Dell Wyse Management Suite

Guía de inicio rápido versión 3.x

Febrero de 2022
Rev. A05

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

1

Introducción

Wyse Management Suite es la solución de administración de última generación que le permite configurar, controlar, administrar y optimizar de forma centralizada las terminales que usan Dell Hybrid Client y los clientes delgados Dell. 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.

Ediciones

Wyse Management Suite se encuentra disponible en las siguientes ediciones:

- **Estándar (gratuita)**: la edición estándar de Wyse Management Suite ofrece funciones básicas y se encuentra disponible para una implementación en nube privada. No se requiere una clave de licencia para usar la edición Estándar. Esta versión puede administrar clientes delgados Dell. La edición estándar es apropiada para empresas pequeñas y medianas.
- **Pro (pagada)**: la edición pro de Wyse Management Suite es una solución más completa. Está disponible para la implementación en nube pública y privada. Se requiere una clave de licencia para usar la edición Pro (licencia basada en suscripción). Con la solución Pro, las organizaciones pueden adoptar un modelo híbrido y usar licencias entre nubes públicas y privadas de ser necesario. Esta versión es necesaria para administrar cualquier dispositivo basado en Teradici, Wyse Covert for PCs y dispositivos que usan Dell Hybrid Client. También ofrece funciones más avanzadas para administrar clientes delgados Dell. Para una implementación en la nube pública, la edición Pro se puede administrar en redes no corporativas (oficina en el hogar, terceros, socios y clientes delgados móviles, entre otros). 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 mediante autentificación de dos factores y autentificación de Active Directory para una administración basada en funciones
  - Política de aplicación y generación de informes avanzadas.

  NOTA:
  - Los servicios en la nube se alojan en los Estados Unidos y Alemania. Es posible que los clientes en países con restricciones de residencia de datos no puedan aprovechar el servicio basado en la nube de Wyse Management Suite edición Pro.
  - La versión local de Wyse Management edición Pro es una mejor solución para los clientes con restricciones de residencia de datos.

Temas:

Matriz de funciones de Wyse Management Suite

En la siguiente tabla, se proporciona información sobre las funciones incluidas en 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	Liberar hasta 10 000 dispositivos	Hasta 120 000 dispositivos	Hasta 1 millón dispositivos
Término de la licencia	Descarga gratuita	Suscripción por computadora	Suscripción por computadora
Clave de licencia	No se requiere	Requerido	Requerido

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

Características	Wyse Management Suite Standard	Wyse Management Suite Pro: nube privada	Wyse Management Suite Pro: edición en nube
Arquitectura	Nube privada	Nube privada	Nube pública
Implementación flexible o nube híbrida	X	√	√
Instalador avanzado	X	√	√
Varios inquilinos	X	√	√
Administración delegada para la granularidad de permisos	X	√	√
Varios repositorios para admitir la arquitectura distribuida	X	√	√
Opción para configurar un alias del servidor de Wyse Management Suite	X	√	√
Arquitectura de referencia de alta disponibilidad	X	√	X
Compatibilidad con proxy: SOCKS5 y HTTPS	√	√	√
Soporte de API	X	√	X
Dell ProSupport for Software incluido	X	√	√
Terminal Dell			
OptiPlex 7070 Ultra con cliente híbrido Dell	X	√	√
OptiPlex 3090 Ultra y 7090 Ultra con cliente híbrido Dell	X	√	√
Latitude 3320 con cliente híbrido Dell	X	√	√
Wyse 5070 con cliente híbrido Dell	X	√	√
Clientes delgados Wyse con ThinOS	√	√	√
Clientes delgados Wyse con ThinLinux	√	√	√
Clientes delgados Wyse con Windows 10 IoT Enterprise	√	√	√
Wyse PCoIP zero clients (firmware Teradici)	X	√	√
Clientes ligeros de software con Wyse Converter for PCs	X	√	√
Generación de informes y monitoreo			
Consola de administración localizada	X	√	√
Alertas, eventos y registros de auditoría mediante correo electrónico y aplicaciones móviles	X	√	√
Generación de informes de categoría empresarial	X	√	√

En la siguiente tabla, se proporciona información sobre las funciones de administración de Dell Hybrid Client incluidas en cada tipo de suscripción.

Tabla 2. Matriz de funciones de administración de Dell Hybrid Client

Funciones de administración de Dell Hybrid Client	Wyse Management Suite Standard	Wyse Management Suite Pro: nube privada	Wyse Management Suite Pro: edición en nube
Visibilidad de activos completa			
Detección automática de dispositivos	X	√	√
Administración de activos, inventario y sistemas	X	√	√
Visualización de la configuración efectiva a nivel de dispositivo de Wyse Management Suite de después de la herencia	X	√	√
Seguridad			
Comunicación segura (HTTPS)	X	√	√
MQTT seguro	X	√	√
Autenticación de multifactor	X	√	√
Autenticación de Active Directory para administración basada en roles	X	√	√
Asignación de AD mediante LDAP	X	√	√
Single Sign On	X	√	√
Ajustes de bloqueo (habilitar/ deshabilitar puertos de extremos admitidos)	X	√	√
Administración integral			
Administración de parches e imágenes de sistema operativo	X	√	√
Programación inteligente	X	√	√
Implementación silenciosa	X	√	√
Aplicaciones en paquete para simplificar la implementación y minimizar los reinicios	X	√	√
Creación y asignación dinámicas de grupos según los atributos del dispositivo	X	√	√
Asignación del repositorio a la política de la aplicación y mapeo de subred	X	√	√
Administración avanzada de aplicaciones y política de aplicaciones	X	√	√
Herencia de grupos de usuarios	X	√	√
Excepción de usuario final	X	√	√

Tabla 2. Matriz de funciones de administración de Dell Hybrid Client (continuación)

Funciones de administración de Dell Hybrid Client	Wyse Management Suite Standard	Wyse Management Suite Pro: nube privada	Wyse Management Suite Pro: edición en nube
Anulación automática del registro de dispositivos	X	√	√
Configuración			
Configuración de Dell Hybrid Client con asistente	X	√	√
Compatibilidad con varios monitores	X	√	√
Perfil de seguimiento	X	√	√
Afiliación del archivo para priorizar el modo de entrega de la aplicación	X	√	√
Soporte para la configuración y los ajustes del BIOS	X	√	√
Configuraciones de política de exportación o importación	X	√	√
Política de grupo de usuarios predeterminada	X	√	√
Configuración del navegador	X	√	√
Configuración del proveedor de servicio en la nube	X	√	√
Actualización automática de aplicaciones firmadas por Dell	X	√	√
Roaming de datos de personalización de usuario	X	√	√
Configurar VNC	X	√	√
Configurar SSH	X	√	√

NOTA: Dell Technologies recomienda actualizar el sistema a 12 GB de RAM, ya que se requiere más memoria para permitir la comunicación segura.

NOTA: Para obtener una licencia estándar, puede utilizar una conexión MQTT segura (8443) bloqueando el puerto 1883 desde el servidor de Wyse Management Suite mediante el firewall de Windows.

En la siguiente tabla, se proporciona información sobre las funciones de administración de clientes delgados Wyse y clientes cero incluidos en cada suscripción.

Tabla 3. Matriz de funciones de administración de clientes delgados Wyse y clientes cero

Funciones de administración de clientes delgados Wyse y clientes cero	Wyse Management Suite Standard	Wyse Management Suite Pro: nube privada	Wyse Management Suite Pro: edición en nube
Visibilidad de activos completa			
Detección automática de dispositivos	√	√	√
Administración de activos, inventario y sistemas	√	√	√

Tabla 3. Matriz de funciones de administración de clientes delgados Wyse y clientes cero (continuación)

Funciones de administración de clientes delgados Wyse y clientes cero	Wyse Management Suite Standard	Wyse Management Suite Pro: nube privada	Wyse Management Suite Pro: edición en nube
Ver configuración efectiva a nivel del dispositivo después de la herencia	√	√	√
Generación de informes y monitoreo			
Vigilancia remota mediante VNC	√	√	
Latido configurable e intervalo de verificación	√	√	√
Seguridad			
Comunicación segura (HTTPS)	√	√	√
Implementación de certificado de 802.1x	√	√	√
MQTT seguro	√	√	√
Autentificación de dos factores	X	√	√
Autenticación de Active Directory para administración basada en roles	X	√	√
Función de unión de dominio (Windows 10 IoT Enterprise)	X	√	√
Asignación de AD mediante LDAP	X	√	√
Ajustes de bloqueo (habilitar o deshabilitar de puertos de extremos admitidos)	X	√	√
Administración integral			
Administración de parches e imágenes de sistema operativo	√	√	√ **
Programación inteligente	√	√	√
Implementación silenciosa	√	√	√
Aplicaciones en paquete para simplificar la implementación y minimizar los reinicios	X	√	√
Creación y asignación dinámicas de grupos según los atributos del dispositivo	X	√	√
Asignación del repositorio a la política de la aplicación y mapeo de subred	X	√	√
Anulación automática del registro de dispositivos	√	√	√
Política de aplicación avanzada	X	√	√
Configuración			
Configuración de Wyse ThinOS 8.x y 9.x con asistente	√	√	√

Tabla 3. Matriz de funciones de administración de clientes delgados Wyse y clientes cero (continuación)

Funciones de administración de clientes delgados Wyse y clientes cero	Wyse Management Suite Standard	Wyse Management Suite Pro: nube privada	Wyse Management Suite Pro: edición en nube
Compatibilidad con varios monitores	√	√	√
Wyse Easy Setup y Wyse Overlay Optimizer	√	√	√
Soporte de scripts para personalizar la instalación de la aplicación	X	√	√
Soporte para la configuración y los ajustes del BIOS	X	√	√
Configuraciones de política de exportación e importación	X	√	√
Soporte de paquete RSP	X	√	√
Herramienta de importación de WDM	X	√	X
Excepción de dispositivo masivo	X	√	√

NOTA: ** Un asterisco doble indica que para los sistemas operativos ThinLinux y Windows 10 IoT Enterprise, se requiere un repositorio en las instalaciones cuando se utiliza el entorno de nube pública de Wyse Management Suite.

NOTA: Dell Technologies recomienda actualizar el sistema a 12 GB de RAM, ya que se requiere más memoria para permitir la comunicación segura.

NOTA: Para obtener una licencia estándar, puede utilizar una conexión MQTT segura (8443) bloqueando el puerto 1883 desde el servidor de Wyse Management Suite mediante el firewall de Windows.

NOTA: ThinOS 9.1.x, Dell Hybrid Client 1.5 y versiones posteriores, Wyse Device Agent 14.5.3.11 y versiones posteriores soportan MQTT seguro.

2

Introducción a Wyse Management Suite

En esta sección se entrega información sobre las funciones generales que lo ayudarán a desempeñarse como administrador y a administrar clientes delgados desde el software de Wyse Management Suite.

Temas:

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
   - **Centro de datos de la Unión Europea:** 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 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.

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**.

Requisitos previos para implementar Wyse Management Suite en la nube privada

Tabla 4. 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. El servidor web de Wyse Management Suite tiene un servidor web Apache Tomcat incorporado. Asegúrese de no instalar Microsoft IIS ni servidores web Apache Tomcat por separado. 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	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. ● TCP 443: comunicación HTTPS ● TCP 1883: comunicación MQTT ● TCP 3306: MariaDB (opcional si es remoto) ● TCP 27017: MongoDB (opcional si es remoto) ● TCP 11211: Memcached ● TCP 5172, 49159; Software Development Kit de administración de usuario final (EMSDK): opcional y se requiere solo para administrar los dispositivos Teradici Es posible que se cambien los puertos predeterminados que utiliza el instalador por uno alternativo durante la instalación.			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.
Navegadores compatibles	Internet Explorer versión 11 Google Chrome versión 58.0 y posteriores Mozilla Firefox versión 52.0 y posteriores Navegador Edge en Windows: solo inglés			

- 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.

NOTA: Para la configuración de 10 000 dispositivos, la memoria mínima (RAM) debe ser de 12 GB para las comunicaciones de MQTT seguro.

NOTA: Desde Wyse Management Suite 3.3, debe usar la versión 4.2.12 de MongoDB para las configuraciones distribuidas. No puede instalar ni actualizar Wyse Management Suite versión 3.3 mediante cualquier otra versión del servidor de MongoDB externo.

NOTA: La instalación del servidor y del repositorio de Wyse Management Suite no está soportada en los servidores alojados en la nube, como Azure, Amazon Web Services y Google Cloud Platform.

3

Instalación de Wyse Management Suite en nube privada

Requisitos previos

- Obtener y configurar todo el hardware y software necesarios. Puede descargar el software de Wyse Management Suite desde downloads.dell.com/wyse/wms.
- Instalar un sistema operativo de servidor compatible en uno o más equipos servidores.
- Asegúrese de que los sistemas están actualizados con los más recientes paquetes de servicio, parches y actualizaciones de Microsoft.
- Asegúrese de instalar la última versión del explorador compatible.
- Obtenga credenciales y derechos de administrador en todos los sistemas relacionados con los procedimientos de instalación.
- Para las funciones de Pro, obtenga una licencia válida de Wyse Management Suite. La edicion Estándar no requiere una licencia.
- Asegúrese de que haya suficiente espacio en la unidad en la cual está instalado Wyse Management Suite y que el repositorio local esté configurado.
- Si instaló o configuró algún antivirus u otra herramienta de monitoreo en la configuración de Wyse Management Suite, Dell Technologies recomienda desactivar las herramientas temporalmente hasta que se complete la actualización. También puede agregar una exclusión correspondiente para el directorio de instalación, el directorio temporal y el directorio del repositorio local de Wyse Management Suite.

Sobre esta tarea

Una instalación sencilla de Wyse Management Suite consiste en lo siguiente:

- Servidor de Wyse Management Suite (incluye repositorio para aplicaciones e imágenes de sistema operativo)
- Opcional: servidores adicionales del repositorio de Wyse Management Suite (repositorios para imágenes, aplicaciones y autentificación AD adicionales)
- Opcional: certificado HTTPS de una autoridad de certificación como www.geotrust.com/.

Pasos

1. Haga doble clic en el paquete del instalador.
2. En la pantalla de **Bienvenida**, haga clic en **Siguiente**.
   Aparecerán los detalles del **EULA**.
   NOTA: Esta pantalla solo se muestra en Wyse Management Suite versión 3.1 o posterior.
3. Lea el acuerdo de licencia.
4. Seleccione la casilla de verificación **Acepto los términos del contrato de licencia** y haga clic en **Siguiente**.
5. En la página **Tipo de configuración**, seleccione los componentes que desea instalar y haga clic en **Siguiente**. Las opciones posibles son:
   - Wyse Management Suite: hay dos tipos de configuración disponibles para los componentes de Wyse Management Suite.
     - Típica: necesita un mínimo de interacción del usuario e instala bases de datos integradas.
     - Personalizada: requiere la interacción completa del usuario y se recomienda para usuarios avanzados. Para obtener más información, consulte Instalación personalizada.
   - Teradici EM SDK: los componentes de Teradici EM SDK se instalan como servicio.

   NOTA: Cuando la función Configuración de seguridad mejorada de Internet Explorer está habilitada, se muestra una ventana de notificación. Para desactivar esta función, seleccione la casilla de verificación **Apagar configuración de seguridad mejorada de IE** en la página **Tipo de instalación**.

   Si EM SDK está instalado en el servidor junto con Wyse Management Suite de una instalación anterior, los componentes de Teradici EM SDK se actualizan automáticamente.
6. Seleccione **Típica** como su **tipo de instalación**.
7. Ingrese las nuevas **Credenciales de la base de datos** para las bases de datos integradas y las nuevas **Credenciales de administrador**, y haga clic en **Siguiente.**

NOTA: Se requieren credenciales de administrador para iniciar sesión en la consola web de Wyse Management Suite después de la instalación.

8. En la página **Configuración**, haga lo siguiente:
   a. Configure los derechos de acceso y las carpetas compartidas para el usuario de CIFS. Las opciones posibles son:
      - **Utilizar un usuario existente**: seleccione esta opción para validar las credenciales del usuario existente.
      - **Crear un nuevo usuario**: seleccione esta opción e ingrese las credenciales para crear un nuevo usuario.

        La contraseña debe tener más de ocho caracteres.

        NOTA: Si la opción **Teradici EM SDK** está habilitada en la página **Tipo de configuración**, puede configurar el puerto del servidor Teradici en la página **Configuración**.

   b. Haga clic en **Siguiente**.

      Aparecerá la pantalla **Credenciales de cuenta de usuario** con las siguientes opciones:
      - **Crear un nuevo usuario local**: seleccione esta opción para ingresar las credenciales y crear un nuevo usuario local con los privilegios mínimos. El nuevo usuario se agrega al grupo **Usuarios**, pero no tendrá derechos de administrador.

