contextual.
3. En **Zonas de búsqueda directa**, haga clic con el botón secundario en el dominio y, a continuación, seleccione **Otros nuevos registros** en el menú contextual.
4. En el cuadro de diálogo **Tipo de registro de recursos**, seleccione **Ubicación de servicio (SRV)** en la lista y haga clic en **Crear registro**.
5. Establezca **Servicio** en **\_pcoip-bootstrap**, el protocolo en **\_tcp** y el **número de puerto** en **5172**, que es el puerto de escucha predeterminado del MC. En el caso del **host que ofrece este servicio**, ingrese el FQDN del MC.

 **NOTA:** Se debe ingresar el FQDN del MC, ya que la especificación de DNS no permite que exista una dirección IP en los registros de SRV.

6. Haga clic en **Aceptar**.

## Agregar un registro TXT de DNS

1. En **Zonas de búsqueda directa**, haga clic con el botón secundario en el dominio y, a continuación, seleccione **Otros nuevos registros** en el menú contextual.
2. En el cuadro de diálogo **Tipo de registro de recursos**, seleccione el **Texto (TXT)** en la lista y, a continuación, haga clic en **Crear registro**.
3. Especifique los siguientes detalles.
  - a. En el campo **Nombre de registro**, ingrese el hostname del servidor Wyse Management Suite que ofrece el servicio. El campo FQDN se completará automáticamente. Eso debe coincidir con el FQDN del servidor Wyse Management Suite.
  - b. En el campo **Texto**, ingrese **pcoip-bootstrap-cert=** y, a continuación, pegue la huella digital SHA-256 del certificado del servidor Wyse Management Suite.
4. Haga clic en **Aceptar**.
5. Vaya al navegador web del cliente.
6. El cliente se conectará al servidor Wyse Management Suite mencionado en el servidor DNS.


## Crear huellas digitales SHA-256

1. Inicie Mozilla Firefox.
2. Diríjase a la pestaña **Opciones Avanzadas**
3. Haga clic en **Certificados** para ver los certificados.
4. En **Administrador de certificados**, haga clic en **Autoridades** y, a continuación, haga clic en **Importar**.
5. Examine el certificado y, a continuación, haga clic en **Ver**.
6. Copie la huella digital **SHA-256**.

Identifíer	GUID-ACEC22C3-D02A-4BE4-B430-72CA8A120EC2
Version	1
Status	Translation approved

## Situaciones de casos de uso de CIFS

Los siguientes casos de uso son compatibles con Wyse Management Suite:

- Cuando selecciona **Wyse Management Suite** como **tipo de instalación** mientras se instala la nube privada de Wyse Management Suite.
    - Se mostrará la página de configuración de CIFS. Esta página es necesaria, pues se debe configurar la carpeta compartida.
-  **NOTA:** De manera predeterminada, la opción **Configurar credenciales de usuario de CIFS** está **desactivada**.

- Cuando selecciona **Teradici EMSDK** como **tipo de instalación** mientras se instala la nube privada de Wyse Management Suite.
  - En el caso de las credenciales de CIFS, puede utilizar una cuenta existente o crear una nueva.
- Cuando selecciona **Wyse Management Suite** y **Teradici EMSDK** como **tipo de instalación** mientras se instala la nube privada de Wyse Management Suite.
  - Se mostrará la página de configuración de CIFS. Esta página es necesaria, pues se debe configurar la carpeta compartida.
    - **NOTA: De manera predeterminada, la opción Configurar credenciales de usuario de CIFS está desactivada.**
    - En el caso de las credenciales de CIFS, puede utilizar una cuenta existente o crear una nueva.
- Cuando instala solo EMSDK en un sistema que ya cuenta con el servicio EMSDK instalado.
  - Si selecciona EMSDK Teradici, a continuación, se mostrará un mensaje de aviso cuando haga clic en **Siguiente** en la página **Tipo de instalación**. El mensaje es **El instalador ha detectado que el Teradici EMSDK ya está instalado. El EMSDK se actualizará si es necesario**. No se requiere ningún número de puerto.
    - Si se selecciona la opción **Configurar credenciales de usuario de CIFS** (de manera predeterminada)
      1. Detenga el servicio.
      2. Actualice el servicio EMSDK.
      3. Reinicie el servicio. Funcionará según el mismo usuario preconfigurado.
    - Si la opción **Configurar credenciales de usuario de CIFS** se selecciona con la opción **Utilizar un usuario existente**.
      1. Detenga el servicio.
      2. Actualice el servicio EMSDK.
      3. Actualice el usuario de inicio de sesión del servicio al usuario seleccionado.
      4. Reinicie el servicio. Funcionará según el mismo usuario preconfigurado.
    - Si la opción **Configurar credenciales de usuario de CIFS** se selecciona con la opción **Crear un nuevo usuario**.
      1. Detenga el servicio.
      2. Actualice el servicio EMSDK.
      3. Actualice el usuario de inicio de sesión del servicio al usuario recién creado.
      4. Reinicie el servicio. Funcionará según el mismo usuario preconfigurado.
- Cuando se instalan **Wyse Management Suite** y **Teradici EMSDK** en un sistema que ya cuenta con el servicio EMSDK instalado.
  - Es la misma situación que **Cuando instala solo EMSDK en un sistema que ya cuenta con el servicio EMSDK instalado**, excepto que la opción **Configurar credenciales de usuario de CIFS** está seleccionada de manera predeterminada y aparece desactivada en color gris. Debe ingresar las credenciales de CIFS.

Identifíer	GUID-006A1165-3FCB-435F-910E-EDCC0BD1BD7D
Version	1
Status	Translation approved

## Administrar suscripción a la licencia

Esta sección le permite ver y administrar la suscripción de licencia de la consola de administración y su uso.

En la página **Administrador del portal**, puede ver la opción **Suscripción**. En esta página se proporciona la información siguiente:

- Suscripción de licencia
- Pedidos de licencias
- Uso de licencias: dispositivos de cliente esbelto registrados
- Información del servidor
- Importar licencia: nube privada
- Exportar licencia para nube privada: nube pública

### Temas:

- [Importar licencias desde la nube pública de Wyse Management Suite](#)
- [Exportar licencias a la nube privada de Wyse Management Suite](#)
- [Asignación de licencias de clientes delgados](#)
- [Pedidos de licencias](#)

Identifíer	GUID-F6504746-C17B-4B7F-9EE2-5F0DFAA2655E
Version	2
Status	Translation approved

## Importar licencias desde la nube pública de Wyse Management Suite

Puede importar licencias desde la nube pública de Wyse Management Suite a la nube privada de Wyse Management Suite.