        NOTA: El nombre de usuario que ingrese en la pantalla **Credenciales de la cuenta de servicio** no debe ser el mismo que el nombre de usuario de Teradici. El nombre de usuario debe tener entre 2 y 20 caracteres. La contraseña debe tener entre 9 y 127 caracteres con al menos una mayúscula, una minúscula, un número y un carácter especial. No se permite colocar espacios en la contraseña.
      - **Usar un usuario local existente**: seleccione esta opción para ingresar las credenciales de un usuario local existente. Cuando seleccione esta opción, se mostrará un mensaje. Procure que el usuario ya exista, tenga derechos de inicio de sesión de servicio (**SeServiceLogonRight**) y haya iniciado sesión correctamente al menos una vez en el sistema. Dell Technologies recomienda procurar que el usuario no tenga derechos administrativos.

        NOTA: Si selecciona esta opción, la complejidad de la contraseña no se verifica y el nombre de usuario que ingrese debe tener entre 2 y 20 caracteres.
      - **Usar un usuario de dominio existente**: seleccione esta opción para ingresar las credenciales de un usuario de dominio existente. Cuando seleccione esta opción, se mostrará un mensaje. Procure que el usuario ya exista en el dominio, tenga derechos de inicio de sesión de servicio (**SeServiceLogonRight**) y haya iniciado sesión correctamente al menos una vez en el sistema. Dell Technologies recomienda procurar que el usuario no tenga derechos administrativos.

        NOTA: Si selecciona esta opción, no se verifica la complejidad de la contraseña.

   c. Haga clic en **Siguiente** después de ingresar las credenciales.
      Aparece la pantalla **Credenciales del vault de software**. El vault de software se utiliza para almacenar datos confidenciales requeridos por la aplicación Dell Wyse Management Suite.
   d. Ingrese la contraseña del vault de software.
      La contraseña debe tener más de ocho caracteres.
   e. Haga clic en **Siguiente**.
9. Asegúrese de seleccionar todas las versiones adecuadas de TLS según los criterios de soporte de los dispositivos que se están administrando.

   NOTA: La versión de WDA inferior a WDA_14.4.0.135_Unified, la herramienta Importar y la imagen Merlin de 32 bits no son compatibles con TLSv1.1 y versiones posteriores. Seleccione TLSv1.0 si el entorno Wyse Management Suite tiene dispositivos con una versión anterior de WDA, la herramienta Importar o dispositivos instalados con la imagen Merlin de 32 bits.

10. Navegue hasta la ubicación donde desea instalar el software y el repositorio de archivos de grupo de usuarios local y, a continuación, haga clic en **Siguiente.**

    La ruta de acceso predeterminada de la carpeta de destino para instalar el software es `C:\Program Files\DELL\WMS`.
11. Haga clic en **Siguiente**.
    Se mostrará la página **Resumen previo a la instalación**.
12. Haga clic en **Siguiente** para instalar el software.

    El instalador tarda aproximadamente entre 4 y 5 minutos para completar la instalación. Sin embargo, puede tardar más tiempo si los componentes dependientes como VC-runtime no están instalados en el sistema.
13. Haga clic en **Iniciar** para abrir la consola web de Wyse Management Suite.
14. En la consola web, haga clic en **Introducción**.

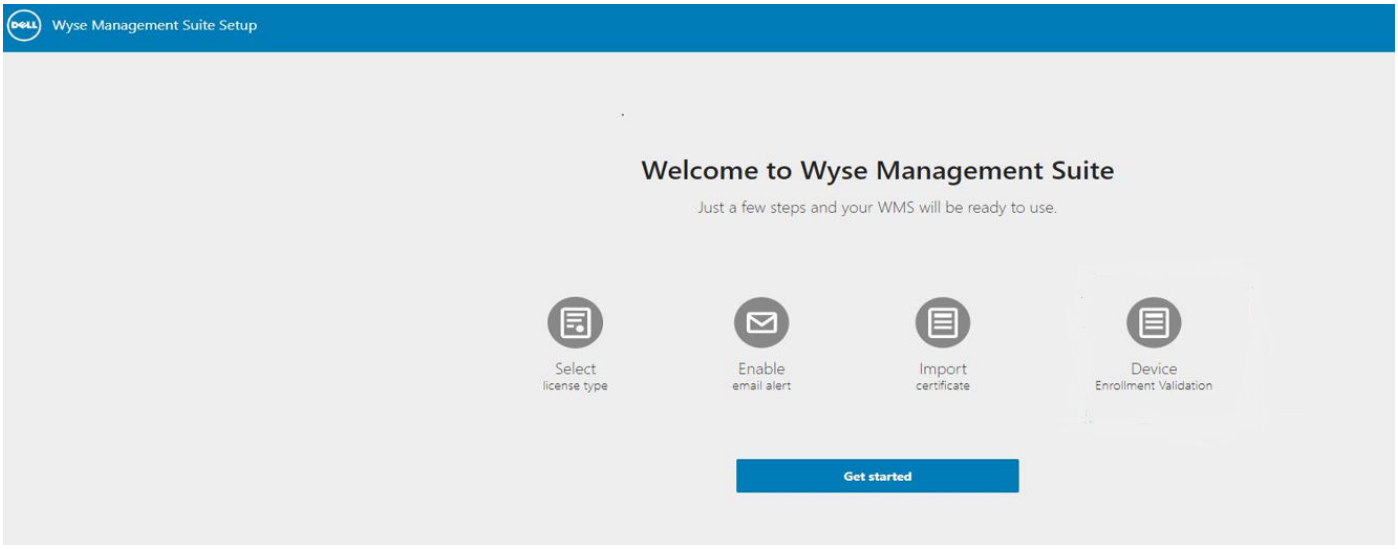

Ilustración 1. Página de bienvenida

15. Seleccione su licencia preferida.
    - Si selecciona el tipo de licencia **Estándar**, puede hacer clic en **Siguiente** para continuar con la instalación estándar de Wyse Management Suite.
    - Si selecciona el tipo de licencia **Pro**, debe importar una licencia válida de Wyse Management Suite. Para importar la licencia de Wyse Management Suite, ingrese la información solicitada para importar la licencia si el servidor tiene conectividad a Internet. También puede generar la clave de licencia si inicia sesión en el portal de nube pública de Wyse Management Suite e ingresa la clave en el campo Clave de licencia.

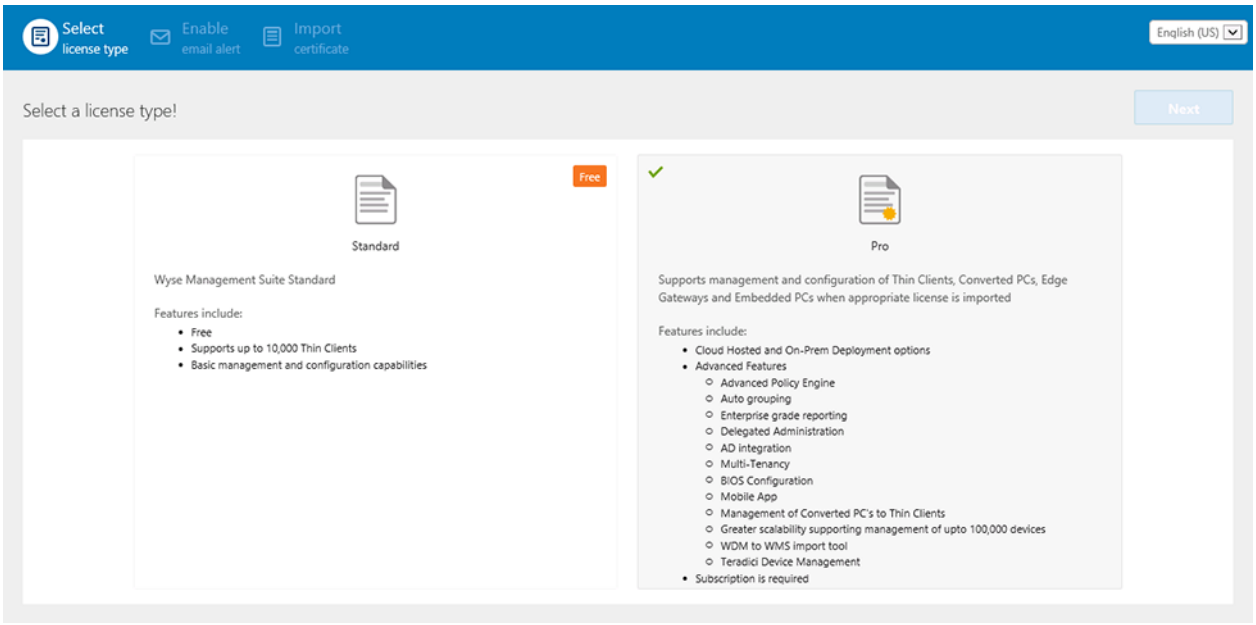

Ilustración 2. Tipo de licencia

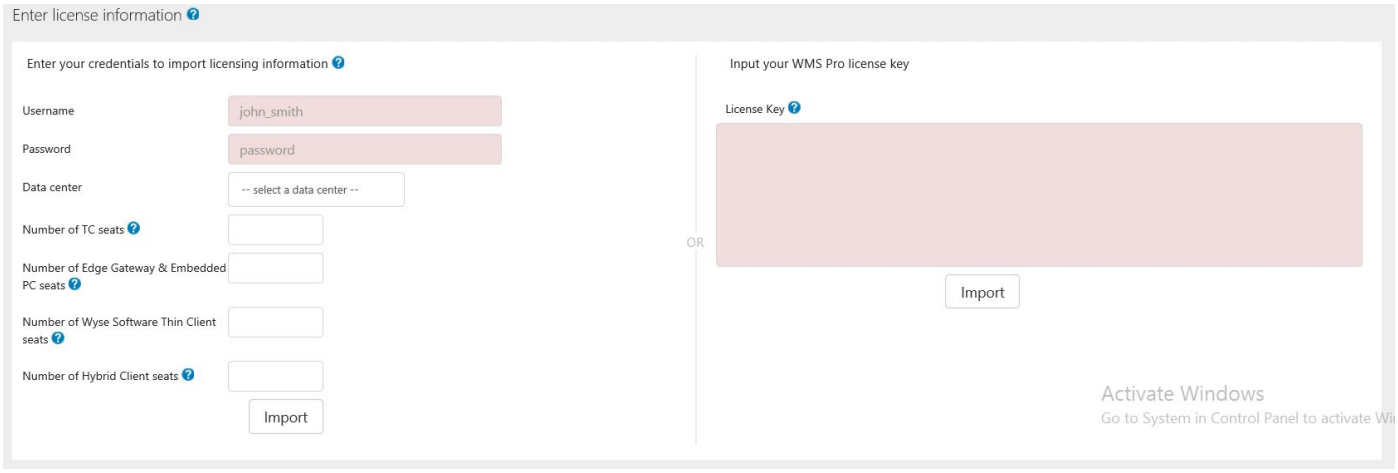

Ilustración 3. Información de la licencia

Para exportar una clave de licencia desde el portal de nube de Wyse Management Suite, haga lo siguiente:

a. Inicie sesión en el portal de nube pública de Wyse Management Suite mediante uno de los siguientes enlaces:
   - Centro de datos de Estados Unidos: us1.wysemanagementsuite.com/ccm-web
   - Centro de datos de la Unión Europea: eu1.wysemanagementsuite.com/ccm-web
b. Vaya a **Administración del portal** > **Suscripción**.

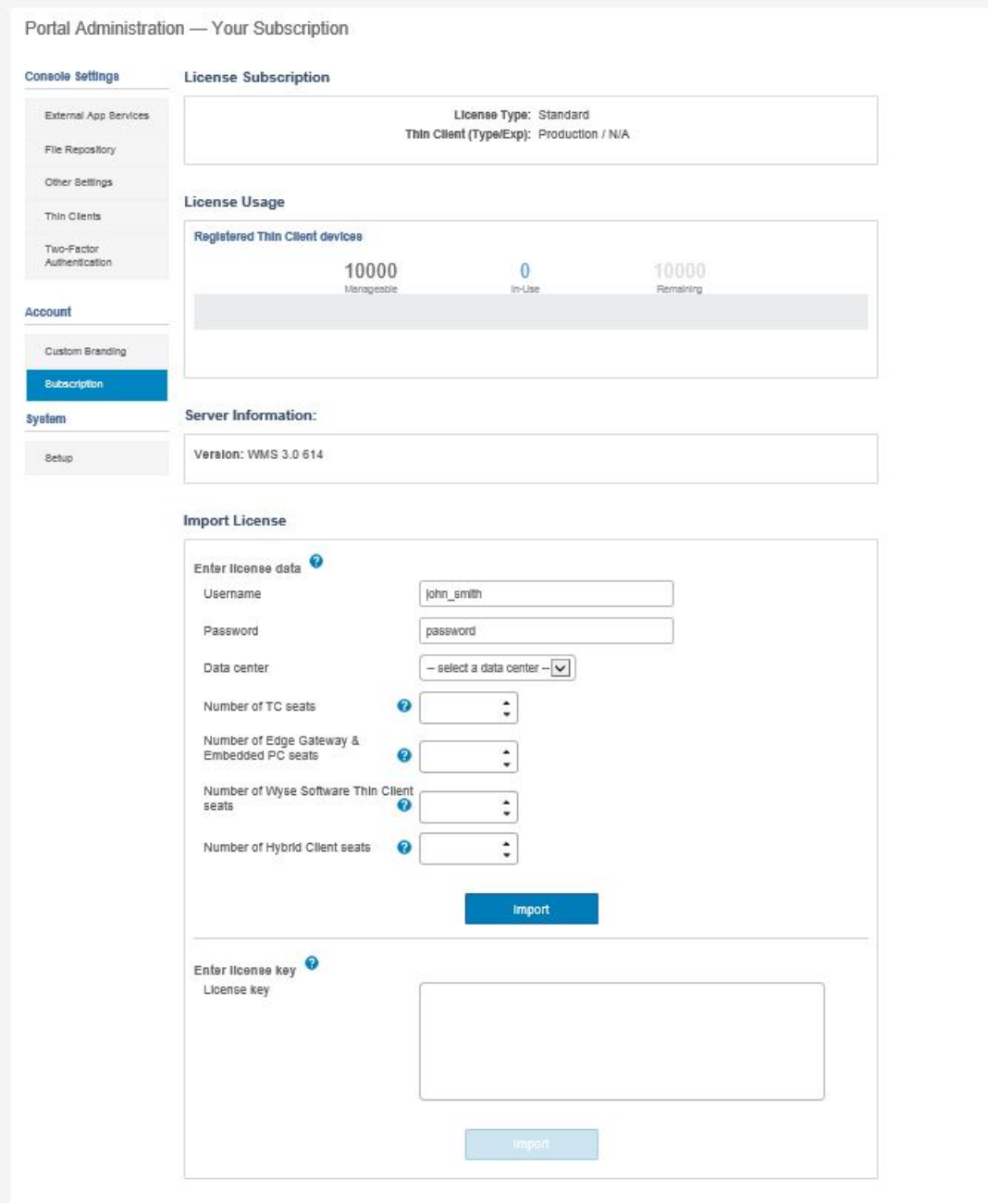

Ilustración 4. Administración del portal

c. Ingrese el n.º de puestos de Thin client.

d. Haga clic en **Exportar**.

Para exportar la licencia, seleccione **WMS 1.1** o **WMS 1.0** en la lista desplegable.

La página Resumen muestra los detalles de la licencia después de importar la licencia correctamente.

16. Ingrese la información del servidor SMTP y haga clic en **Guardar**.

NOTA: Puede omitir esta pantalla y realizar cambios en la consola más adelante.

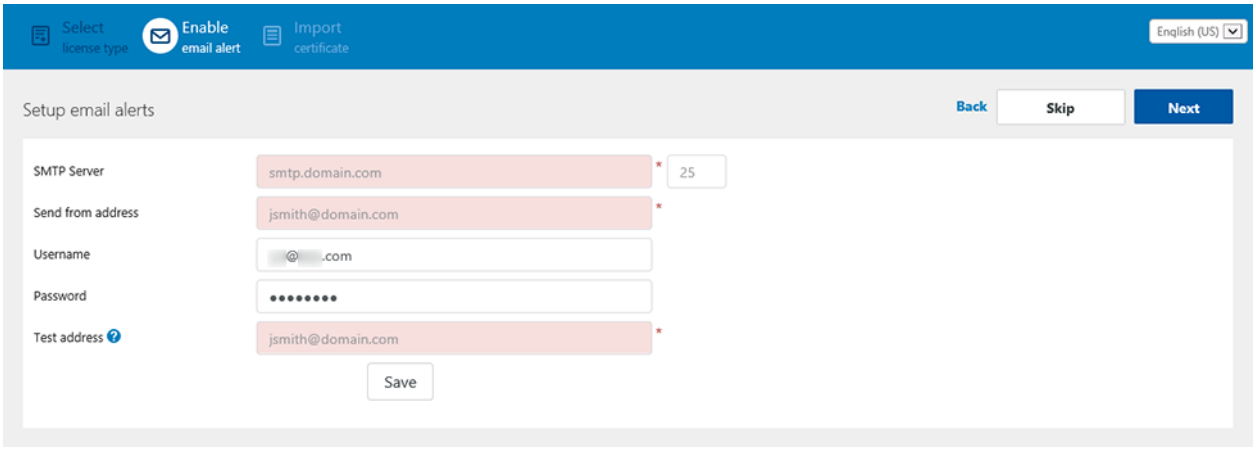

Ilustración 5. Alerta por correo electrónico

NOTA: Debe ingresar información válida del servidor SMTP para recibir notificaciones de correo electrónico de Wyse Management Suite.

17. Importe su certificado SSL para mantener comunicaciones seguras con el servidor Wyse Management Suite. Ingrese los certificados público, privado y Apache, y haga clic en el botón **Importar**. La importación del certificado tarda tres minutos en configurar y reiniciar los servicios Tomcat. Puede omitir esta pantalla y finalizar esta configuración o hacer cambios en la consola más adelante iniciando sesión en la nube privada de Wyse Management Suite e importando desde la página **Administración del portal**.

NOTA:

De manera predeterminada, Wyse Management Suite importa el certificado SSL autofirmado que se genera durante la instalación para establecer una comunicación segura entre el cliente y el servidor Wyse Management Suite. Si no importa un certificado válido para su servidor Wyse Management Suite, aparecerá un mensaje de advertencia de seguridad cuando acceda a Wyse Management Suite desde un equipo distinto al servidor donde está instalado. Este mensaje de advertencia se muestra porque el certificado firmado automáticamente que se generó durante la instalación no está firmado por una autoridad de certificación como geotrust.com. Puede importar un certificado .pem o .pfx.

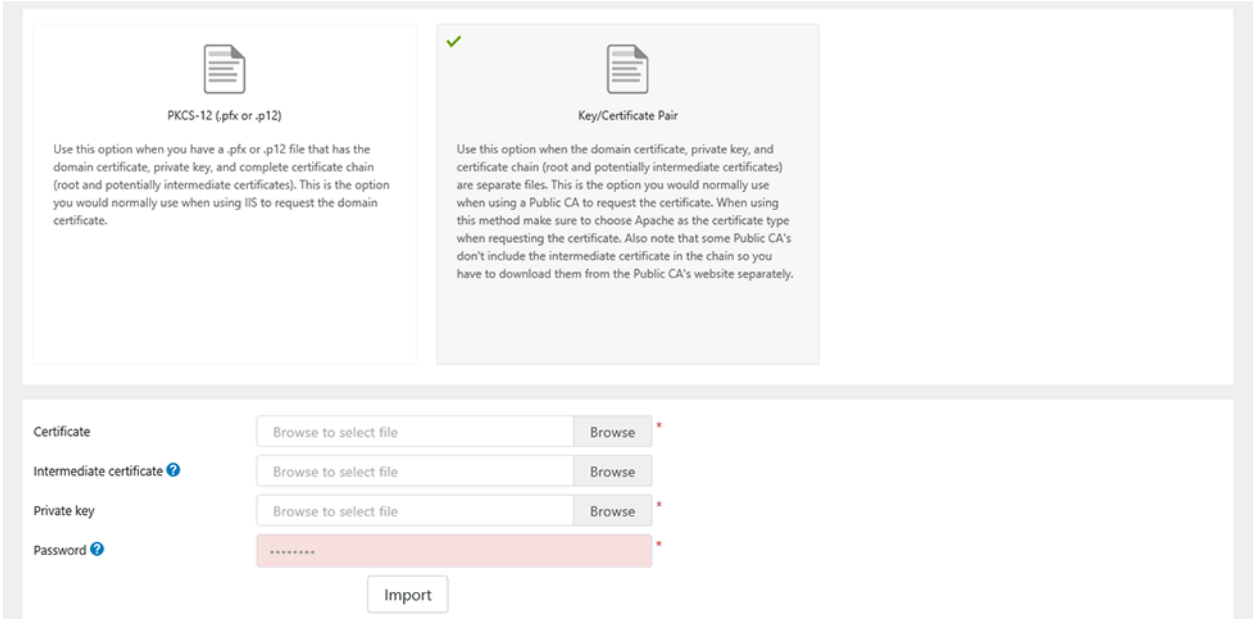

Ilustración 6. Par de valores de clave o certificado

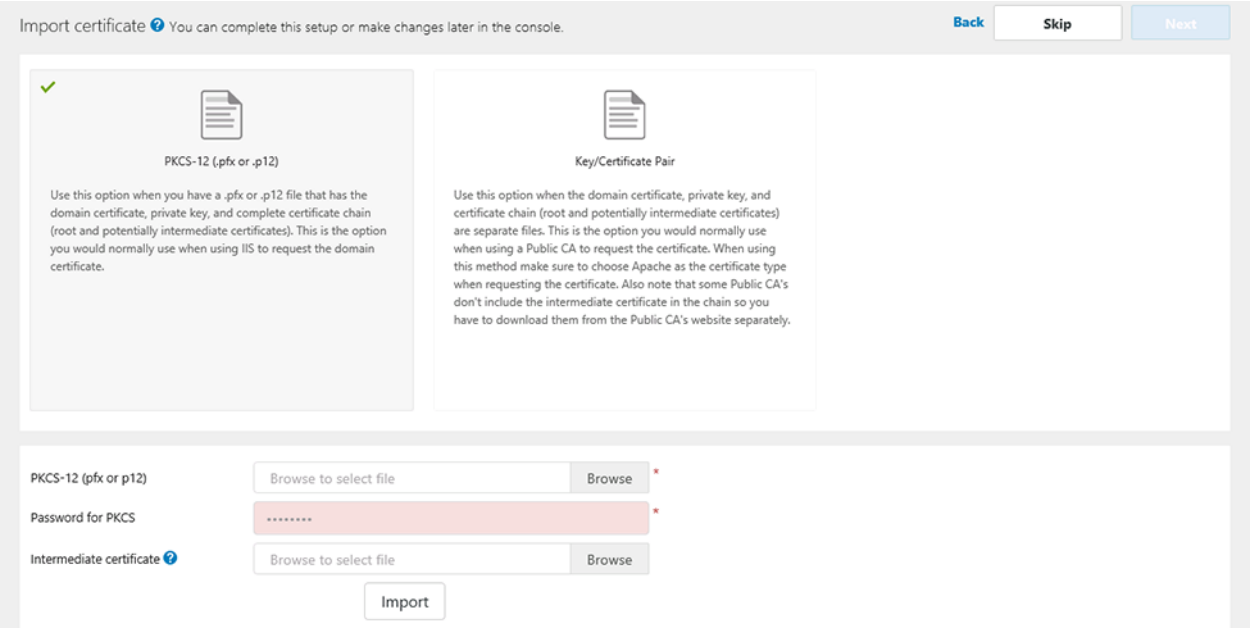

Ilustración 7. PKCS-12

18. En la página **Dispositivo**, puede habilitar la opción **Validación de la inscripción** para permitir que los administradores controlen el registro manual y automático de los clientes esbeltos en un grupo.

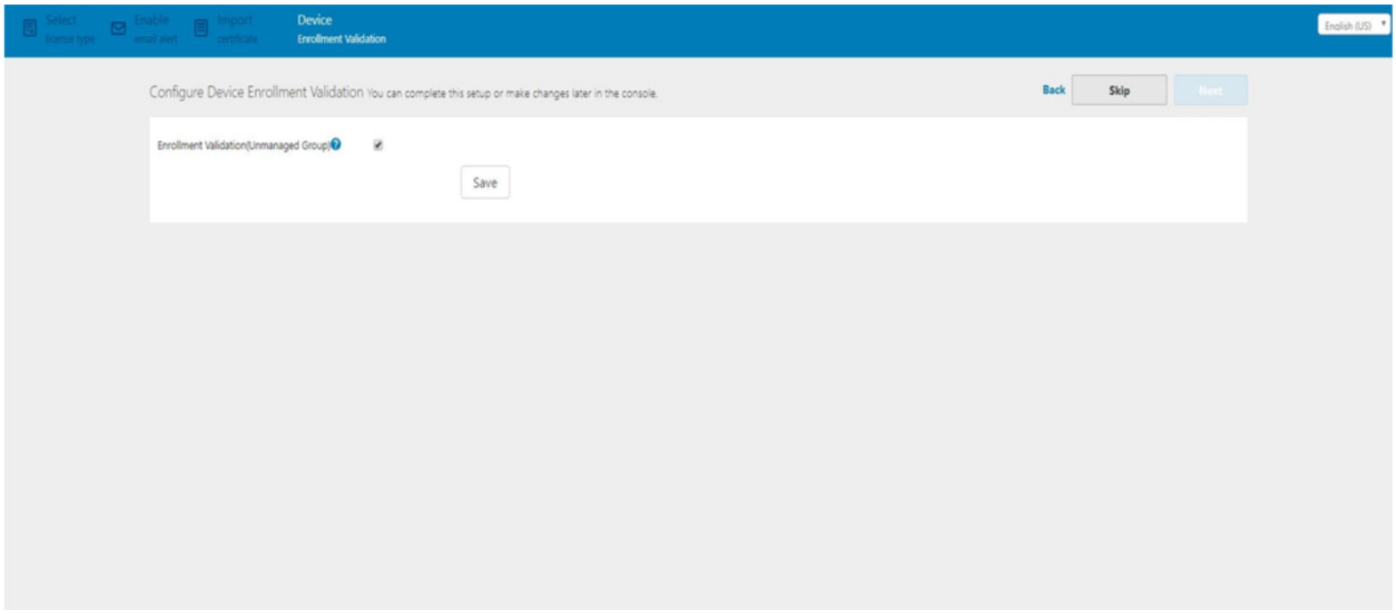

Ilustración 8. Validación de la inscripción

19. Haga clic en **Guardar** y, a continuación, haga clic en **Siguiente**.
20. Haga clic en **Iniciar sesión en WMS**.
    Aparece la página de inicio de sesión al **Dell Management Portal**.

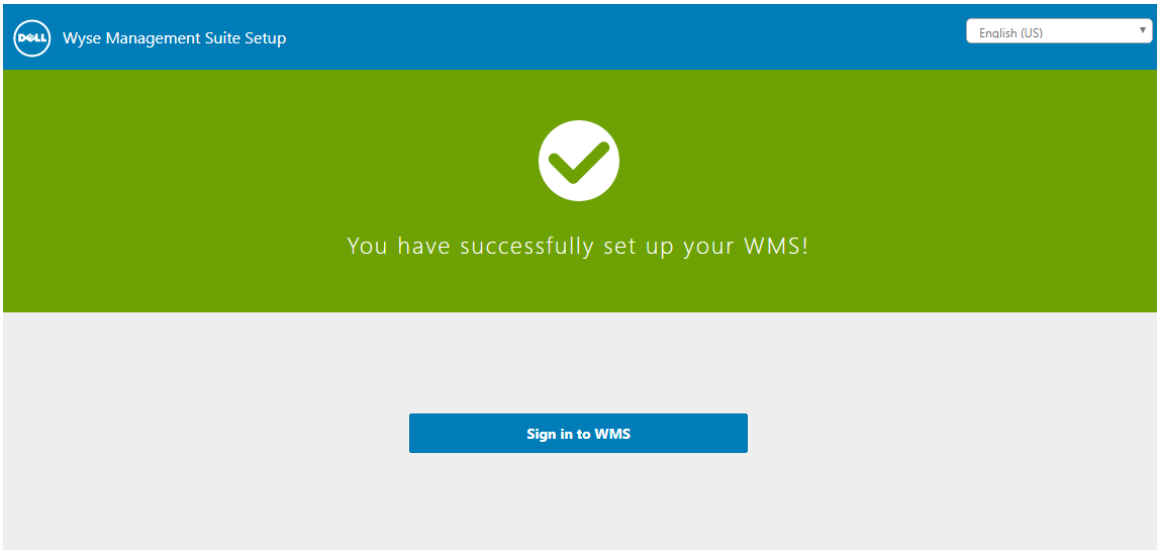

Ilustración 9. Página de inicio de sesión

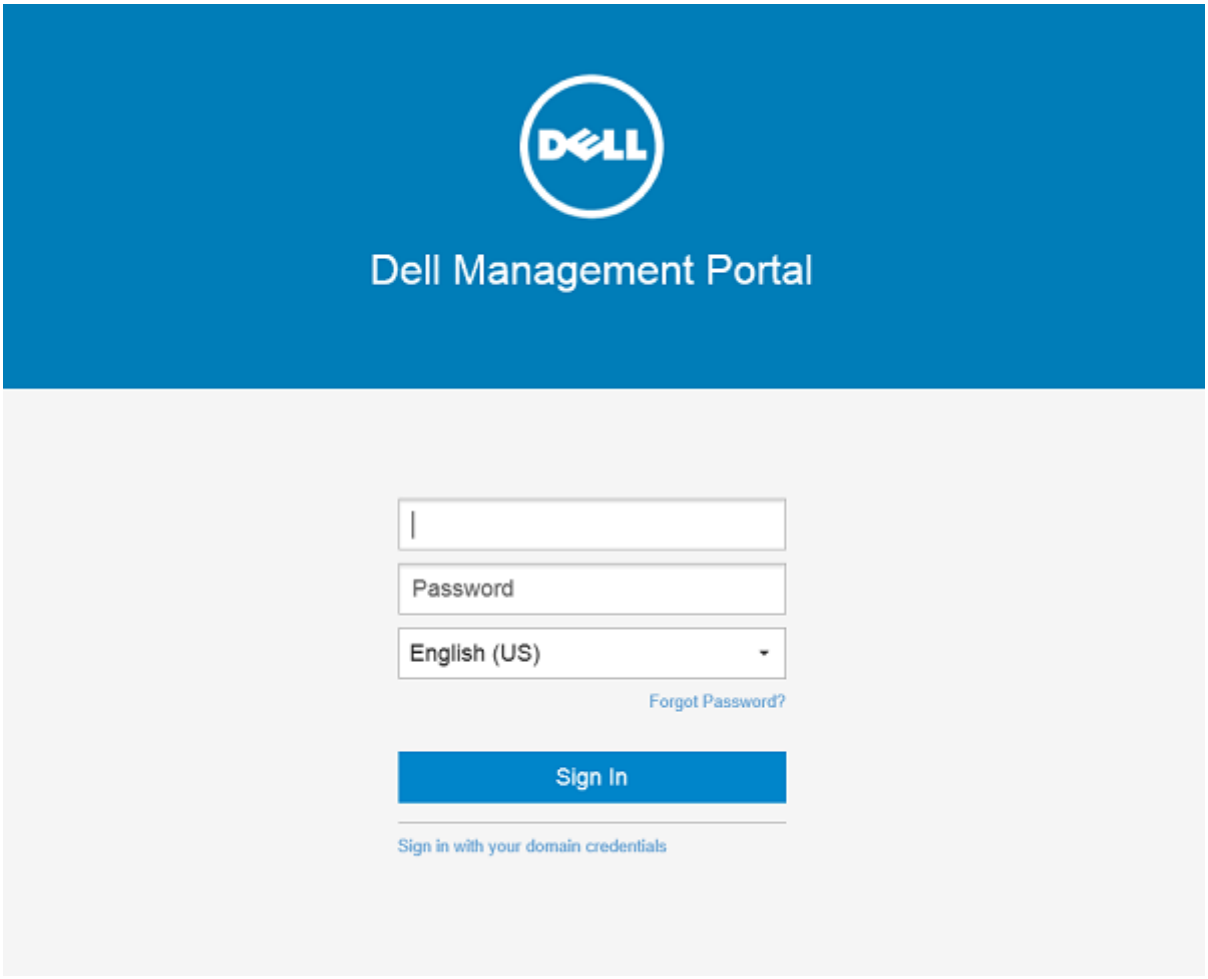

Ilustración 10. Dell Management Portal

NOTA: Las licencias se pueden actualizar o extender más adelante desde la página **Administración del portal**.