### Pasos

1. Inicie sesión en el servidor de nube privada de Wyse Management Suite.
2. Vaya a **Administración del portal > Cuentas > Suscripción**.
3. Ingrese los detalles de la nube pública de Wyse Management Suite:

- Nombre de usuario
- Contraseña
- Centro de datos
- Número de puestos de TC
- Número de puestos de Edge Gateway y Embedded PC
- Número de puestos de clientes delgados de software Wyse

4. Haga clic en **Importar**.



**NOTA:** La nube privada de Wyse Management Suite debe estar conectada a la nube pública de Wyse Management Suite.

Identifíer	GUID-F67E029F-A3B2-4E44-97CF-08E1D9C826E3
Version	2
Status	Translation approved

## Exportar licencias a la nube privada de Wyse Management Suite

Puede exportar licencias a la nube privada de Wyse Management Suite desde la nube pública de Wyse Management Suite.

### Pasos

1. Inicie sesión en la consola de la nube pública de Wyse Management Suite.
2. Vaya a **Administración del portal > Cuentas > Suscripción**.
3. Ingrese el número de puestos de clientes delgados que se deben exportar a la nube privada de Wyse Management Suite.
4. Haga clic en **Exportar**.
5. Copie la clave de licencia que se genera.
6. Inicie sesión en el servidor de nube privada de Wyse Management Suite.
7. Vaya a **Administración del portal > Cuentas > Suscripción**.
8. Ingrese la clave de licencia generada en la casilla.
9. Haga clic en **Importar**.

Identifíer	GUID-7B7EE737-8184-4143-AEB7-94ED81AB3629
Version	2
Status	Translation approved

## Asignación de licencias de clientes delgados

Para asignar las licencias de clientes esbeltos entre la cuenta de la nube privada de Wyse Management Suite y la nube pública de Wyse Management Suite.

### Pasos

1. Inicie sesión en la consola de nube pública de Wyse Management Suite.
2. Vaya a **Administración del portal > Cuentas > Suscripción**.
3. Ingrese el n.º de puestos de Thin client.

**NOTA:** Deberían ser administrables los puestos de clientes delgados en la nube pública. El número ingresado de puestos de clientes delgados no debe exceder al número que se muestra en la opción Administrable.

4. Haga clic en **Exportar**.

**NOTA:** El número de licencias de la nube pública se ajusta según el número de puestos de clientes delgados exportados a la nube privada.

5. Copie la clave de licencia que se genera.
6. Inicie sesión en el servidor de nube privada de Wyse Management Suite.
7. Vaya a **Administración del portal > Cuentas > Suscripción**.
8. Importar la clave de licencia exportada a la nube privada.

**NOTA:** La licencia no se puede importar si no tiene suficientes puestos de clientes delgados para administrar la cantidad de dispositivos que se están administrando actualmente en la nube privada. En este caso repita los pasos 3 a 8 para asignar los puestos de clientes delgados.

Identifier	GUID-985E2140-60AA-43ED-AFC1-7CA4724FA242
Version	2
Status	Translation approved

## Pedidos de licencias

En la nube pública, la sección **Pedidos de licencia** muestra la lista de pedidos realizados que incluye las licencias vencidas. De manera predeterminada, los pedidos caducados no se muestran. Seleccione la casilla de verificación **Incluir pedidos caducados** para poder revisarlos. Los pedidos vencidos se muestran en color rojo y los pedidos que vencen dentro de 30 días o menos se muestran en color naranja.

**i** **NOTA:** Esta función no se aplica a las implementaciones locales, ya que no muestra el historial de pedidos. Sin embargo, el historial de pedidos de licencias en las instalaciones se encuentra disponible cuando inicia sesión en el portal de la nube pública como administrador del grupo de usuarios.

Identifier	GUID-44D0F37A-9D53-4777-8424-ADE518E34D58
Version	1
Status	Translation approved

## Actualización del firmware

Puede utilizar Wyse Management Suite para actualizar el firmware.

### Temas:

- [Actualizar ThinLinux 1.x a 2.1 y versiones posteriores](#)
- [Actualizar ThinOS 8.x a 9.0](#)

Identifier	GUID-24747078-8B6D-42D2-9613-D4633CD28D14
Version	1
Status	Translation approved

## Actualizar ThinLinux 1.x a 2.1 y versiones posteriores

Si desea extraer una imagen personalizada desde TL 2.x antes de la actualización, debe preparar ThinLinux 2.x y luego actualizar la imagen de ThinLinux 1.x.

Identifier	GUID-A59635E7-65AA-4230-B40B-901ECB4318A9
Version	4
Status	Translation approved

## Preparar la imagen de ThinLinux 2.x

### Requisitos previos

Utilice Wyse Management Suite versión 1.4 o posterior para actualizar la versión de compilación de ThinLinux 2.0.19 o 2.1 a 2.2.

### Pasos

1. Vaya a [www.dell.com/support](http://www.dell.com/support).
2. Haga clic en **Soporte de productos**, ingrese la **Etiqueta de servicio** del cliente esbelto y presione **Intro**.

 **NOTA:** Si no tiene una Etiqueta de servicio, busque el modelo de cliente esbelto de forma manual.

3. Haga clic en **Controladores y descargas**.
4. En el menú desplegable **Sistema operativo**, seleccione **ThinLinux**.
5. Descargue el complemento `merlin_nonpxe-4.0.1-0 0.04.amd64.deb` y `wda_3.4.6-05_amd64.tar`.
6. Copie el complemento descargado en `<drive C>/wms/localrepo/repository/thinClientsApps/`.
7. En el cliente esbelto que ejecuta ThinLinux 2.x, vaya a **Configuración > Administración > Wyse Device Agent**.
8. Registre el dispositivo en el servidor de Wyse Management Suite.
9. Cierre la ventana **Configuración**.

 **NOTA:** Si la ventana Configuración no se cierra, aparece el error Perfil bloqueado después de implementar la imagen.

10. Inicie sesión en la consola de Wyse Management Suite.
11. Cree e implemente la política de aplicación para los complementos `merlin_nonpxe-4.0.1-0 0.04.amd64.deb` y `wda_3.4.6-05_amd64.tar`.
12. Reinicie el cliente esbelto.