Temas:

Iniciar sesión en Wyse Management Suite

Sobre esta tarea

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

Pasos

1. Si utiliza Internet Explorer, desactive la **seguridad mejorada de Internet Explorer** y la configuración **Vista de compatibilidad**
2. Utilice un explorador web compatible en cualquier equipo con acceso a Internet y acceda a la edición de nube privada de Wyse Management Suite desde https://<FQDN>/ccm-web. Por ejemplo, https://wmsserver.domain.com/ccm-web, donde wmsserver.domain.com es el nombre de dominio completo del servidor.
3. Introduzca su nombre de usuario y contraseña.
4. Haga clic en **Iniciar sesión**

Áreas funcionales de la consola de administración

La consola de Wyse Management Suite está organizada en las siguientes áreas funcionales:

Sobre esta tarea

- La página **Panel** proporciona información sobre cada área funcional del sistema.
- La página **Grupos y configuraciones** emplea una administración jerárquica de política de grupo para la configuración de dispositivos. De manera opcional, se pueden crear subgrupos de la política de grupos global para clasificar los dispositivos según estándares corporativos. Por ejemplo, se pueden agrupar dispositivos según funciones de trabajo, tipo de dispositivo, dispositivo personal, entre otras clasificaciones.
- La página **Dispositivos** le permite ver y administrar dispositivos, tipos de dispositivos y configuraciones específicas de dispositivos.
- La página **Aplicaciones y datos** proporciona administración de aplicaciones de dispositivo, imágenes del sistema operativo, políticas, archivos de certificado, logotipos e imágenes de fondo de pantalla.
- La página **Reglas** le permite agregar, editar y activar o desactivar reglas como agrupamiento automático y notificaciones de alerta.
- La página **Trabajos** le permite crear trabajos para tareas como reinicio, WOL y políticas de aplicación o imagen que deban implementarse en dispositivos registrados.
- La página **Eventos** le permite ver y auditar eventos y alertas del sistema.
- La página **Usuarios** permite asignar a los usuarios locales y los usuarios importados desde Active Directory roles de administrador global, administrador de grupo y visor para iniciar sesión en Wyse Management Suite. A los usuarios se les asigna permisos para realizar operaciones según sus roles asignados.
- La página **Administración del portal** permite que los administradores puedan configurar varios parámetros del sistema, como la configuración del repositorio local, la suscripción a la licencia, la configuración de Active Directory y la autentificación de dos factores. Para obtener más información, consulte la *Guía del administrador de Dell Wyse Management Suite* en support.dell.com.

Configuración y administración de clientes ligeros

Administración de configuración: Wyse Management Suite admite una jerarquía de grupos y subgrupos. Los grupos se pueden crear manualmente o automáticamente según las reglas definidas por el administrador del sistema. Puede organizar según grupos funcionales como, por ejemplo, marketing, ventas e ingeniería, o según su jerarquía de ubicación como, por ejemplo, país, estado y ciudad.

NOTA:

En la edición Pro, los administradores del sistema pueden agregar reglas para crear grupos. También puede asignar dispositivos a un grupo existente según los atributos del dispositivo como, por ejemplo, subred, zona horaria y ubicación.

También puede configurar lo siguiente:

- Configuraciones y políticas que se aplican a todos los dispositivos en la cuenta de inquilino que se establece en el grupo de política predeterminada. Estas configuraciones y políticas son el conjunto global de parámetros que todos los grupos y subgrupos heredan.
- Las configuraciones o los parámetros que se configuran en grupos de nivel inferior tienen preferencia por sobre los valores configurados en grupos principales o de nivel superior.
- Parámetros específicos de un dispositivo en particular que se pueden configurar desde la página **Detalles del dispositivo**. Estos parámetros, como en el caso de los grupos de nivel inferior, tienen preferencia por sobre los valores configurados en grupos de nivel superior.

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

Una vez que una configuración se publica y propaga a los dispositivos, los valores no pueden volverse a enviar a los dispositivos hasta que el administrador realice un cambio. Los nuevos dispositivos que se registren reciben la política de configuración que corresponda con el grupo al que están registrados. Esto incluye los parámetros heredados desde el grupo global y los grupos de nivel intermedio.

Las políticas de configuración se publican inmediatamente y no se pueden programar para más tarde. Algunos cambios de política como, por ejemplo, la configuración de pantalla pueden forzar un reinicio.

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

NOTA: La política de aplicaciones avanzada permite implementar una aplicación en todos los subgrupos y en el subgrupo actual, según sus requisitos. Las imágenes de sistema operativo se pueden implementar solo al grupo actual.

Wyse Management Suite admite políticas de aplicación estándar y avanzadas. Una política de aplicaciones estándar le permite instalar un único paquete de aplicación. Es necesario reiniciar el dispositivo antes y después de cada instalación de aplicación. Con una política de aplicaciones avanzada, se pueden instalar múltiples paquetes de aplicaciones con solo dos reinicios. Esta función solo está disponible en la edición Pro. Las políticas avanzadas de aplicaciones también admiten la ejecución de secuencias de comandos antes y después de la instalación, según se requiera para instalar una aplicación en particular.

Puede configurar la aplicación automática de políticas de aplicaciones estándar y avanzadas cuando se registre un dispositivo con Wyse Management Suite o cuando un dispositivo se mueve a un grupo nuevo.

La implementación de políticas de aplicaciones e imágenes de sistema operativo a clientes ligeros 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 encontrar haciendo clic en la pestaña **Dispositivos**. De manera predeterminada, esta opción muestra una lista compaginada de todos los dispositivos en el sistema. El administrador puede elegir ver un subconjunto de dispositivos mediante varios criterios de filtrado, como grupos o subgrupos, tipo de dispositivo, tipo de sistema operativo, estado, subred, plataforma o zona horaria.

Para ir a la página **Detalles del dispositivo** para ese dispositivo, haga clic en la entrada de dispositivo que se indica en esta página. Aparecerán todos los detalles del dispositivo.

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

Esta página también permite que los administradores establezcan parámetros de configuración específicos para ese dispositivo mediante la activación del botón **Excepciones del dispositivo**. Los parámetros configurados en esta sección sobrescriben cualquier parámetro configurado a nivel global o de grupo.

Informes: los administradores pueden generar y ver informes predefinidos según los filtros predefinidos. Para generar informes predefinidos, haga clic en la pestaña **Informes** en la página **Administración del portal**

Aplicación móvil: el administrador puede recibir notificaciones de alerta y administrar dispositivos usando la aplicación móvil disponible para dispositivos Android. Para descargar la aplicación móvil y la guía de inicio rápido, haga clic en la pestaña **Alertas y clasificación** en la página **Administración del portal**.

Crear grupo de políticas y actualizar configuración

Para crear una política y actualizar la configuración, haga lo siguiente:

1. Inicie sesión como administrador.

2. Para crear un grupo de políticas, haga lo siguiente:
   a. Seleccione **Grupos y configuraciones** y haga clic en el botón **+** en el panel izquierdo.
   b. Ingrese el nombre del grupo y la descripción.
   c. Marque la casilla de verificación **Activado**.
   d. Ingrese el token de grupo.
   e. Haga clic en **Guardar**.
3. Para actualizar o editar un grupo de políticas, haga lo siguiente:
   a. Haga clic en **Editar políticas** y seleccione el sistema operativo que debe administrar la política.
   b. Seleccione las políticas que se modificarán y complete la configuración.
   c. Haga clic en **Guardar y publicar**.

NOTA:
- Para obtener más detalles sobre las diversas políticas de configuración compatibles con Wyse Management Suite, consulte la *Guía del administrador de Dell Wyse Management Suite* en support.dell.com.
- Puede crear una regla para crear automáticamente un grupo o para asignar un dispositivo a un grupo según atributos específicos como subred, zona horaria y ubicación.

Registro de nuevos clientes ligeros

NOTA: Para obtener información sobre el entorno de seguridad del cliente, consulte Wyse Device Agent.

Se puede registrar un Thin Client con Wyse Management Suite manualmente mediante Wyse Device Agent (WDA). También puede registrar automáticamente un Thin Client configurando etiquetas de opción apropiadas en el servidor DHCP o configurando registros SRV de DNS apropiados en el servidor DNS.

Si desea que los dispositivos en subredes distintas se registren automáticamente en grupos diferentes de Wyse Management Suite con subredes múltiples, utilice las etiquetas de opción DHCP para registrar un cliente ligero. Por ejemplo, los dispositivos en la TimeZone_A pueden registrarse en el ProfileGroup configurado para la TimeZoneA.

Si desea ingresar la información del servidor Wyse Management Suite en TLD y si ha instalado Wyse Management Suite Pro para permitir la asignación automática de grupos según reglas de dispositivos, utilice los registros SRV de DNS en el servidor DNS para registrar un cliente ligero. Por ejemplo, si el dispositivo se registra desde la TimeZoneA, asígnelo a un ProfileGroup configurado para la TimeZoneA.

Para Wyse Management Suite en una nube privada con certificados autofirmados, los clientes ligeros deben tener instaladas las siguientes versiones de Wyse Device Agents o firmware para una comunicación segura:

- 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 un dispositivo con una versión de agente más antigua usando la URL HTTP en lugar de HTTPS. Una vez que el agente o el firmware se actualicen a la versión más reciente, la comunicación con Wyse Management Suite cambiará automáticamente a https.
- Puede descargar la versión más reciente de WDA en downloads.dell.com/wyse/wda.
- En el caso de que Wyse Management Suite esté instalado en una nube privada, vaya a **Administración del portal** > **Configuración** y seleccione la casilla de verificación **Validación de certificado** si ha importado certificados de una autoridad de certificación como www.geotrust.com. No se debe seleccionar esta casilla de verificación si no ha importado certificados de una autoridad de certificación reconocida. Esta opción no está disponible para Wyse Management Suite en una nube pública, ya que la validación de certificados en nube pública siempre está activada.

Registrar dispositivo ThinOS manualmente

Para registrar dispositivos ThinOS manualmente, haga lo siguiente:

Pasos

1. Desde el menú de escritorio, vaya a **Configuración del sistema Configuración central**.
   Aparecerá la ventana **Configuración central**.
2. Haga clic en la pestaña **WDA**.

   WMS aparece seleccionado de manera predeterminada.

   NOTA: El servicio WDA se ejecuta automáticamente después de que el proceso de arranque del cliente se haya completado.

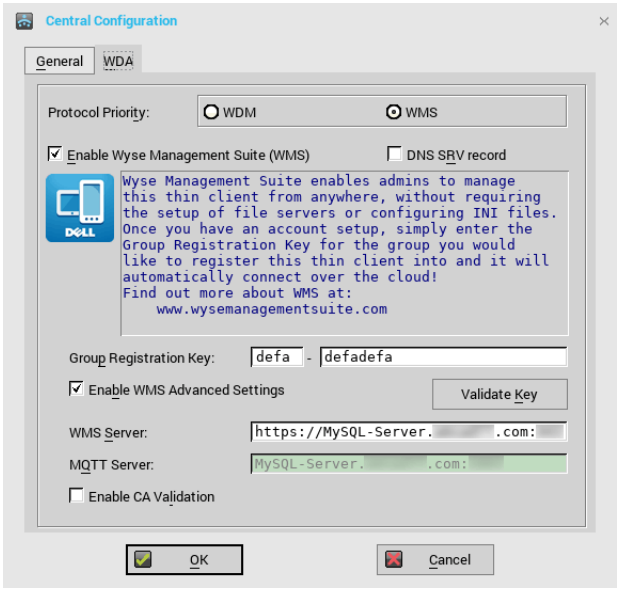

Ilustración 11. Configuración central

3. Seleccione la casilla de verificación **Activar Wyse Management Suite** para activar Wyse Management Suite.
4. Ingrese la **Clave de registro de grupo** según lo configurado por su 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: nube pública o nube privada.
   - Nube pública: seleccione la casilla de verificación **Activar validación de CA** si el dispositivo se ha registrado con Wyse Management Suite en una nube pública.
   - 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.

   NOTA:

   En el caso de la versión de nube Pro de Wyse Management Suite en EE. UU., no cambie los detalles predeterminados de servidor WMS y servidor MQTT. En el caso de la versión de nube Pro de Wyse Management Suite en Europa, utilice lo siguiente:

   - Servidor CCM: eu1.wysemanagementsuite.com
   - Servidor MQTT: *eu1-pns.wysemanagementsuite.com:1883*

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

   NOTA: Si la clave no se valida, verifique las credenciales que ha proporcionado. Asegúrese de que los puertos 443 y 1883 no estén bloqueados por la red.

8. Haga clic en **Aceptar**.
   El dispositivo se registra en la consola de Wyse Management Suite.

Siguientes pasos

Para obtener información sobre cómo registrar los dispositivos Windows Embedded Standard y los dispositivos Linux, consulte Registrar dispositivo Windows Embedded manualmente y Registrar dispositivo Linux manualmente.

Registrar dispositivos ThinOS mediante archivos INI

Si desea configurar los dispositivos ThinOS mediante wnos.ini o xen.ini, entonces se puede publicar la información adicional en los archivos .ini para informar a los dispositivos que se registren a un servidor Wyse Management Suite.

Ejemplos:

- Ejemplo para ThinOS 8.5:

  WDAService=yes \

  Priority=WMS

  WMSEnable=yes \

  Server= <URL del servidor> \

  CAValidation=no \

  Override=yes

- Ejemplo para ThinOS 8.4:

  WDAService=yes \

  Priority=CCM

  CCMEnable=yes \

  CCMServer= <URL del servidor> \

  GroupPrefix=< Prefijo > \

  GroupKey=< Clave > \

  MQTTServer= <URL del servidor> \

  Override=yes \

  CAValidation=no

Para obtener más información, consulte la última *Guía INI ThinOS de Dell Wyse* en el sitio support.dell.com.

NOTA:

- Para ThinOS 8.3 (ThinOS Lite 2.3) y versiones posteriores, un comando `WDA Service Priority` le permite especificar el protocolo de administración. Este comando se utiliza para descubrir el servidor de administración.
- Las etiquetas CCM para ThinOS versión 8.3, 8.4 y 8.5 son diferentes.

Registrar dispositivos mediante etiquetas de opciones de DHCP

NOTA:

- Para obtener instrucciones detalladas sobre cómo agregar etiquetas de opción DHCP en el servidor Windows, consulte Crear y configurar etiquetas de opción DHCP. Para obtener información sobre el entorno de seguridad del cliente, consulte Wyse Device Agent.

Puede registrar los dispositivos utilizando las siguientes etiquetas de opciones de DHCP:

Tabla 5. Registrar un dispositivo mediante etiquetas de opciones de DHCP

Etiqueta de opciones	Descripción
Nombre: WMS **Tipo de dato**: cadena **Código**: 165 **Descripción**: FQDN de servidor de WMS	Esta etiqueta señala la URL del servidor de Wyse Management Suite. Por ejemplo, `wmsserver.acme.com:443`, donde wmsserver.acme.com es el nombre de dominio completo del servidor en el cual Wyse Management Suite se encuentra instalado. Para obtener enlaces para registrar sus dispositivos en Wyse Management Suite en una nube pública, consulte Introducción a Wyse Management Suite en nube pública. **NOTA:** No utilice https:// en la URL del servidor, o el cliente delgado no se registrará en Wyse Management Suite. Utilice https:// si no puede registrar el dispositivo Thinos 9.x en Wyse Management Suite.

Tabla 5. Registrar un dispositivo mediante etiquetas de opciones de DHCP (continuación)

Etiqueta de opciones	Descripción
Nombre: MQTT **Tipo de dato**: cadena **Código**: 166 **Descripción**: servidor de MQTT	Esta etiqueta dirige el dispositivo al servidor de notificación de inserción 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: `wmsservername.domain.com:1883`. 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: EE. UU.1:us1-pns.wysemanagementsuite.com UE1:eu1-pns.wysemanagementsuite.com Debe ingresar los detalles del servidor MQTT cuando configura detalles de Wyse Device Agent en la versión anterior de ThinOS y en dispositivos Windows Embedded. MQTT es un componente de WMS que se requiere para enviar notificaciones a los clientes delgados. Las direcciones URL, con y sin detalles de MQTT, se deben agregar a la lista allowlist en el entorno de nube pública de Wyse Management Suite. **NOTA:** No puede usar las direcciones URL de MQTT para iniciar sesión en Wyse Management Suite.
Nombre: Validación de CA **Tipo de dato**: cadena **Código**: 167 **Descripción**: Validación de la entidad emisora de certificados	Esta etiqueta se requiere si Wyse Management Suite se encuentra instalada en el sistema en su nube privada. No agregue esta etiqueta de opciones si desea registrar sus dispositivos con Wyse Management Suite en la nube pública. Ingrese **Verdadero** si importó los certificados de SSL desde una entidad emisora conocida para la comunicación https entre el cliente y servidor de Wyse Management Suite. Ingrese **Falso** 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.
Nombre: token de grupo **Tipo de dato**: cadena **Código**: 199 **Descripción**: token de grupo	Esta etiqueta es necesaria para registrar los dispositivos ThinOS con Wyse Management Suite en una nube privada o pública. 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 durante la instalación local.

Registrar dispositivos mediante registro SRV DNS

NOTA: Para obtener información sobre el entorno de seguridad del cliente, consulte Wyse Device Agent.

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 valores válidos.

NOTA: Para obtener instrucciones detalladas sobre cómo agregar registros SRV de DNS en el servidor Windows, consulte Crear y configurar registro SRV de DNS.