13. Inicie sesión en el servidor de Wyse Management Suite.
14. Vaya a la página Dispositivo y asegúrese de que las versiones de Merlin y WDA estén actualizadas.
15. Haga clic en el dispositivo registrado y vaya a **Más acciones > Extraer imagen de SO**. Se muestra la ventana **Extraer imagen de SO**.
16. Ingrese el nombre de la imagen.
17. En la lista desplegable Repositorio de archivos, seleccione el repositorio de archivos.
18. Seleccione el tipo de operación de extracción que desea realizar.
  - **Predeterminado:** seleccione la casilla de verificación **SO + recuperación** y extraiga la imagen (comprimida/descomprimida).
  - **Avanzado:** seleccione la plantilla `Compress_OS_Recovery_Commandsxml/uncompress_OS_Recovery_CommandsXml` y extraiga la imagen.

## Resultados



### **NOTA:**

- **Si utiliza el repositorio remoto de Wyse Management Suite 1.3, entonces el archivo XML no va a estar disponible en el repositorio. Debe actualizar Wyse Management Suite a la versión 1.4 o una versión posterior para acceder al archivo.**
- **La operación de extracción de recuperación no conserva la configuración del usuario.**

Identifier	GUID-51CA71B5-728B-456C-A838-F64112F061DA
Version	2
Status	Translation approved

# Actualizar ThinLinux 1.x a 2.x

## Pasos

1. Vaya a [www.dell.com/support](http://www.dell.com/support).
2. Haga clic en **Soporte de productos**, ingrese la **Etiqueta de servicio** del cliente esbelto y presione **Intro**.
  -  **NOTA: Si no tiene una Etiqueta de servicio, busque el modelo de cliente esbelto de forma manual.**
3. Haga clic en **Controladores y descargas**.
4. En el menú desplegable **Sistema operativo**, seleccione **ThinLinux**.
5. Desplácese por la página y realice las siguientes acciones:
  - Descargue los complementos `Platform_util-1.0.26-0.3.x86_64.rpm`, `wda-2.1.23-00.01.x86_64.rpm` y `merlin-nonpxe_3.7.7-00.05_amd64.deb`.
  - Descargue el archivo de imagen de ThinLinux versión 2.x más reciente ( `2.1.0.01_3040_16GB_merlin.exe` o `2.2.0.00_3040_merlin_16GB.exe`).
6. En el cliente esbelto, vaya a **Configuración > Administración > Wyse Device Agent**.
7. Registre el dispositivo en el servidor de Wyse Management Suite.
8. Inicie sesión en la consola de Wyse Management Suite.
9. Cree e implemente la política de la aplicación para los complementos `Platform_util-1.0.26-0.3.x86_64.rpm`, `wda-2.1.23-00.01.x86_64.rpm` y `merlin-nonpxe_3.7.7-00.05_amd64.deb`.
10. Reinicie el cliente esbelto.
11. Inicie sesión en el servidor de Wyse Management Suite.
12. Copie la imagen descargada (archivo `2.2.0.00_3040_merlin_16GB.exe`) en `<drive C>/wms/localrepo/repository/osimages/zipped/`.
  -  **NOTA: La imagen en la carpeta comprimida se extrae en una carpeta válida. Es posible que el proceso de extracción tarde de 10 a 15 minutos.**
13. Inicie sesión en la consola de Wyse Management Suite.
14. Vaya a **Aplicaciones y datos > Repositorio de imágenes del SO > WES/ThinLinux** y verifique que la imagen de ThinLinux esté disponible.
15. Vaya a **Aplicaciones y datos > Políticas de imagen del SO (WES/ThinLinux)** y haga clic en **Agregar política**.
16. En la ventana Agregar política, configure las siguientes opciones:

- **Tipo de SO:** ThinLinux
- **Filtro secundario del SO:** ThinLinux (ThinLinux)
- **Regla:** solo actualizar/forzar esta versión

**NOTA:** Seleccione la imagen extraída o la imagen nueva que se copia en el repositorio mientras crea la política.

17. Actualice los otros campos obligatorios según sea necesario y haga clic en **Guardar**.
18. Programe el trabajo.
19. Haga clic en **Actualizar ahora** en el cliente para actualizar la imagen.

Identifíer	GUID-A38FFB08-56F5-4E2A-B0A9-08AA8CA62B5E
Version	2
Status	Translation in review

## Actualizar ThinOS 8.x a 9.0

Debe utilizar Wyse Management Suite versión 2.0 y posterior para actualizar el firmware de ThinOS a 9.0.

La siguiente tabla detalla las imágenes de firmware de ThinOS:

**Tabla 6. Imágenes de firmware**

Plataforma	Imagen de firmware de ThinOS
Cliente delgado Wyse 3040	A10Q_wnos
Cliente esbelto Wyse 5070; procesador Celeron	X10_wnos
Cliente esbelto Wyse 5070; procesador Pentium	X10_wnos
Cliente esbelto extendido Wyse 5070; procesador Pentium	X10_wnos
Cliente delgado Wyse 5470	X10_wnos
Cliente delgado Wyse 5470 todo en uno	X10_wnos

Identifíer	GUID-97A72AED-64BE-4EB3-8D9A-F91C87DFD0C8
Version	2
Status	Translation approved

## Agregar el firmware de ThinOS al repositorio

### Pasos

1. Inicie sesión en Wyse Management Suite mediante sus credenciales del grupo de usuarios.
2. En la pestaña **Aplicaciones y datos**, en **Repositorio de imágenes del SO**, haga clic en **ThinOS**.
3. Haga clic en **Agregar archivo de firmware**. Aparece la pantalla **Agregar archivo**.
4. Para seleccionar un archivo, haga clic en **Buscar** y vaya a la ubicación donde se encuentra el archivo.
5. Ingrese la descripción para el archivo.
6. Seleccione la casilla de verificación si desea invalidar un archivo existente.
7. Haga clic en **Cargar**.

**NOTA:**

- El firmware cargado solo se puede utilizar para actualizar ThinOS 8.6 a ThinOS 9.0.
- El archivo se agrega al repositorio cuando selecciona la casilla de verificación, pero no se asigna a ningún grupo o dispositivo. Para implementar el firmware en un dispositivo o un grupo de dispositivos, diríjase a la página de configuración del dispositivo o del grupo correspondiente.

Identifíer	GUID-E1883BA3-D2A4-4231-8E94-E5EE54CD5CA6
Version	3
Status	Translation in review

## Actualizar ThinOS 8.6 a ThinOS 9.x

### Requisitos previos

- Debe agregar la imagen de conversión de ThinOS al repositorio del firmware de ThinOS. Para obtener más información, consulte [Agregar el firmware de ThinOS al repositorio](#).
- Cree un grupo en Wyse Management Suite con un token de grupo. Utilice este token de grupo para registrar los dispositivos ThinOS 8.6.
- El cliente esbelto debe estar registrado en Wyse Management Suite.
- No configure ningún ajuste de fondo de pantalla en Wyse Management Suite.

### Pasos

1. Vaya a la página **Grupos y configuraciones** y seleccione un grupo.
2. En el menú desplegable **Editar políticas**, haga clic en **ThinOS**. Se muestra la ventana **Seleccionar modo de configuración de ThinOS**.
3. Seleccione **Modo de configuración avanzada**.
4. Vaya a **Actualización del firmware** y haga clic en **Configurar este elemento**.
5. Borre las opciones **Deshabilitar la actualización en directo** y **Verificar firma**.
6. En el menú desplegable **Tipo de plataforma**, seleccione la plataforma.
7. En la lista desplegable **Firmware para implementar automáticamente**, seleccione el firmware que agregó al repositorio.
8. Haga clic en **Guardar y publicar**. El firmware se implementa en el cliente esbelto. El proceso de conversión toma de 15 a 20 segundos y el cliente esbelto se reinicia automáticamente.

**NOTA:** Después de actualizar el firmware, el dispositivo se registra automáticamente en Wyse Management Suite. Las configuraciones de la versión 8.6 no se heredan después de actualizar el firmware.

Identifíer	GUID-28B1EB43-BC2A-49E6-BE12-76F42AE90417
Version	3
Status	Translation in review

## Actualización de ThinOS 9.x a versiones posteriores mediante Wyse Management Suite

### Requisitos previos

- Asegúrese de haber instalado la imagen ThinOS v9.0.1136 en el cliente delgado.
- Asegúrese de haber creado un grupo en Wyse Management Suite con un token de grupo. Utilice este token de grupo para registrar los dispositivos ThinOS 9.x.
- Asegúrese de que el cliente delgado se encuentre registrado en Wyse Management Suite.
- Asegúrese de que no configuró ningún ajuste de fondo de pantalla en Wyse Management Suite. Esto se aplica cuando se ejecuta ThinOS compilación 9.0.1136 y desea actualizar a la compilación 9.0.2081. Si el fondo de pantalla se configura simultáneamente con la imagen de ThinOS 9.0.2081, no se descarga el fondo de pantalla y se muestra un mensaje de error. Sin embargo, esto no afecta el proceso de actualización. Dell recomienda deshabilitar primero la configuración del fondo de pantalla, actualizar a 9.0.2081 y, luego, volver a configurar el fondo de pantalla.

### Pasos

1. Vaya a la página **Grupos y configuraciones** y seleccione un grupo.
2. En el menú desplegable **Editar políticas**, haga clic en **ThinOS 9.x**. Aparece la ventana **Control de configuración | ThinOS**.
3. Haga clic en **Opciones avanzadas**.
4. En el campo **Firmware**, seleccione **Actualizaciones de firmware del SO**.
5. Haga clic en **Navegar** para explorar y cargar el certificado.
6. En el menú desplegable **Seleccionar el firmware de ThinOS que se debe implementar**, seleccione el firmware que cargó.

7. Haga clic en **Guardar y publicar**.

El cliente esbelto descarga el firmware y se reinicia. La versión del firmware se actualizó.

Identifíer	GUID-D692B3D9-6597-46FA-BE24-B295B2A1724B
Version	8
Status	Translation in review

## Repositorio remoto

Wyse Management Suite le permite tener repositorios remotos y locales para aplicaciones, imágenes de sistemas operativos, entre otros. Si las cuentas de usuario se distribuyen entre zonas geográficas, sería conveniente tener un repositorio local separado para cada una de las cuentas de usuario distribuidas, de modo que los dispositivos puedan descargar imágenes desde su repositorio local. Esta flexibilidad se proporciona con el software `WMS_Repo.exe`. `WMS_Repo.exe` corresponde a un software repositorio de archivo de Wyse Management Suite que ayuda a crear repositorios remotos distribuidos, los cuales se pueden registrar con Wyse Management Suite. `WMS_Repo.exe` solo está disponible para los suscriptores de licencias **Pro**.

### Requisitos previos

Los requisitos de servidor para instalar el software de repositorio de Wyse Management Suite son los siguientes:

- Windows 2012 R2 o Windows 2016 Server
- 4 CPU
- 8 GB de RAM
- 40 GB de espacio de almacenamiento

### Sobre esta tarea

Realice lo siguiente para instalar el software **WMS-repo**:

### Pasos

1. Descargue el archivo `WMS_Repo.exe` desde Dell Digital Locker.
2. Inicie sesión como **Administrador** e instale `WMS_Repo.exe` en el servidor de repositorio.
3. Haga clic en **siguiente** y siga las instrucciones que aparecen en la pantalla para completar la instalación.
4. Haga clic en **Iniciar** para abrir la pantalla de **registro de WMS Repository** en el navegador web.

### Wyse Management Suite Repository

Registration

Register to Public WMS Management Portal

WMS Management Portal

Validate server certificate authority ⓘ

MQTT Server URL

Note: This field is only required when registering to WMS Server version 1.0. Later versions automatically retrieve mqtt url from the server.

WMS Repository URL

[Change Repository URL?](#)

Admin Name

Admin Password

Repository Location

Version: 3.0.0-33

**Ilustración 12. Detalles de registro**

5. Haga clic en **Registrarse** para iniciar el proceso de registro. Seleccione **Registrarse en el portal público de WMS Management** si se va a registrar en la nube pública.

### Wyse Management Suite Repository

Registration

Register to Public WMS Management Portal

WMS Server

WMS Repository URL  
 [Change Repository URL?](#)

Admin Name

Admin Password

Repository Location

Version: 3.0.0-33

**Ilustración 13. Registro en una nube pública**

6. Ingrese los siguientes detalles y haga clic en **Registrarse**:

a. URL del servidor de Wyse Management Suite

**NOTA: A menos que se registre con Wyse Management Suite v1.0, no podrá utilizar la URL del servidor MQTT.**

b.

c. URL de WMS Repository (actualice la URL con el nombre de dominio)

d. Información de nombre de usuario para el inicio de sesión del administrador de Wyse Management Suite

e. Información de contraseña para el inicio de sesión del administrador de Wyse Management Suite

f. Información de la ruta de acceso del repositorio

7. Si el registro se realizó correctamente, se mostrará la ventana **Registro**:

## Wyse Management Suite Repository

**Registration**

WMS Management Portal

WMS Repository URL

MQTT Server

Repository Location

Version: 3.0.0-33

**Unregister**

**Ilustración 14. Registro correcto**

- En la siguiente pantalla del portal de Wyse Management Suite se confirma que se ha completado correctamente el registro del repositorio remoto:

Portal Administration — File Repositories

**Console Settings**

- Active Directory (AD)
- Alert Classification
- Edge Gateway & Embedded PC Registration
- External App Services
- File Repository**
- Other Settings
- Thin Clients
- Teradici
- Two-Factor Authentication
- Reports

**User instructions**

Automatic Replication

	Active	Name/URL	Last Check-In	Version	Files	Notes	Others
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Local repository - WMSIP11 C:\WMS\LocalRepo	N/A	N/A	69		Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Subnets:
<input type="checkbox"/>	<input checked="" type="checkbox"/>	WMS Repo - wms63101 https://100.106.63.101:443	5 hours ago	2.0.0	62		Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Subnets:100.106.66.x, 100.106.63.x
<input type="checkbox"/>	<input checked="" type="checkbox"/>	WMS Repo - Repolp10 https://100.106.66.10:443	5 hours ago	2.0.0	70		Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Subnets:100.106.63.x, 100.106.66.x

**Ilustración 15. Registro correcto en el portal**

- El HTTPS se activa de manera predeterminada con `WMS_Repo.exe` y se instala con el certificado autofirmado. Para instalar su propio certificado específico de dominio, vaya a la parte inferior de la página de registro para cargar los certificados SSL.

Server SSL Certificates: Enabled SSL Certificate Guide

**Current Certificate**

Issued to: .....com  
Issued from: .....com  
Valid to: August 18, 2118

---

**PKCS-12** Key/Certificate Pair

---

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

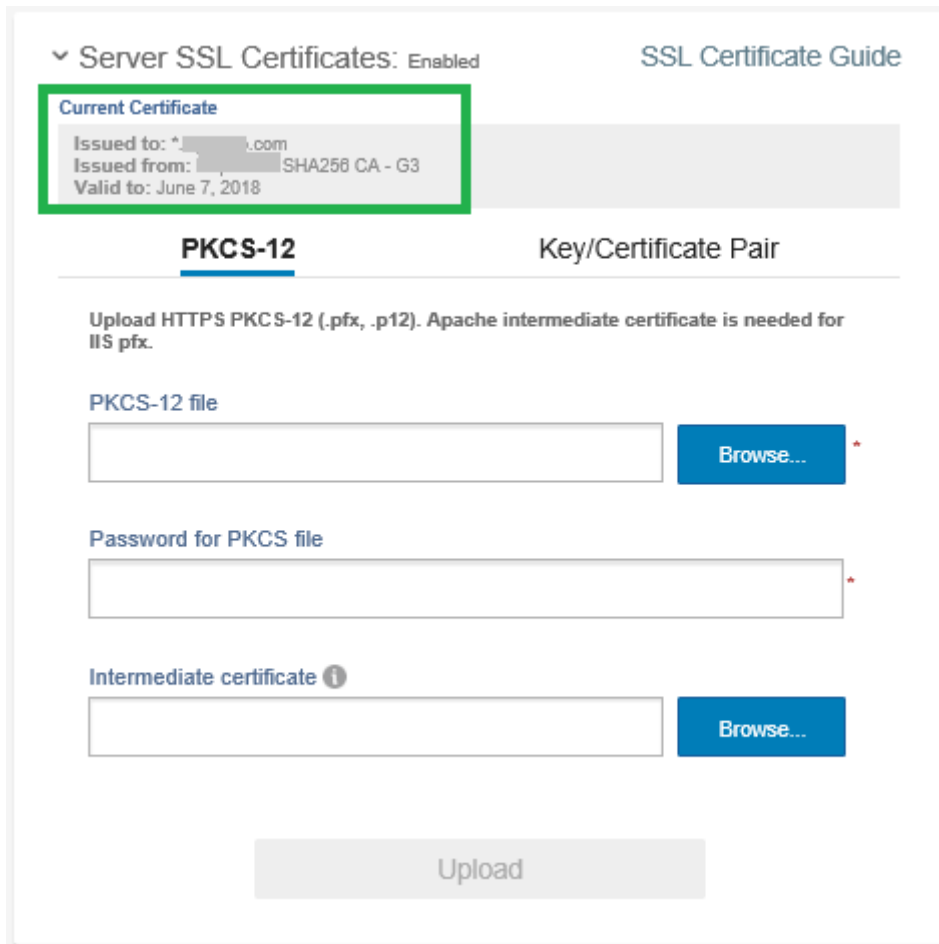
PKCS-12 file

Password for PKCS file

Intermediate certificate ⓘ

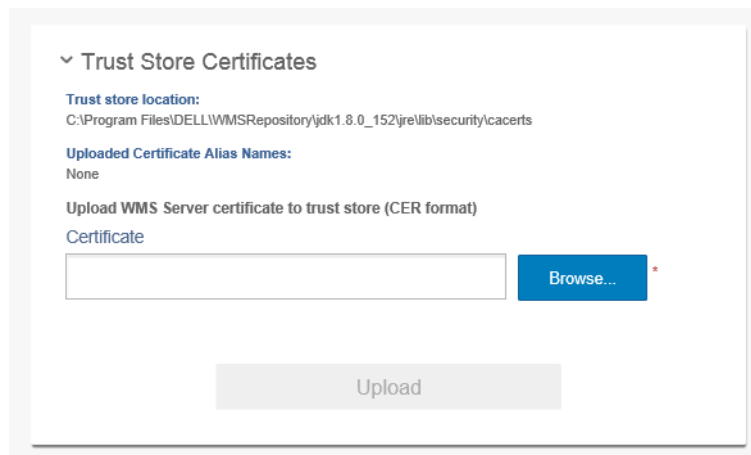
**Ilustración 16. Carga de certificados**

10. El servidor se reinicia y se muestra el certificado cargado.



**Ilustración 17. Certificado SSL activado**

- Si Wyse Management Suite está activado con un certificado autofirmado o uno de dominio privado, se puede cargar el certificado en el servidor de repositorio de Wyse Management Suite para validar las credenciales de CA de Wyse Management Suite.