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

Tabla 6. Configurar el dispositivo mediante un registro SRV de DNS

URL/etiqueta	Descripción
Nombre de registro: _WMS_MGMT **FQDN de registro:** _WMS_MGMT._tcp. <Domainname> **Tipo de registro:** SRV	Este registro señala la URL del servidor de Wyse Management Suite. Por ejemplo, `wmsserver.acme.com:443`, donde wmsserver.acme.com es el nombre de dominio completo del servidor en el cual Wyse Management Suite se encuentra instalado. Para obtener enlaces para registrar sus dispositivos en Wyse Management Suite en una nube pública, consulte Introducción a Wyse Management Suite en nube pública. **NOTA:** No utilice https:// en la URL del servidor, o el cliente delgado no se registrará en Wyse Management Suite. Utilice https:// si no puede registrar el dispositivo Thinos 9.x en Wyse Management Suite.
Nombre de registro: _WMS_MQTT **FQDN de registro**: _WMS_MQTT._tcp. <Domainname> **Tipo de registro:** SRV	Este registro dirige el dispositivo al servidor de notificación de inserción 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: `wmsservername.domain.com:1883`. **NOTA:** MQTT es opcional para la versión más reciente de Wyse Management Suite. 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: EE. UU.1: us1-pns.wysemanagementsuite.com UE1: eu1-pns.wysemanagementsuite.com Debe ingresar los detalles del servidor MQTT cuando configura detalles de Wyse Device Agent en la versión anterior de ThinOS y en dispositivos Windows Embedded. MQTT es un componente de WMS que se requiere para enviar notificaciones a los clientes delgados. Las direcciones URL, con y sin detalles de MQTT, se deben agregar a la lista allowlist en el entorno de nube pública de Wyse Management Suite. **NOTA:** No puede usar las direcciones URL de MQTT para iniciar sesión en Wyse Management Suite.
Nombre de registro: _WMS_GROUPTOKEN **FQDN de registro**: _WMS_GROUPTOKEN.<Domain> **Tipo de registro:** TEXTO	Este registro es necesario para registrar los dispositivos ThinOS con Wyse Management Suite en una nube privada o pública. 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 local. **NOTA:** El token de grupo es opcional para la versión más reciente de Wyse Management Suite en nube privada.
Nombre de registro: _WMS_CAVALIDATION **FQDN de registro**: _WMS_CAVALIDATION.<Domain> **Tipo de registro:** TEXTO	Este registro es necesario si Wyse Management Suite se encuentra instalada en el sistema en su nube privada. No agregue este registro opcional si registra sus dispositivos con Wyse Management Suite en la nube pública. Ingrese **Verdadero** si importó los certificados de SSL desde una entidad emisora conocida para la comunicación https entre el cliente y servidor de Wyse Management Suite.

Tabla 6. Configurar el dispositivo mediante un registro SRV de DNS (continuación)

URL/etiqueta	Descripción
	Ingrese **Falso** 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. **NOTA:** Validación de CA es opcional para la versión más reciente de Wyse Management Suite.

Registrar dispositivos mediante campos de registro de DNS seguro u opciones de alcance de DHCP seguro

Desde Wyse Management Suite 3.5, puede registrar dispositivos mediante los campos de registro de DNS seguro o las opciones de alcance de DHCP.

Sobre esta tarea

Puede registrar los dispositivos en el servidor de Wyse Management Suite si los campos de registro de DNS o las opciones de alcance de DHCP se establecen con los siguientes valores:

- Campos de registro SRV de DNS:
  - _WMS_MGMTV2
  - _WMS_GROUPTOKENV2
- Opciones de alcance de DHCP:
  - URL de WMS: 201
  - Token de grupo: 202

Pasos

1. Vaya a **Administración del portal** > **Ajustes de la consola** > **Detección de WMS**.
2. Ingrese el token de grupo.
3. Seleccione el tipo de detección en la lista desplegable **Tipo de detección**.
4. Haga clic en **Generar detalles**.
   Se muestran los detalles cifrados de la URL de WMS y el token de grupo.
   NOTA: Si se cambia el certificado de Wyse Management Suite, se debe volver a crear el código de DNS y DHCP seguro para registrar un nuevo dispositivo.

4

Implementar aplicaciones en clientes delgados

La política de la aplicación estándar le permite instalar un paquete de aplicación único y requiere reiniciar antes y después de instalar cada aplicación. Con la política de la aplicación avanzada, puede instalar varios paquetes de aplicación con solo dos reinicios. Las políticas de aplicación avanzadas también son compatibles con la ejecución de secuencias de comandos previa y posterior a la instalación que se pueden necesitar para instalar una aplicación particular. Para obtener más información, consulte el Anexo B.

Temas:

Carga e implementación de inventario de imágenes de firmware ThinOS

Para agregar un archivo al inventario de imágenes ThinOS, haga lo siguiente:

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 **Examinar** 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 asignar el archivo, vaya a la página de configuración de dispositivo correspondiente.

Creación e implementación de políticas de aplicaciones estándar en clientes ligeros

Para implementar una política de aplicaciones estándar en clientes ligeros, haga lo siguiente:

1. En el repositorio local, vaya a **thinClientApps** y copie la aplicación a la carpeta.
2. Asegúrese de que la aplicación está registrada; para ello, vaya a la pestaña **Aplicaciones y datos** y seleccione **Thin Client** en **Inventario de aplicaciones**.

   NOTA: La interfaz Inventario de aplicaciones demora aproximadamente dos minutos en llenar cualquier programa recientemente agregado.
3. En **Políticas de la aplicación**, haga clic en **Cliente ligero**.
4. Haga clic en **Agregar política**.
5. Para crear una política de aplicaciones, ingrese la información apropiada en la ventana **Agregar política de la aplicación estándar**.
   a. Seleccione **Nombre de la política**, **Grupo**, **Tarea**, **Tipo de dispositivo** y **Aplicación TC**.
   b. Para implementar esta política en un sistema operativo o una plataforma en específico, seleccione **Filtro del subtipo de SO** o **Filtro de la plataforma**.

El tiempo de espera muestra un mensaje en el cliente que le dará tiempo para guardar su trabajo antes de que comience la instalación. Especifique la cantidad de minutos que debe mostrarse en el cliente el cuadro de diálogo.

c. Para aplicar automáticamente esta política a un dispositivo que se ha registrado con Wyse Management Suite, seleccione **Aplicar la política a nuevos dispositivos** desde la lista desplegable **Aplicar política automáticamente**.

NOTA:

- Cuando algún dispositivo se mueve al grupo definido o se registra directamente a dicho grupo, se aplica la política de aplicación.
- Si selecciona **Aplicar la política a los dispositivos durante registro**, la política se aplica automáticamente en el dispositivo tras registrarse en el servidor de Wyse Management Suite.

6. Para permitir un retraso en la ejecución de la política, seleccione la casilla de verificación **Permitir retraso de la ejecución de la política**. Si se selecciona esta opción, se activarán los siguientes menús desplegables:
   - Desde el menú desplegable **Máx. de horas por retraso**, seleccione la cantidad máxima de horas (de 1 a 24 horas) que puede retrasar la ejecución de la política.
   - Desde el menú desplegable **Máx. de retrasos**, seleccione la cantidad de veces (de 1 a 3) que puede retrasar la ejecución de la política.
7. 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**.
8. Haga clic en **Guardar** para crear una política.

   Se muestra un mensaje para permitir que el administrador programe esta política en los dispositivos según el grupo.
9. Seleccione **Sí** para programar un trabajo en la misma página.

   El trabajo de política de aplicación/imagen se puede ejecutar:

   a. **Inmediatamente**: el servidor ejecuta el trabajo inmediatamente.

   b. **En zona horaria del dispositivo**: el servidor crea un trabajo para cada zona horaria de dispositivo y programa el trabajo en la fecha y hora seleccionadas de la zona horaria del dispositivo.

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

5

Actualizar Wyse Management Suite versión 2.x a 3.x

Requisitos previos

- Asegúrese de que haya suficiente espacio en la unidad en la cual está instalado Wyse Management Suite y que el repositorio local esté configurado.
- Si instaló o configuró algún antivirus u otra herramienta de supervisión en la configuración de Wyse Management Suite, Dell Technologies recomienda deshabilitar las herramientas temporalmente hasta que se complete la actualización. También puede agregar una exclusión correspondiente para el directorio de instalación, el directorio temporal y el directorio del repositorio local de Wyse Management Suite.

Pasos

1. Haga doble clic en el paquete de instalación de Wyse Management Suite 3.x.
2. En la pantalla de **Bienvenida**, haga clic en **Siguiente**.
   Aparecerán los detalles del EULA.
   NOTA: Esta pantalla se muestra cuando se actualiza de Wyse Management Suite 3.0 a 3.1.
3. Lea el acuerdo de licencia.
4. Seleccione **Acepto los términos del contrato de licencia** y haga clic en **Siguiente**.
5. En la página **Actualización**, configure los derechos de acceso y las carpetas compartidas para el usuario de CIFS. Las opciones posibles son:
   - Utilizar un usuario existente: seleccione esta opción para validar las credenciales del usuario existente.
   - Crear un nuevo usuario: seleccione esta opción e ingrese las credenciales para crear un nuevo usuario.

   NOTA: Si EM SDK está instalado en el servidor durante la instalación anterior de Wyse Management Suite, los componentes de Teradici EM SDK se actualizan automáticamente. Si EM SDK no está instalado en el dispositivo durante la instalación anterior, seleccione la casilla de verificación Teradici EM SDK para instalar y configurar los componentes de Teradici EM SDK.

   NOTA: También puede instalar y actualizar Teradici EM SDK con el instalador de Wyse Management Suite.
6. Seleccione la casilla de verificación **Vincular Memcached a 127.0.0.1** para vincular el memcache al servidor local: 127.0.0.1. Si esta casilla de verificación no está seleccionada, el memcache se **vincula** a FQDN.
7. Seleccione todas las versiones adecuadas de TLS según los criterios de soporte de los dispositivos que se están administrando.
   NOTA: La versión de WDA inferior a WDA_14.4.0.135_Unified, la herramienta Importar y la imagen Merlin de 32 bits no son compatibles con TLSv1.1 y versiones posteriores. Seleccione TLSv1.0 si el entorno Wyse Management Suite tiene dispositivos con una versión anterior de WDA, la herramienta Importar o dispositivos instalados con la imagen Merlin de 32 bits.
8. Haga clic en **Iniciar** para abrir la consola web de Wyse Management Suite.

6

Actualizar Wyse Management Suite de la versión 3.x a la 3.3

Requisitos previos

- Asegúrese de que haya suficiente espacio en la unidad en la cual está instalado Wyse Management Suite y que el repositorio local esté configurado.
- Si instaló o configuró un antivirus u otra herramienta de monitoreo en la configuración de Wyse Management Suite, Dell Technologies recomienda deshabilitar las herramientas temporalmente hasta que se complete la actualización. También puede agregar una exclusión apropiada para el directorio de instalación, el directorio temporal y el directorio del repositorio local de Wyse Management Suite.

Pasos

1. Haga doble clic en el paquete de instalación de Wyse Management Suite 3.2.
2. En la pantalla de **Bienvenida**, haga clic en **Siguiente**.
   Aparecerán los detalles del EULA.
   NOTA: Esta pantalla se muestra cuando se actualiza de Wyse Management Suite 3.0 a 3.x.
3. Lea el acuerdo de licencia.
4. Seleccione **Acepto los términos del contrato de licencia** y haga clic en **Siguiente**.
5. En la página **Actualización**, configure los derechos de acceso y las carpetas compartidas para el usuario de CIFS. Las opciones posibles son:
   - Utilizar un usuario existente: seleccione esta opción para validar las credenciales del usuario existente.
   - Crear un nuevo usuario: seleccione esta opción e ingrese las credenciales para crear un usuario.

   NOTA: Si EM SDK está instalado en el servidor durante la instalación anterior de Wyse Management Suite, los componentes de Teradici EM SDK se actualizan automáticamente. Si EM SDK no está instalado en el dispositivo durante la instalación anterior, seleccione la casilla de verificación Teradici EM SDK para instalar y configurar los componentes de Teradici EM SDK.

   NOTA: También puede instalar y actualizar Teradici EM SDK con el instalador de Wyse Management Suite.
6. Seleccione la casilla de verificación **Vincular Memcached a 127.0.0.1** para vincular el memcache al servidor local: 127.0.0.1. Si esta casilla de verificación no está seleccionada, el memcache se **vincula** a FQDN.
7. Seleccione un puerto para la comunicación MQTT segura. El puerto predeterminado es 8443.
   NOTA: El número de puerto para la comunicación MQTT segura no debe ser 0. La opción de selección de puertos se muestra cuando se actualiza Wyse Management Suite de las versiones 3.1 y 3.1.1 a la versión 3.3.

   Se muestra la ventana **Actualizar configuración de MQTT** cuando no hay coincidencia de nombre de host entre las direcciones URL de MQTT en la base de datos.
8. Seleccione la casilla de verificación **Aplicar cambios recomendados** si desea cambiar las direcciones URL.
   NOTA: Se muestra la ventana **Actualizar configuración de MQTT** cuando se actualiza Wyse Management Suite de las versiones 3.2 y 3.2.1 a la versión 3.3.
9. Haga clic en **Siguiente**.
10. Haga clic en **Iniciar** para abrir la consola web de Wyse Management Suite.

7

Actualizar Wyse Management Suite de la versión 3.x a la 3.5

Requisitos previos

- Asegúrese de que haya suficiente espacio en la unidad en la cual está instalado Wyse Management Suite y que el repositorio local esté configurado.
- Si instaló o configuró un antivirus u otra herramienta de monitoreo en la configuración de Wyse Management Suite, Dell Technologies recomienda deshabilitar las herramientas temporalmente hasta que se complete la actualización. También puede agregar una exclusión apropiada para el directorio de instalación, el directorio temporal y el directorio del repositorio local de Wyse Management Suite.

Pasos

1. Haga doble clic en el paquete de instalación de Wyse Management Suite 3.5.
2. En la pantalla de **Bienvenida**, haga clic en **Siguiente**.
   Aparecerán los detalles del EULA.
   NOTA: Esta pantalla se muestra cuando se actualiza de Wyse Management Suite 3.0 a 3.x.
3. Lea el acuerdo de licencia.
4. Seleccione **Acepto los términos del contrato de licencia** y haga clic en **Siguiente**.
5. En la página **Actualización**, haga lo siguiente:
   a. Configure los derechos de acceso y las carpetas compartidas para el usuario de CIFS. Las opciones posibles son:
      - **Utilizar un usuario existente**: seleccione esta opción para validar las credenciales del usuario existente.
      - **Crear un nuevo usuario**: seleccione esta opción e ingrese las credenciales para crear un nuevo usuario.

      La contraseña debe tener más de 8 caracteres.
   b. Haga clic en **Siguiente**.
   c. Se muestra la pantalla **Credenciales de cuentas de usuario**. Se crea un usuario local con menos privilegios con las credenciales que se ingresan en esta pantalla. Los servicios de Dell Wyse Management Suite se ejecutan en esta cuenta de usuario.
   d. Ingrese las credenciales de la cuenta de servicio.
      La contraseña debe tener entre 9 y 127 caracteres.
   e. Haga clic en **Siguiente**.
      Aparece la pantalla **Credenciales del vault de software**. El vault de software se utiliza para almacenar datos confidenciales requeridos por la aplicación Dell Wyse Management Suite.
   f. Ingrese la contraseña del vault de software.
      La contraseña debe tener más de 8 caracteres.
   g. Haga clic en **Siguiente**.

   NOTA: Si EM SDK está instalado en el servidor durante la instalación anterior de Wyse Management Suite, los componentes de Teradici EM SDK se actualizan automáticamente. Si EM SDK no está instalado en el dispositivo durante la instalación anterior, seleccione la casilla de verificación **Teradici EM SDK** para instalar y configurar los componentes de Teradici EM SDK.

   NOTA: También puede instalar y actualizar Teradici EM SDK con el instalador de Wyse Management Suite.

6. Seleccione un puerto para la comunicación MQTT segura. El puerto predeterminado es 8443.
   NOTA: El número de puerto para la comunicación MQTT segura no debe ser 0. La opción de selección de puertos se muestra cuando se actualiza Wyse Management Suite de las versiones 3.1 y 3.1.1 a la versión 3.5.
7. Seleccione la casilla de verificación **Aplicar cambios recomendados** si desea cambiar las direcciones URL.
   NOTA: Se muestra la ventana **Actualizar configuración de MQTT** cuando se actualiza Wyse Management Suite de las versiones 3.2 y 3.2.1 a la versión 3.5.
8. Haga clic en **Siguiente**.
9. Haga clic en **Iniciar** para abrir la consola web de Wyse Management Suite.

8

Actualizar Wyse Management Suite de la versión 3.x a 3.6

Requisitos previos

- Asegúrese de que haya suficiente espacio en la unidad en la cual está instalado Wyse Management Suite y que el repositorio local esté configurado.
- Si instaló o configuró un antivirus u otra herramienta de monitoreo en la configuración de Wyse Management Suite, Dell Technologies recomienda desactivar las herramientas temporalmente hasta que se complete la actualización. También puede agregar una exclusión apropiada para el directorio de instalación, el directorio temporal y el directorio del repositorio local de Wyse Management Suite.