**Ilustración 18. Certificados de almacén de confianza**

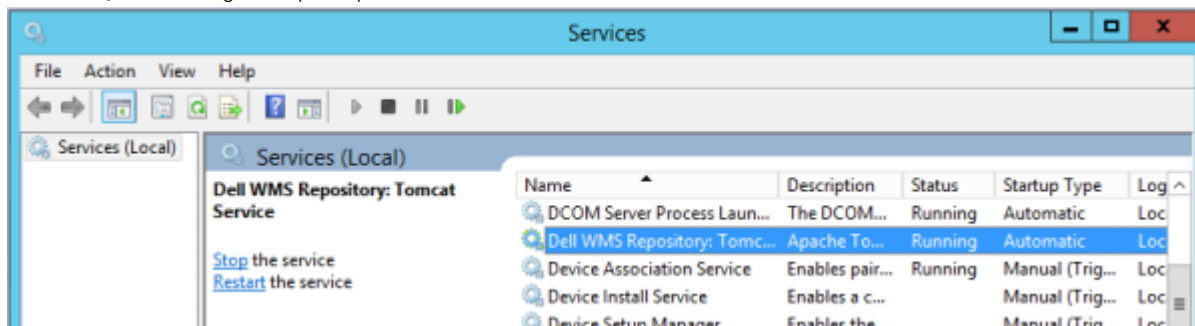
- Vaya a la ubicación `C:\wmsrepo` que haya ingresado durante el registro para ver las carpetas en las que se guardan y gestionan los archivos del repositorio.

**Temas:**

- Administración del servicio de repositorio de Wyse Management Suite

# Administración del servicio de repositorio de Wyse Management Suite

El repositorio de Wyse Management Suite aparece como **Dell WMS Repository: Tomcat Service** en la ventana de servicios locales de Windows y está configurado para que se inicie automáticamente cuando se reinicie el servidor como se muestra a continuación:



Identifíer	GUID-E3FCEFC7-C5FD-461F-8B26-3E898DFC9624
Version	1
Status	Translation approved

## Solución de problemas del dispositivo

Puede ver y administrar la información de solución de problemas mediante la página **Dispositivos**.

### Pasos

1. En la página **Detalles de los dispositivos**, haga clic en la pestaña **Solución de problemas**.
2. Haga clic en **Solicitar captura de pantalla**.  
Puede obtener una captura de pantalla del cliente esbelto con o sin permiso del cliente. Si selecciona la casilla de verificación **Necesita aceptación del usuario**, entonces aparece un mensaje en el cliente. Esta opción solo es válida para dispositivos Windows Embedded Standard, Linux y ThinLinux.
3. Haga clic en **Solicitar lista de procesos** para ver la lista de procesos que se ejecutan en el Thin client.
4. Haga clic en **Solicitar lista de servicios** para ver la lista de servicios que se ejecutan en el Thin client.
5. Haga clic en **Iniciar la supervisión** para acceder a la consola de métrica de rendimiento. En la consola de **Métrica de rendimiento**, se muestran los siguientes detalles:
  - Último minuto promedio de la CPU
  - Último minuto promedio de uso de la memoria

### Temas:

- [Solicitar un archivo de registro mediante Wyse Management Suite](#)
- [Ver registros de auditoría mediante Wyse Management Suite](#)
- [El dispositivo no se puede registrar en Wyse Management Suite cuando el proxy WinHTTP está configurado](#)
- [La política de redirección de USB RemoteFX no se aplica a dispositivos de almacenamiento masivo USB](#)

Identifíer	GUID-A2FFBE27-88F4-4CFE-B7A9-AC9640AF17CA
Version	1
Status	Translation approved


## Solicitar un archivo de registro mediante Wyse Management Suite

### Requisitos previos

El dispositivo debe estar activado para extraer el archivo de registro.

### Pasos

1. Vaya a la página **Dispositivos** y haga clic en un dispositivo particular.  
Se muestran los detalles del dispositivo.
2. Haga clic en la pestaña **Registro del dispositivo**.
3. Haga clic en **Solicitar archivo de registro**.
4. Después de cargar los archivos de registro en el servidor de Wyse Management Suite, haga clic en el enlace **Haga clic aquí** y descargue los registros.

 **NOTA:** El dispositivo ThinOS carga los registros del sistema.

Identifíer	GUID-61BC2BD6-D9EA-45F2-BA42-200C0DD23AF3
Version	1
Status	Translation approved

## Ver registros de auditoría mediante Wyse Management Suite

### Pasos

1. Vaya a **Eventos > Auditoría**.
2. En la lista desplegable **Grupos de configuración**, seleccione un grupo para el cual desee ver un registro de auditoría.
3. En la lista desplegable **Período**, seleccione el período para ver los eventos que ocurrieron durante ese tiempo.  
La ventana **Auditoría** ordena la información en una vista típica de registros de auditoría. Puede ver la marca de hora, el tipo de evento, la fuente y la descripción de cada evento en orden de hora.

Identifíer	GUID-DD2A57F0-CB12-4326-AF88-A1DA51900F6D
Version	1
Status	Translation approved

## El dispositivo no se puede registrar en Wyse Management Suite cuando el proxy WinHTTP está configurado

WDA es un Cliente WinHTTP y obtiene información del proxy WinHTTP desde el sistema local.

Si ha configurado el Proxy de WinHTTP y el dispositivo no puede comunicarse con el servidor de Wyse Management Suite, realice lo siguiente para habilitar la información del proxy disponible en el nivel del sistema:

- **Caso 1:** cuando el dispositivo se agregue a un dominio, habilite las configuraciones de IE-Proxy para cada usuario utilizando la política de grupo del dominio. Debe configurar la política de grupo desde la controladora de dominio para habilitar las configuraciones de IE-Proxy para cada cliente y no para cada usuario.

Consulte Configuración del Equipo\Plantillas Administrativas\Componentes de Windows\Internet Explorer\Realizar configuración de proxy por máquina, y seleccione **Activar**. Además, consulte Configuración de IE > Opciones de Internet > Conexiones > Configuración de LAN en Internet Explorer y habilite la **Configuración de detección automática**.

- **Caso 2:** cuando el dispositivo no se agregue a un dominio, consulte HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet y cree un **DWORD de 32 bits** llamado **ProxySettingsPerUser**; configúrelo en 0. Además, consulte Configuración de IE > Opciones de Internet > Conexiones > Configuración de LAN en Internet Explorer y habilite la **Configuración de detección automática**.

Identifíer	GUID-A74283C4-3441-45B2-9667-02D15BF7C627
Version	1
Status	Translation approved

## La política de redirección de USB RemoteFX no se aplica a dispositivos de almacenamiento masivo USB

### Pasos

1. Inicie sesión en el dispositivo como administrador.
2. Deshabilite el Filtro de escritura.
3. Vaya al comando **Ejecutar** y escriba **Regedit**.
4. Vaya a HKLM\Software\Policies\Microsoft\Windows NT\Terminal Services\Client\UsbSelectDeviceByInterfaces.