Pasos

1. Haga doble clic en el paquete de instalación de Wyse Management Suite 3.6.
2. En la pantalla de **Bienvenida**, haga clic en **Siguiente**.
   Aparecerán los detalles del EULA.
   NOTA: Esta pantalla se muestra cuando se actualiza de Wyse Management Suite 3.0 a 3.x.
3. Lea el acuerdo de licencia.
4. Seleccione **Acepto los términos del contrato de licencia** y haga clic en **Siguiente**.
5. En la página **Actualización**, haga lo siguiente:
   a. Configure los derechos de acceso y las carpetas compartidas para el usuario de CIFS. Las opciones posibles son:
      - **Utilizar un usuario existente**: seleccione esta opción para validar las credenciales del usuario existente.
      - **Crear un nuevo usuario**: seleccione esta opción e ingrese las credenciales para crear un usuario.

      La contraseña debe tener más de ocho caracteres.
   b. Haga clic en **Siguiente**.
      Se muestra la pantalla **Credenciales de cuentas de usuario**. Seleccione las opciones según la versión existente de Wyse Management Suite.
      - Si está actualizando de la versión 3.3 o 3.3.1 a 3.6 de Wyse Management Suite, se mostrarán las siguientes opciones:
        - **Crear un nuevo usuario local**: seleccione esta opción para ingresar las credenciales y crear un nuevo usuario local con los privilegios mínimos. El nuevo usuario se agrega al grupo **Usuarios**, pero no tendrá derechos de administrador.
          NOTA: El nombre de usuario que ingrese en la pantalla **Credenciales de la cuenta de servicio** no debe ser el mismo que el nombre de usuario de Teradici. El nombre de usuario debe tener entre 2 y 20 caracteres. La contraseña debe tener entre 9 y 127 caracteres con al menos una mayúscula, una minúscula, un número y un carácter especial. No se permite colocar espacios en la contraseña.
        - **Usar un usuario local existente**: seleccione esta opción para ingresar las credenciales de un usuario local existente. Cuando seleccione esta opción, se mostrará un mensaje. Procure que el usuario ya exista, tenga derechos de inicio de sesión de servicio (**SeServiceLogonRight**) y haya iniciado sesión correctamente al menos una vez en el sistema. Dell Technologies recomienda procurar que el usuario no tenga derechos administrativos.
          NOTA: Si selecciona esta opción, la complejidad de la contraseña no se verifica y el nombre de usuario que ingrese debe tener entre 2 y 20 caracteres.
        - **Usar un usuario de dominio existente**: seleccione esta opción para ingresar las credenciales de un usuario de dominio existente. Cuando seleccione esta opción, se mostrará un mensaje. Procure que el usuario ya exista en el dominio, tenga derechos de inicio de sesión de servicio (**SeServiceLogonRight**) y haya iniciado sesión correctamente al menos una vez en el sistema. Dell Technologies recomienda procurar que el usuario no tenga derechos administrativos.
          NOTA: Si selecciona esta opción, no se verifica la complejidad de la contraseña.
      - Si va a actualizar de la versión 3.5 a 3.6 de Wyse Management Suite, ingrese las credenciales para crear un usuario local con privilegios mínimos. Los servicios de Dell Wyse Management Suite se ejecutan en esta cuenta de usuario.
   c. Haga clic en **Siguiente** después de ingresar las credenciales.
      Aparece la pantalla **Credenciales del vault de software**. El vault de software se utiliza para almacenar datos confidenciales requeridos por la aplicación Dell Wyse Management Suite.

d. Ingrese la contraseña del vault de software.
   La contraseña debe tener más de ocho caracteres.
e. Haga clic en **Siguiente**.

NOTA: Si EM SDK está instalado en el servidor durante la instalación anterior de Wyse Management Suite, los componentes de Teradici EM SDK se actualizan automáticamente. Si EM SDK no está instalado en el dispositivo durante la instalación anterior, seleccione la casilla de verificación **Teradici EM SDK** para instalar y configurar los componentes de Teradici EM SDK.

NOTA: También puede instalar y actualizar Teradici EM SDK con el instalador de Wyse Management Suite.

6. Seleccione un puerto para la comunicación MQTT segura. El puerto predeterminado es 8443.

   NOTA: El número de puerto para la comunicación MQTT segura no debe ser 0. La opción de selección de puertos se muestra cuando se actualiza Wyse Management Suite de las versiones 3.1 y 3.1.1 a la versión 3.6.

7. Seleccione la casilla de verificación **Aplicar cambios recomendados** si desea cambiar las direcciones URL.

   NOTA: Se muestra la ventana **Actualizar configuración de MQTT** cuando se actualiza Wyse Management Suite de las versiones 3.2 y 3.2.1 a la versión 3.6.

8. Haga clic en **Siguiente**.
9. Haga clic en **Iniciar** para abrir la consola web de Wyse Management Suite.

9

Desinstalación de Wyse Management Suite

Para desinstalar Wyse Management Suite, haga lo siguiente:

1. Haga doble clic en el icono **WMS**.

   Se iniciará el asistente de desinstalación y aparecerá la pantalla **Desinstalador de Wyse Management Suite**.

2. Haga clic en **Siguiente**. De manera predeterminada, el botón de selección **Quitar** estará seleccionado para desinstalar todos los componentes del instalador de Wyse Management Suite.

10

Solución de problemas en Wyse Management Suite

En esta sección, se proporciona información para la solución de problemas en Wyse Management Suite.

Problemas con el acceso a la consola web de Wyse Management Suite

- Problema: Cuando intenta conectarse a la consola de Wyse Management Suite, la GUI de autenticación no aparece y se muestra una página de estado HTTP 404.

  Solución alternativa: detenga e inicie los servicios en el orden siguiente:
  1. Dell WMS: MariaDB
  2. Dell WMS: memcached
  3. Dell WMS: MongoDB
  4. Dell WMS: Servicio de agente de MQTT
  5. Dell WMS: Servicio Tomcat

- Problema: cuando intenta conectarse a la consola de Wyse Management Suite, la GUI de autenticación no aparece y se muestra el siguiente mensaje de error:

  Esta página no puede mostrarse

  Solución: reinicie Dell WMS: servicio Tomcat

- Problema: La consola web de Wyse Management Suite no responde o la información en la página web no se muestra correctamente al utilizar Internet Explorer.

  Solución alternativa:
  - Asegúrese de utilizar la versión compatible de Internet Explorer.
  - Asegúrese de que la seguridad mejorada de Internet Explorer está desactivada.
  - Asegúrese de que la configuración de vista de compatibilidad está desactivada.

Registrar dispositivos con Wyse Management Suite

NOTA: Para obtener información sobre el entorno de seguridad del cliente, consulte Wyse Device Agent.

- Problema: no se pueden registrar dispositivos con Wyse Management Suite en una nube pública

  Solución alternativa:
  - Asegúrese de que los puertos 443 y 1883 estén abiertos.
  - Compruebe su conectividad de red y acceda a la aplicación web Wyse Management desde el explorador para nube pública.
  - Si **Detección automática** está activada, compruebe que los registros DHCP o SVR DNS estén configurados correctamente. Compruebe también la URL del servidor y los token de grupo.
  - Compruebe si puede registrar el dispositivo manualmente.

- Problema: no se pueden registrar dispositivos con Wyse Management Suite en una nube privada.

  Solución alternativa:

- Asegúrese de que los puertos 443 y 1883 estén abiertos.
- Compruebe la conectividad a Internet y si es que puede acceder a la aplicación web Wyse Management desde el explorador.
- Si la opción Detección automática está activada, compruebe que los registros DHCP o SRV DNS estén configurados correctamente. Compruebe también la URL del servidor y los token de grupo.
- Compruebe si puede registrar el dispositivo manualmente.
- Compruebe si está utilizando certificados autofirmados o reconocidos.

  NOTA: De manera predeterminada, Wyse Management Suite instala certificados autofirmados. La validación de CA debe estar desactivada para que los dispositivos puedan comunicarse con el servidor de Wyse Management Suite.

Error al enviar comandos al dispositivo

Problema: no es posible enviar comandos como actualización de paquetes, reinicio de dispositivo, entre otros.

Solución alternativa:

- Asegúrese de que Dell WMS: Servicio de agente de MQTT se esté ejecutando en el servidor de Wyse Management Suite.
- Compruebe que el puerto 1883 está abierto.
- Asegúrese de que el dispositivo no está apagado o en estado de reposo antes de enviar un comando.

11

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

12

Recursos adicionales

Para ver tutoriales en video sobre:

- La instalación de Wyse Management Suite, consulte Instalación de Wyse Management Suite.
- La configuración automática de los clientes de ThinOS mediante Wyse Management Suite en las instalaciones con etiquetas de opción de DHCP, consulte Configurar dispositivos ThinOS utilizando Wyse Management Suite.

A

Base de datos remota

Una base de datos (DB) remota o en la nube es una base de datos diseñada para un entorno virtualizado, como una nube híbrida, una nube pública o una nube privada. En Wyse Management Suite, puede configurar la base de datos Mongo (MongoDB), la base de datos Maria (MariaDB) o ambas bases según sus requisitos.

Temas:

Configuración de la base de datos de Mongo

Requisitos previos

La base de datos Mongo (MongoDB) funciona en el puerto TCP (Protocolo de control de transmisión) número 27017.

NOTA: Reemplace cualquier valor que esté en negrita con sus variables de entorno, según corresponda.

Pasos

1. Instale MongoDB versión 4.2.16.
2. Copie los archivos MongoDB a su sistema local: `C:\Mongo`.
3. Cree los siguientes directorios si no existen:
   - `C:\data`
   - `C:\data\db`
   - `C:\data\log`
4. Vaya a la carpeta Mongo (`C:\Mongo`) y cree un archivo llamado `mongod.cfg`.
5. Abra el archivo `mongod.cfg` en un bloc de notas y agregue el siguiente script:

```
systemLog:
destination:file
path:c:\data\log\mongod.log
storage:
dbPath:c:\data\db
```

6. Guarde y cierre el archivo `mongod.cfg`.
7. Abra el símbolo del sistema como administrador y ejecute el siguiente comando:

   ```
   mongod.exe --config "C:\Program Files\MongoDB\Server\4.2\mongod.cfg" -install o sc.exe
   create MongoDB binPath= "\"C:\ProgramFiles\MongoDB\Server\3.2\bin\mongod.exe\"--service --
   config=\"C:\ProgramFiles\MongoDB\Server\4.2\mongod.cfg\"" DisplayName= "Dell WMS: MongoDB"
   start="auto"
   ```

   MongoDB está instalado.
8. Para iniciar los servicios MongoDB, ejecute el siguiente comando:

   ```
   net start mongoDB
   ```
9. Para iniciar la base de datos Mongo, ejecute el siguiente comando:

   ```
   mongo.exe
   ```
10. Para abrir la base de datos de administrador predeterminada, ejecute el siguiente comando:

    ```
    use admin;
    ```
11. Después de que aparezca la hoja MongoDB, ejecute los siguientes comandos:

```
db.createUser(
{
```

```
user:"wmsuser",
pwd:"PASSWORD",
roles:[{role:"userAdminAnyDatabase",db:"admin"},
{role:"dbAdminAnyDatabase",db:"admin"},
{role:"readWriteAnyDatabase",db:"admin"},
{role:"dbOwner",db:"stratus"}]
}
)
```

12. Para cambiar a la base de datos de estrato, ejecute el siguiente comando:

    `use stratus;`

13. Para detener los servicios MongoDB, ejecute el siguiente comando:

    `net stop mongoDB`

14. Agregue un permiso de autenticación a la base de datos de administración. Modifique el archivo `mongod.cfg` con lo siguiente:

```
systemLog:
destination:file
path:c:\data\log\mongod.log
storage:
dbPath:c:\data\db
security:
authorization:enabled
```

15. Para reiniciar el servicio MongoDB, ejecute lo siguiente:

    `net Start mongoDB;`

Siguientes pasos

En el instalador de Wyse Management Suite, el administrador debe utilizar el mismo nombre de usuario y la contraseña que se crearon para acceder a las bases de datos de estrato en MongoDB. Para obtener más información acerca de cómo configurar MongoDB en el instalador de Wyse Management Suite, consulte Instalación personalizada.

Configuración de la base de datos Maria

La base de datos Maria (MariaDB) funciona en el puerto TCP (Protocolo de control de transmisión) número 3306.

Sobre esta tarea

NOTA:

- La dirección IP que aparece aquí pertenece al servidor de Wyse Management Suite que aloja los componentes web.
- Reemplace cualquier valor que esté en negrita con sus variables de entorno, según corresponda.

Para configurar MariaDB, haga lo siguiente:

Pasos

1. Instale MariaDB versión 10.2.29.
2. Vaya a la ruta de instalación de MariaDB: `C:\Program Files\MariaDB 10.2\bin>mysql.exe -u root -p.`
3. Proporcione la contraseña raíz que se creó durante la instalación
4. Cree el estrato de la base de datos: `DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_unicode_ci;.`
5. Cree el usuario `'stratus'@'localhost';`
6. Cree el usuario `'stratus'@'`**IP ADDRESS**`';`
7. Establezca una contraseña para `'stratus'@'localhost'=password('`**PASSWORD**`');`
8. Establezca una contraseña para `'stratus'@'IP ADDRESS'=password('`**PASSWORD**`');`
9. Proporcione todos los privilegios en `*.* to 'stratus'@'`**IP ADDRESS**`'` identificado por `'`**PASSWORD**`'` con una opción de concesión.
10. Proporcione todos los privilegios en `*.* to 'stratus'@'localhost'` identificado por `'`**PASSWORD**`'` con una opción de concesión.

Siguientes pasos

NOTA: Para configurar un puerto personalizado para MariaDB, vaya a `C:\Program Files\MariaDB 10.2\bin>mysql.exe -u root -p -P<custom port>` en el segundo paso.

En el instalador de Wyse Management Suite, el administrador debe utilizar el mismo nombre del usuario y la contraseña que se crearon para acceder a las bases de datos de estrato en MariaDB. Para obtener más información acerca de cómo configurar MariaDB en el instalador de Wyse Management Suite, consulte Instalación personalizada.

B

Instalación personalizada

En la instalación personalizada, puede seleccionar una base de datos para configurar Wyse Management Suite y debe manejar los conocimientos técnicos operativos básicos de Wyse Management Suite. Dell recomienda la instalación personalizada solo para usuarios avanzados.

1. Seleccione el **Tipo de configuración** como **Personalizada** y haga clic en **Siguiente**.

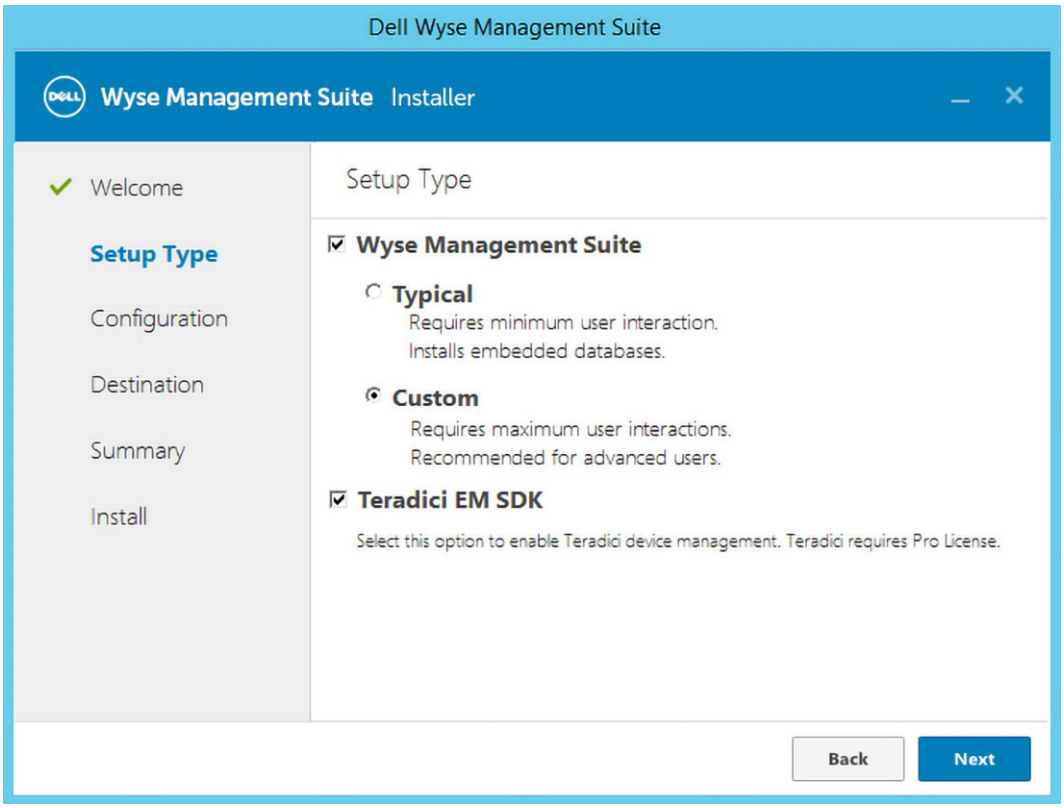

Ilustración 12. Tipo de configuración

Aparecerá la página **Servidor de base de datos Mongo**.

2. Seleccione **MongoDB integrado** o **MongoDB externo** como el servidor de base de datos Mongo.
   - Si **MongoDB integrado** está seleccionado, entonces proporcione su contraseña y haga clic en **Siguiente**.

     NOTA: La contraseña debe tener entre 9 y 31 caracteres.

     NOTA: Los detalles de nombre de usuario y servidor de base de datos no son necesarios si se selecciona la base de datos Mongo integrado y los campos correspondientes aparecerán en gris.

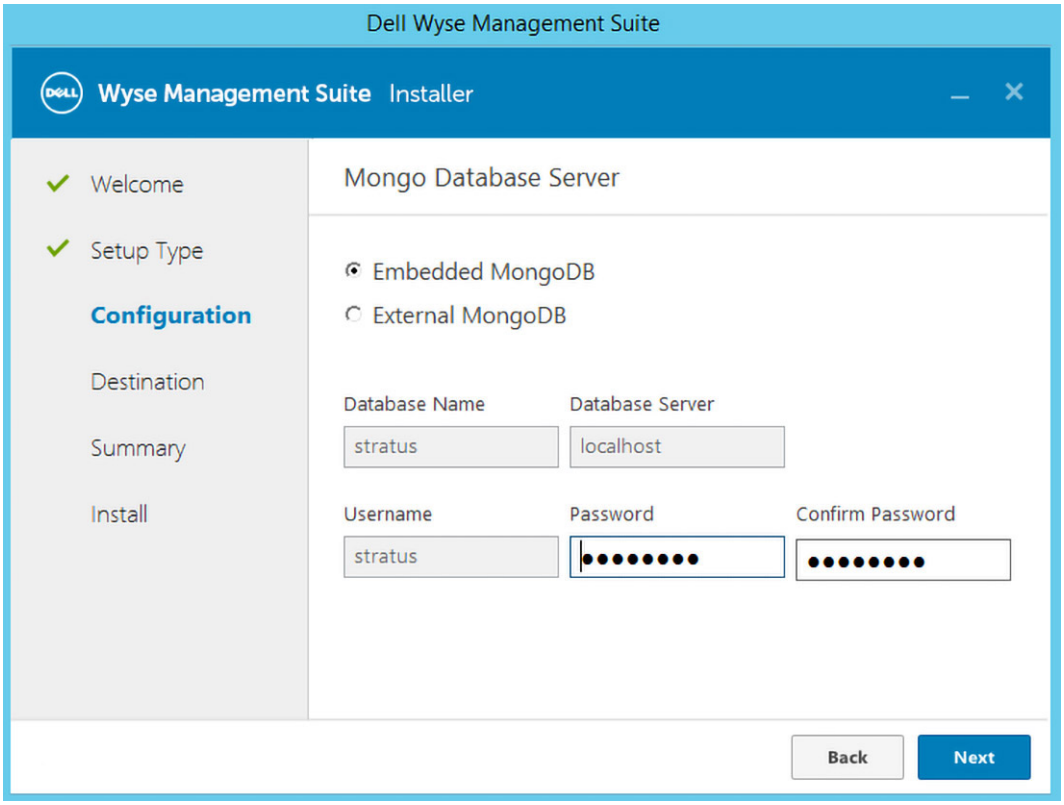

Ilustración 13. Servidor de base de datos Mongo integrado

- Si **MongoDB externo** está seleccionado, entonces proporcione el nombre del usuario, la contraseña, los detalles del servidor de base de datos y los detalles de puerto, y haga clic en **Siguiente**.

  NOTA: El campo "puerto" rellena el puerto predeterminado, el cual se puede cambiar.

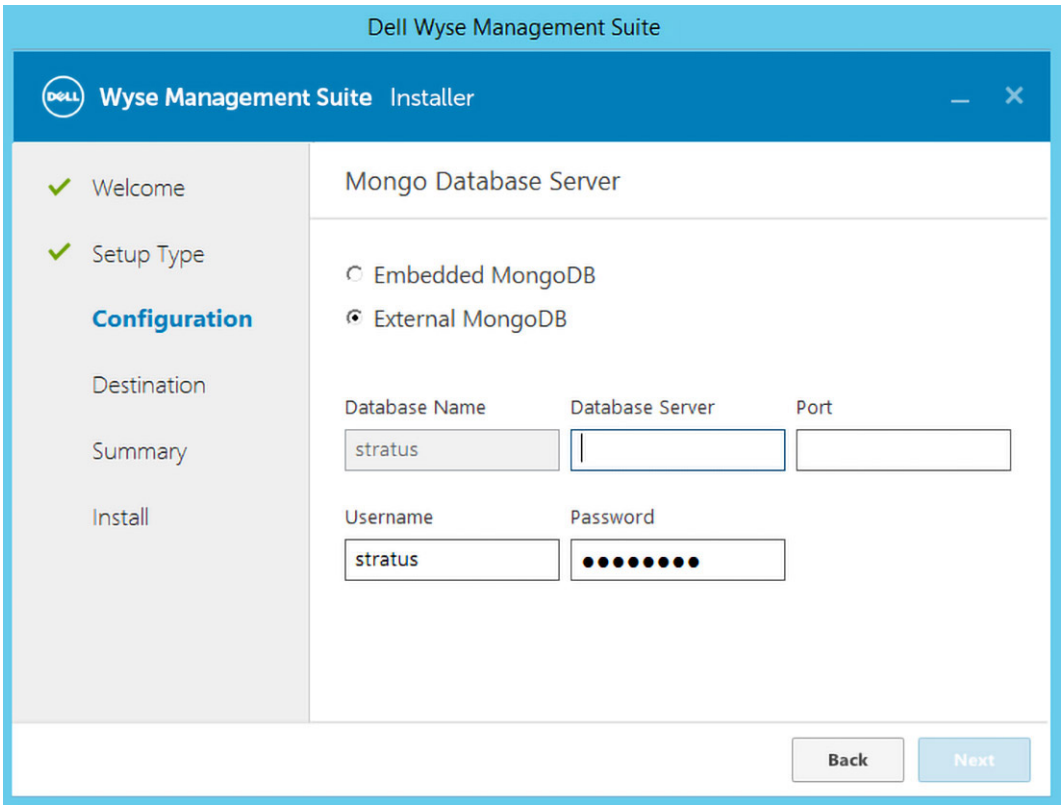

Ilustración 14. MongoDB externo

Aparecerá la página **Servidor de base de datos MariaDB**.

3. Seleccione **MariaDB integrado** o **MariaDB externo** como el servidor de base de datos MariaDB.

- Si **MariaDB integrado** está seleccionado, proporcione el nombre de usuario y la contraseña, y haga clic en **Siguiente**.

  NOTA: La contraseña debe tener entre 9 y 31 caracteres.

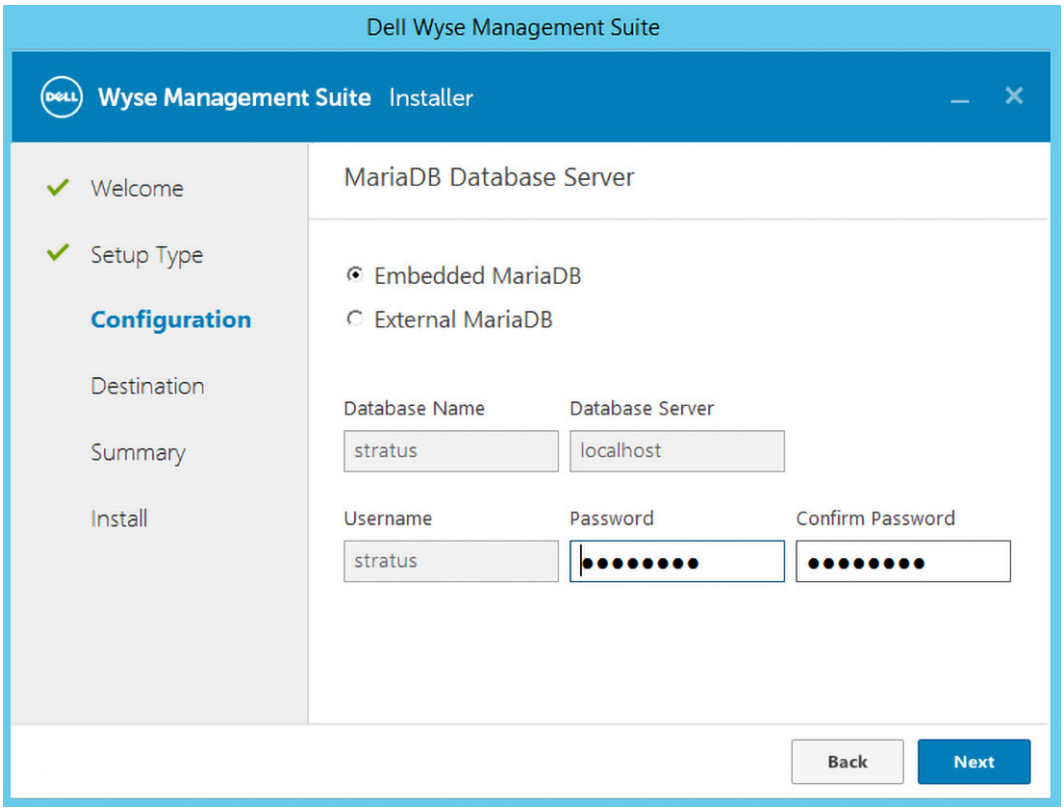

Ilustración 15. MariaDB integrado

- Si **MariaDB externo** está seleccionado, proporcione el nombre del usuario, la contraseña, los detalles del servidor de base de datos y los detalles de puerto, y haga clic en **Siguiente**.

  El campo "puerto" rellena el puerto predeterminado, el cual se puede cambiar.

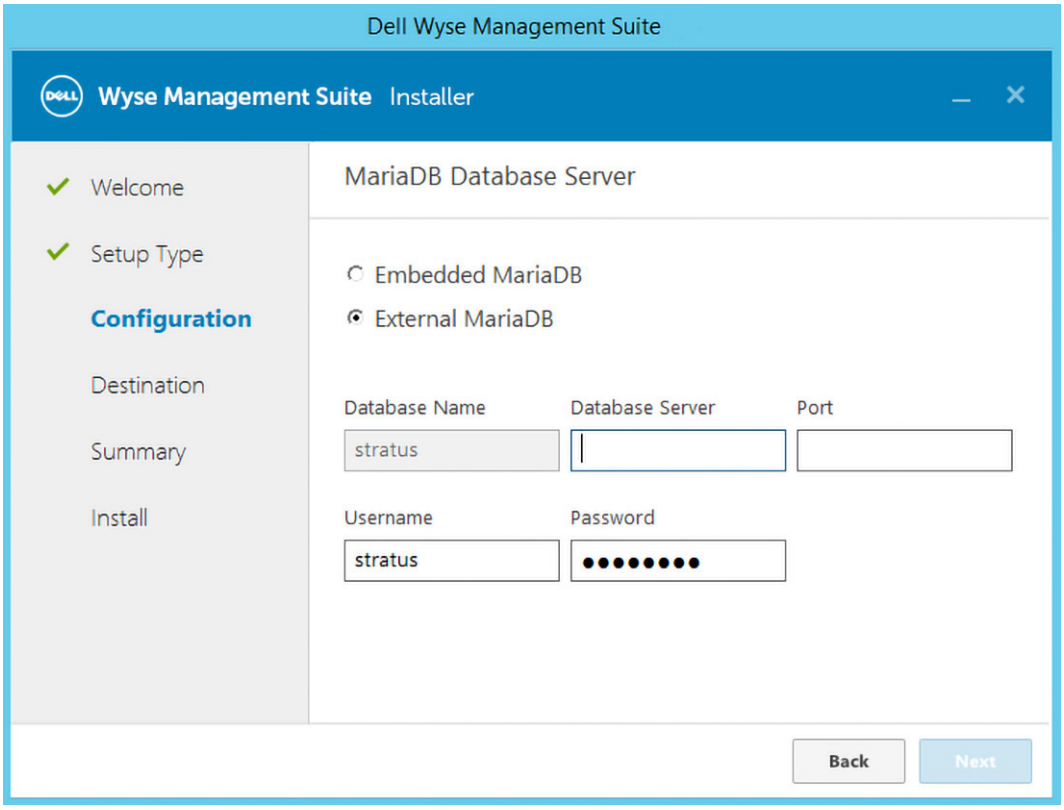

Ilustración 16. MariaDB externo

4. Aparecerá la página **Puerto**, la cual le permite personalizar los puertos para las siguientes bases de datos:
   - Apache Tomcat
   - Base de datos MySQL
   - Base de datos Mongo
   - Agente MQTT v3.1
   - Memcached

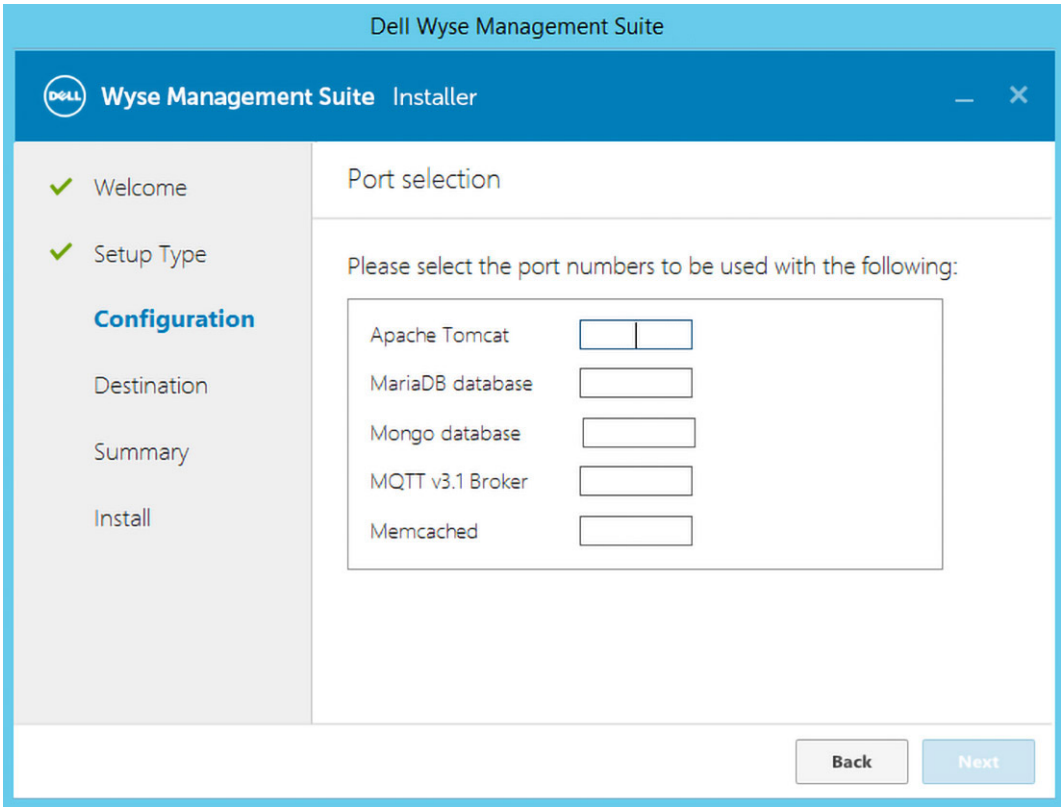

Ilustración 17. Selección de puerto

NOTA: Wyse Management Suite utiliza las bases de datos Maria y Mongo para lo siguiente:

Base de datos Maria: base de datos relacional para datos que requieren una estructura y una normalización bien definidas

Base de datos Mongo: base de datos no perteneciente a SQL para obtener rendimiento y escalabilidad

Para completar la instalación, siga los pasos indicados en la sección Instalación local de WMS y configuración inicial.

C

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.

La versión de TLS seleccionada debe ser igual o superior a la versión de TLS configurada en el servidor de Wyse Management Suite. Asegúrese de seleccionar todas las versiones adecuadas de TLS según los criterios de soporte de los dispositivos que se están administrando.