5. Agregue la clave de registro de la cadena como **100** y establezca el valor para el dispositivo de almacenamiento masivo como {53F56307-B6BF-11D0-94F2-00A0C91EFB8B} for CD ROM : {53F56308-B6BF-11D0-94F2-00A0C91EFB8B}.

 **NOTA: Los corchetes son obligatorios.**

Identifíer	GUID-7FB7FA7F-B2CD-4262-99D3-FB7D5D96D286
Version	1
Status	Translation approved

## Preguntas frecuentes

### Temas:

- ¿Qué tiene prioridad entre Wyse Management Suite y la interfaz del usuario de ThinOS cuando se aplica una configuración en conflicto?
- ¿Cómo utilizo el repositorio de archivos de Wyse Management Suite?
- ¿Cómo importo usuarios desde un archivo .csv?
- Cómo puedo verificar la versión de Wyse Management Suite
- Cómo crear y configurar etiquetas de opción de DHCP
- Cómo crear y configurar registros SRV de DNS
- Cómo cambiar el nombre de host a dirección IP
- Cómo creo una imagen del dispositivo mediante un repositorio remoto autofirmado

Identifíer	GUID-3A4492F6-A701-4E8C-A205-38B92BB766DA
Version	1
Status	Translation approved

## ¿Qué tiene prioridad entre Wyse Management Suite y la interfaz del usuario de ThinOS cuando se aplica una configuración en conflicto?

Cualquier ajuste configurado con Wyse Management Suite tiene prioridad sobre los ajustes que se configuraron localmente en el cliente de ThinOS o que se publicó mediante la herramienta de políticas de administración.

El siguiente orden define la prioridad establecida para las configuraciones de ThinOS:

**Políticas de Wyse Management Suite > Herramienta de políticas de administración > IU de ThinOS local**

Identifíer	GUID-6110FE95-707C-44C7-8A0A-9F2ADE46B5F4
Version	1
Status	Translation approved

## ¿Cómo utilizo el repositorio de archivos de Wyse Management Suite?

### Pasos

1. Descargue el repositorio de Wyse Management Suite de la consola de la nube pública.
2. Después del proceso de instalación, inicie la aplicación.
3. En la página del repositorio de Wyse Management Suite, ingrese las credenciales para registrar el repositorio de Wyse Management Suite en el servidor de Wyse Management Suite.
4. Para registrar el repositorio en la nube pública de Wyse Management Suite, habilite la opción **Registrar en el portal de administración del WMS público**.
5. Haga clic en la opción **Sincronizar archivos** para enviar el comando de sincronización de archivos.
6. Haga clic en **Registrar** y luego en **Enviar comando** para enviar el comando de información del dispositivo al dispositivo.
7. Haga clic en la opción **Anular el registro** para anular el registro el servicio in situ.

8. Haga clic en **Editar** para editar los archivos.
  - a. En la lista desplegable de la opción **Descargas de archivo simultáneas**, seleccione el número de archivos.
  - b. Active o desactive la opción **Wake on LAN**.
  - c. Active o desactive la opción **Carga y descarga rápida de archivos (HTTP)**.
    - Cuando HTTP está activado, la carga y la descarga de archivos ocurren por medio de HTTP.
    - Cuando HTTP está no está activado, la carga y la descarga de archivos ocurren por medio de HTTPS.
  - d. Seleccione la casilla de verificación **Validación del certificado** para habilitar la validación de CA para una nube pública.

**NOTA:**

- **Cuando se habilita la validación de CA desde el servidor de Wyse Management Suite, el certificado debe estar presente en el cliente. Todas las operaciones, como aplicaciones y datos, extracción/inserción de imágenes, se realizan correctamente. Si el certificado no está presente en el cliente, el servidor de Wyse Management Suite proporciona un mensaje de evento de auditoría genérico Se produjo un error al validar la autoridad de certificación en la página Eventos. Todas las operaciones, como aplicaciones y datos, extracción/inserción de imágenes, no se realizan correctamente.**
- **Cuando se deshabilita la validación de CA desde el servidor de Wyse Management Suite, la comunicación del servidor y el cliente se produce en un canal seguro sin la validación de la firma del certificado.**

- e. Agregue una nota en el cuadro disponible.
- f. Haga clic en **Guardar configuración**.

Identifier	GUID-B56D24B3-D9CF-49F6-B574-60B335984C15
Version	1
Status	Translation approved

## ¿Cómo importo usuarios desde un archivo .csv?

### Pasos

1. Haga clic en **Usuarios**.  
Se muestra la página **Usuarios**.
2. Seleccione la opción **Administrador con asignación cancelada**.
3. Haga clic en **Importación masiva**.  
Aparece la ventana **Importación masiva**.
4. Haga clic en **Buscar** y seleccione el archivo .csv.
5. Haga clic en **Importar**.

Identifier	GUID-607E97A0-870F-419F-828C-2D50BAC6C59A
Version	1
Status	Translation approved

## Cómo puedo verificar la versión de Wyse Management Suite

### Pasos

1. Inicie sesión en Wyse Management Suite.
2. Vaya a **Administración del portal > Suscripción**.  
La versión de Wyse Management Suite se muestra en el campo **Información del servidor**.

Identifíer	GUID-401CA5F7-9191-48EE-9594-992952FD8E8A
Version	1
Status	Translation approved

# Cómo crear y configurar etiquetas de opción de DHCP

## Pasos

1. Abra el Administrador de servidores.
2. Vaya a **Herramientas** y haga clic en **Opción DHCP**.
3. Vaya a **FQDN > IPv4** y haga clic con el botón secundario en **IPv4**.
4. Haga clic en **Establecer opciones predefinidas**.  
Se muestra la ventana **Opciones y valores predefinidos**.
5. En la lista desplegable **Clase de opción**, seleccione el valor **Opción estándar de DHCP**.
6. Haga clic en **Agregar**.  
Se muestra la ventana **Tipo de opción**.
7. Configure las etiquetas de opción de DHCP que se requieran.
  - Para crear la etiqueta de opción de URL del servidor Wyse Management Suite 165, haga lo siguiente:
    - a. Ingrese los siguientes valores y haga clic en **Aceptar**.
      - Nombre: WMS
      - Tipo de datos: cadena
      - Código: 165
      - Descripción: servidor WMS
    - b. Ingrese el siguiente valor y, a continuación, haga clic en **Aceptar**.  
Cadena: WMS FQDN  
  
Por ejemplo, **WMSServerName.YourDomain.Com:443**
  - Para crear la etiqueta de opción de URL del servidor MQTT 166, haga lo siguiente:
    - a. Ingrese los siguientes valores y haga clic en **Aceptar**.
      - Nombre: MQTT
      - Tipo de datos: cadena
      - Código: 166
      - Descripción: servidor de MQTT
    - b. Ingrese el siguiente valor y haga clic en **Aceptar**.  
Cadena: MQTT FQDN  
  
Por ejemplo, **WMSServerName.YourDomain.Com:1883**
  - Para crear la etiqueta de opción de URL de la validación de CA de Wyse Management Suite 167, haga lo siguiente:
    - a. Ingrese los siguientes valores y haga clic en **Aceptar**.
      - Nombre: Validación de CA
      - Tipo de datos: cadena
      - Código: 167
      - Descripción: validación de CA
    - b. Ingrese los siguientes valores y haga clic en **Aceptar**.  
Cadena: VERDADERO o FALSO
  - Para crear la etiqueta de opción de URL del token de grupo de Wyse Management Suite 199, haga lo siguiente:
    - a. Ingrese los siguientes valores y haga clic en **Aceptar**.
      - Nombre: token de grupo
      - Tipo de datos: cadena
      - Código: 199
      - Descripción: token de grupo
    - b. Ingrese los siguientes valores y haga clic en **Aceptar**.

String—defa-quarantine



**NOTA:** Las opciones se deben agregar en las opciones del servidor DHCP o deben abarcar opciones dentro del alcance de DHCP.

Identifier	GUID-CAA17DCA-3BBD-49CE-92A1-35D96C700DBD
Version	1
Status	Translation approved

## Cómo crear y configurar registros SRV de DNS

### Pasos

1. Abra el Administrador de servidores.
2. Vaya a **Herramientas** y haga clic en **DNS**.
3. Vaya a **DNS > Nombre de host del servidor DNS > Reenviar zonas de búsqueda > Dominio > \_tcp**, y haga clic con el botón secundario en la opción **\_tcp**.
4. Haga clic en **Otros registros nuevos**.  
Se muestra la ventana **Tipo de registro de recursos**.
5. Seleccione la **Ubicación del servicio (SRV)**, haga clic en **Crear registro** y haga lo siguiente:
  - a. Para crear un registro del servidor Wyse Management Suite, ingrese los siguientes detalles y haga clic en **Aceptar**.
    - Servicio: **\_WMS\_MGMT**
    - Protocolo: **\_tcp**
    - Número de puerto: **443**
    - Host que ofrece este servicio: **FQDN o servidor de WMS**
  - b. Para crear el registro del servidor MQTT, ingrese los siguientes valores y luego haga clic en **Aceptar**.
    - Servicio: **\_WMS\_MQTT**
    - Protocolo: **\_tcp**
    - Número de puerto: **1883**
    - Host que ofrece este servicio: **FQDN o servidor MQTT**
6. Vaya a **DNS > Nombre de host del servidor DNS > Reenviar zonas de búsqueda > Dominio** y haga clic con el botón secundario en el dominio.
7. Haga clic en **Otros registros nuevos**.
8. Seleccione **Texto (TXT)**, haga clic en **Crear registro** y haga lo siguiente:
  - a. Para crear un registro del token de grupo de Wyse Management Suite, ingrese los siguientes valores y haga clic en **Aceptar**.
    - Nombre de registro: **\_WMS\_GROUPTOKEN**
    - Texto: **token de grupo WMS**
  - b. Para crear un registro de validación de CA de Wyse Management Suite, ingrese los siguientes valores y haga clic en **Aceptar**.
    - Nombre de registro: **\_WMS\_CAVALIDATION**
    - Texto: **VERDADERO/FALSO**

Identifier	GUID-804FC90E-F005-4A92-BA7D-0E333B3383D4
Version	1
Status	Translation approved

## Cómo cambiar el nombre de host a dirección IP

### Sobre esta tarea

Debe cambiar el nombre de host a dirección IP cuando falla la resolución del nombre de host.

### Pasos

1. Abra el símbolo del sistema DOS en un modo de administrador alto.
2. Cambie el directorio a **C:\Program Files\DELL\WMS\MongoDB\bin**.

3. Ingrese el comando `mongo localhost -username stratus -p --authenticationDatabase admin`  
Salida: shell de MongoDB, versión v3.4.10
4. Introduzca la contraseña.  
Salida:
  - conectándose a mongod://127.0.0.1:27017/localhost
  - Servidor de MongoDB versión 3.4.10
5. Ingrese: use stratus  
Salida: cambiada a db stratus
6. Ingrese el comando `> db.bootstrapProperties.updateOne( {'name': 'stratusapp.server.url'}, { $set : {'value' : "https://IP:443/ccm-web"} } )`  
Salida: { "acknowledged" : true, "matchedCount" : 1, "modifiedCount" : 1 }
7. Ingrese el comando `> db.getCollection('bootstrapProperties').find({'name': 'stratusapp.server.url'})`  
Salida: { "\_id" : ObjectId("5b97905e48b7b7e99ad22aa6"), "name" : "stratusapp.server.url", "value" : "https://IP:443/ccm-web", "isActive" : true, "committed" : true }

Identifier	GUID-61DF420D-6BAE-4D87-9987-CCFF92433040
Version	1
Status	Translation approved

## Cómo creo una imagen del dispositivo mediante un repositorio remoto autofirmado

Puede crear imágenes de dispositivos Windows Embedded Standard y ThinLinux desde el repositorio local de la nube privada o desde el repositorio remoto de la nube pública.

### Requisitos previos

Si la imagen se implementa desde el repositorio local de la nube privada o desde el repositorio remoto de la nube pública con un certificado autofirmado, el administrador debe enviar el certificado autofirmado a los clientes esbeltos para realizar imágenes cuando la validación de CA está activada.

### Pasos

1. Exporte el certificado autofirmado desde Internet Explorer o MMC.
2. Cargue el certificado en Wyse Management Suite: consulte [Política de imagen](#).
3. Inserte el certificado en los clientes o grupos de clientes de destino mediante la política de seguridad. Espere hasta que finalice el **Trabajo de la política de configuración**.
4. Active la validación de CA desde el repositorio local de la nube privada o desde el repositorio remoto de la nube pública.
5. Cree una política de imágenes y prográmela en el grupo.