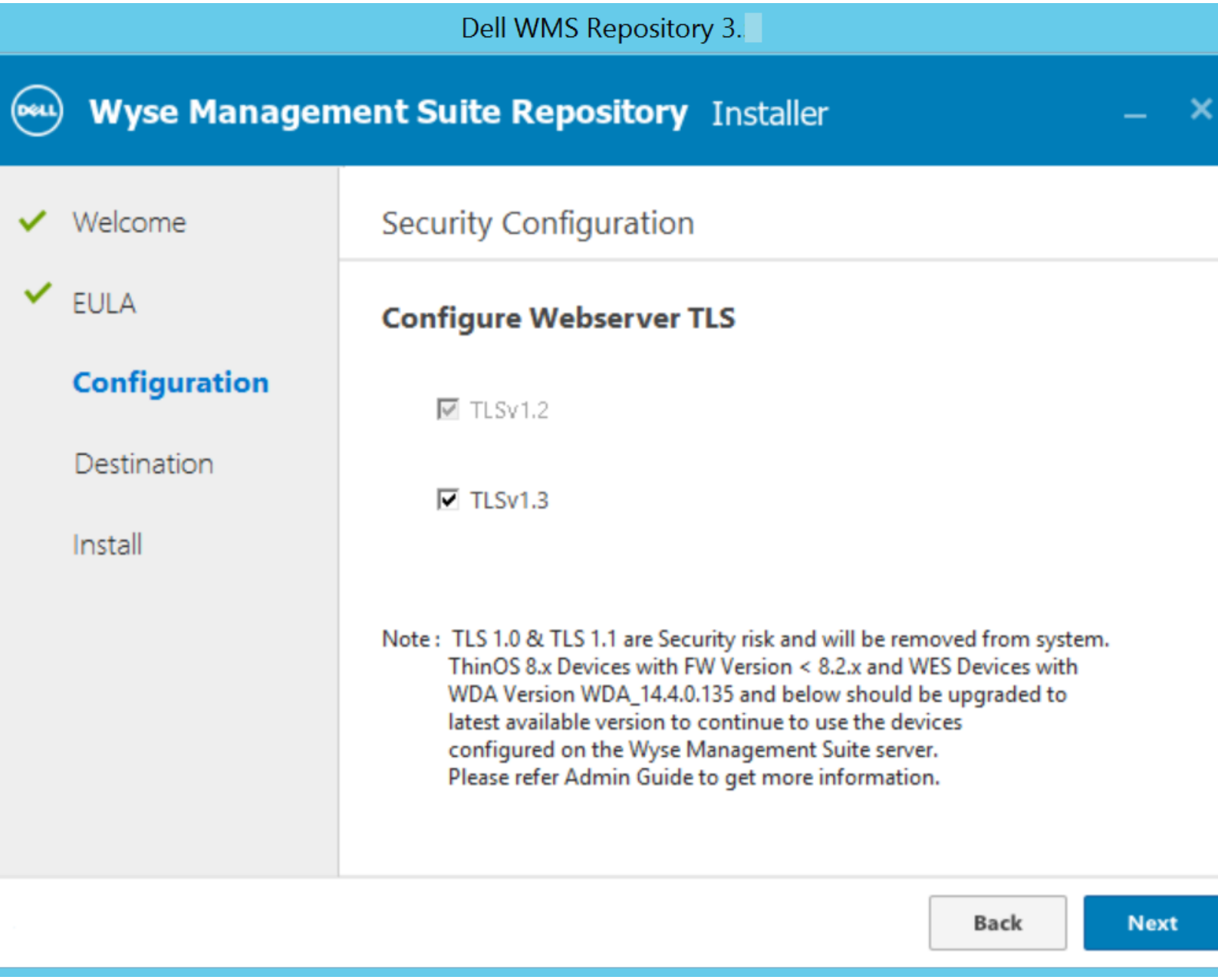

Ilustración 18. Instalador del repositorio de Wyse Management Suite

NOTA: No seleccione TLSv1.1 ni versiones posteriores si la versión de WDA en el dispositivo Windows Embedded es inferior a 14.4.0.153_Unified, y si utiliza el agente de procesamiento de imágenes Merlin. No se debe seleccionar TLSv1.1 ni versiones posteriores si utiliza la herramienta de importación para migrar de Wyse Device Manager a Wyse Management Suite.

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 el 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 está 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.
13. Agregue una nota en el cuadro disponible.
14. Haga clic en **Guardar configuración**.

D

Creación y configuración de las etiquetas de opción DHCP

Sobre esta tarea

NOTA: Para obtener información sobre el entorno de seguridad del cliente, consulte Wyse Device Agent.

Para crear una etiqueta de opciones de DHCP, haga lo siguiente:

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 derecho en **IPv4**.

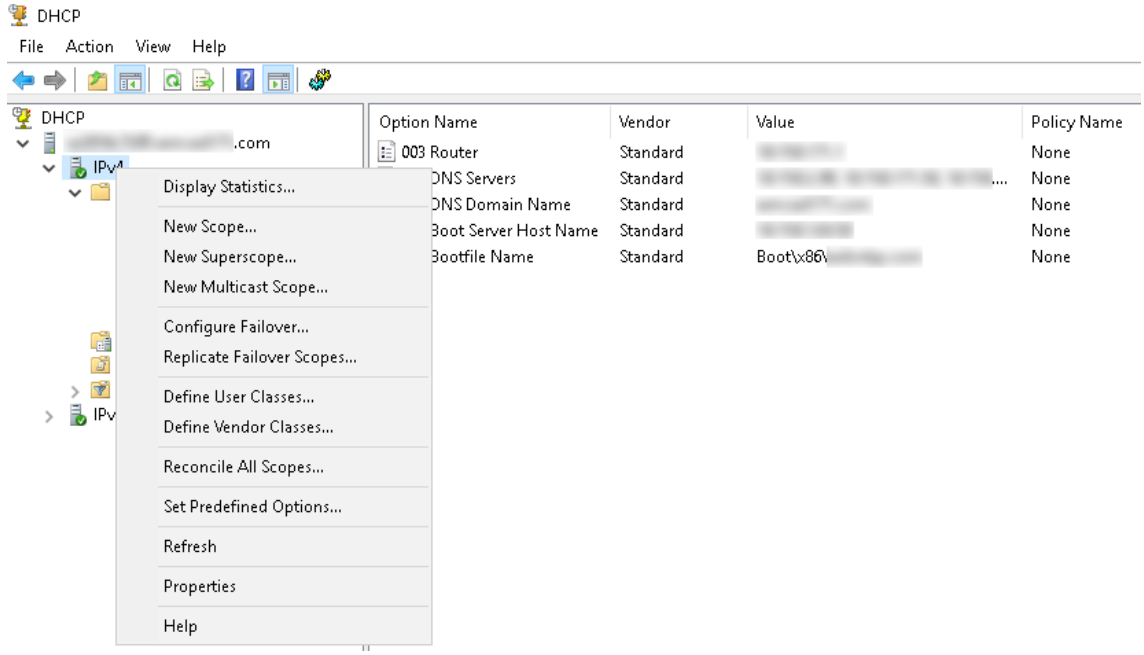

Ilustración 19. DHCP

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**.

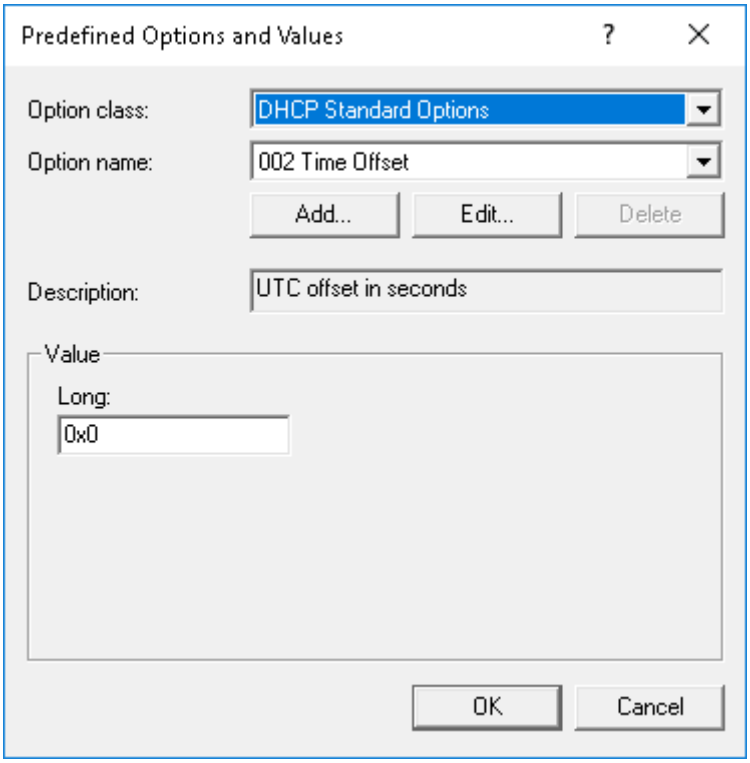

Ilustración 20. Opciones y valores predefinidos

6. Haga clic en **Agregar**.
   Se muestra la ventana **Tipo de opción**.

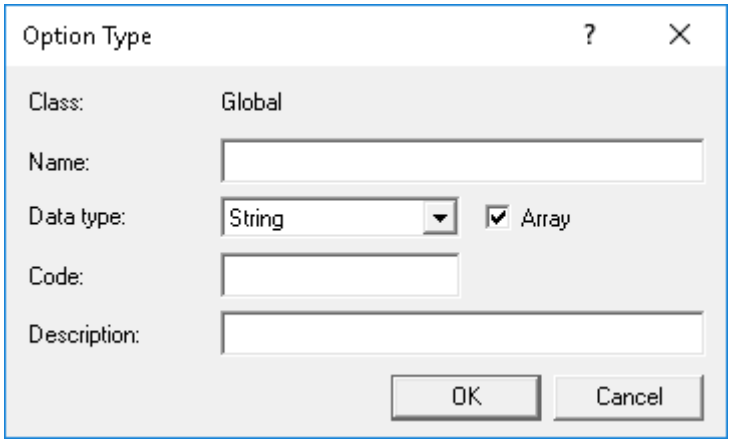

Ilustración 21. Tipo de opción

Ejemplo

Las opciones se deben agregar en las opciones del servidor DHCP o deben abarcar opciones dentro del alcance de DHCP.

Configurar etiquetas de opciones de DHCP

- Para crear la etiqueta de opción de URL del servidor Wyse Management Suite 165, haga lo siguiente:
  1. Ingrese los siguientes valores y haga clic en **Aceptar**.
     - Nombre: WMS
     - Tipo de datos: cadena
     - Código: 165
     - Descripción: servidor WMS
  2. Ingrese el siguiente valor y, a continuación, haga clic en **Aceptar**.

Cadena: `WMS FQDN`

Por ejemplo, WMSServerName.YourDomain.Com:443

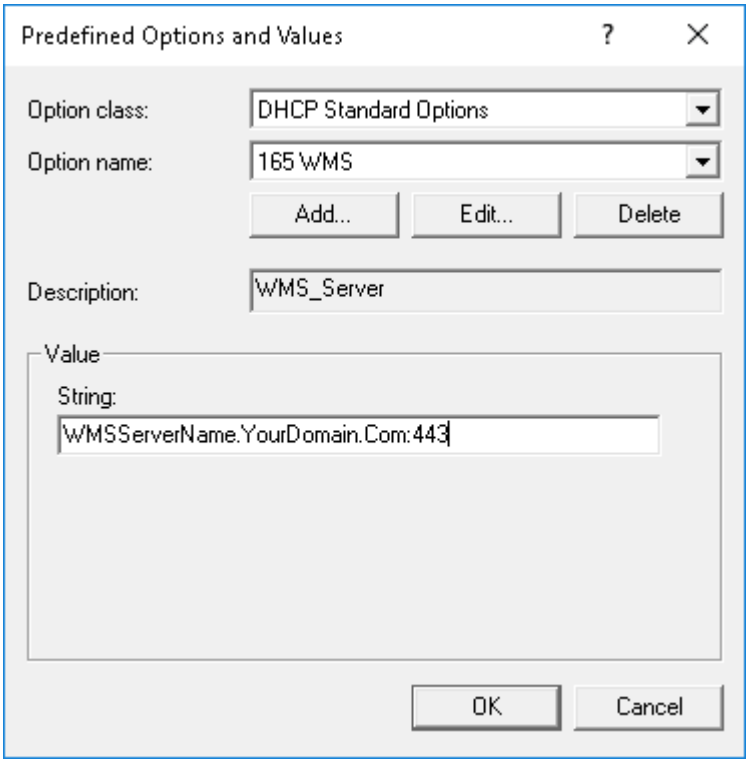

Ilustración 22. Etiqueta de opción de URL del servidor Wyse Management Suite 165

- Para crear la etiqueta de opción de URL del servidor MQTT 166, haga lo siguiente:

1. Ingrese los siguientes valores y haga clic en **Aceptar**.
   - Nombre: MQTT
   - Tipo de datos: cadena
   - Código: 166
   - Descripción: servidor MQTT
2. Ingrese el siguiente valor y haga clic en **Aceptar**.

   Cadena: `MQTT FQDN`

   Por ejemplo, WMSServerName.YourDomain.Com:1883

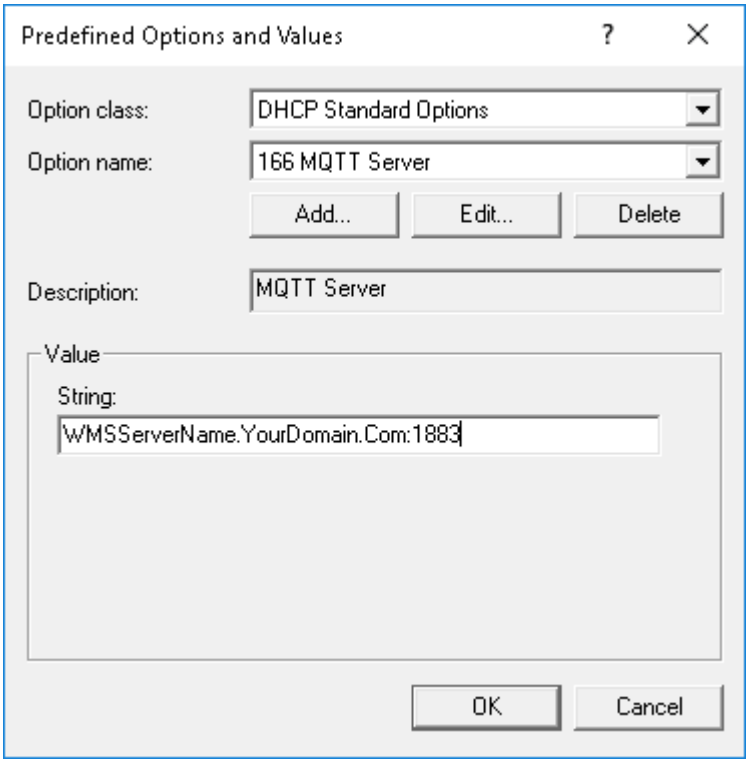

Ilustración 23. Etiqueta de opción de URL del servidor Wyse Management Suite 166

- Para crear la etiqueta de opción de URL de la validación de CA de Wyse Management Suite 167, haga lo siguiente:

  1. Ingrese los siguientes valores y haga clic en **Aceptar**.
     - Nombre: validación de CA
     - Tipo de datos: cadena
     - Código: 167
     - Descripción: validación de CA
  2. Ingrese los siguientes valores y haga clic en **Aceptar**.

     Cadena: VERDADERO/FALSO

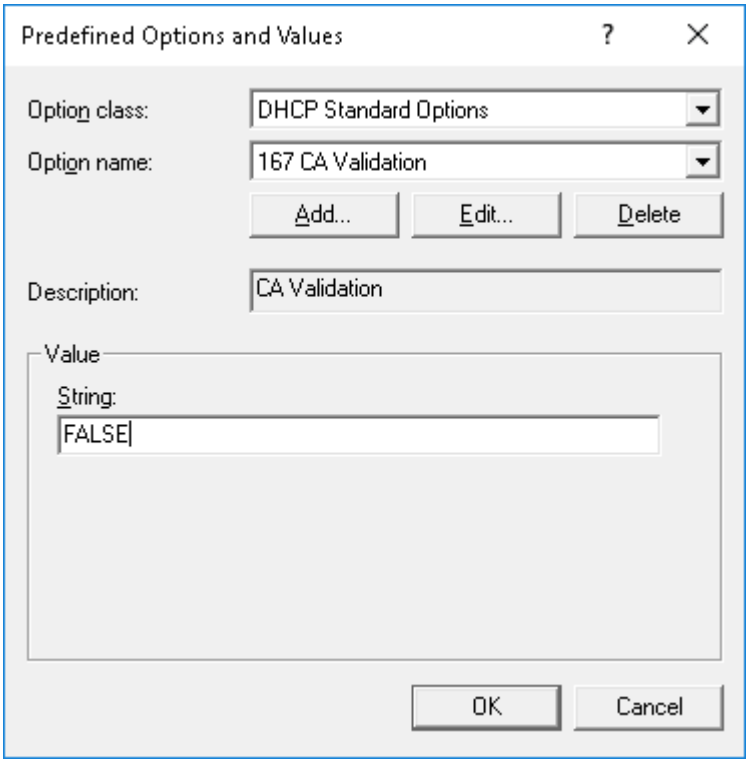

Ilustración 24. Etiqueta de opción de URL del servidor Wyse Management Suite 167

- Para crear la etiqueta de opción de URL del token de grupo de Wyse Management Suite 199, haga lo siguiente:

1. Ingrese los siguientes valores y haga clic en **Aceptar**.
   - Nombre: token de grupo
   - Tipo de datos: cadena
   - Código: 199
   - Descripción: token de grupo
2. Ingrese los siguientes valores y haga clic en **Aceptar**.

   String—defa-quarantine

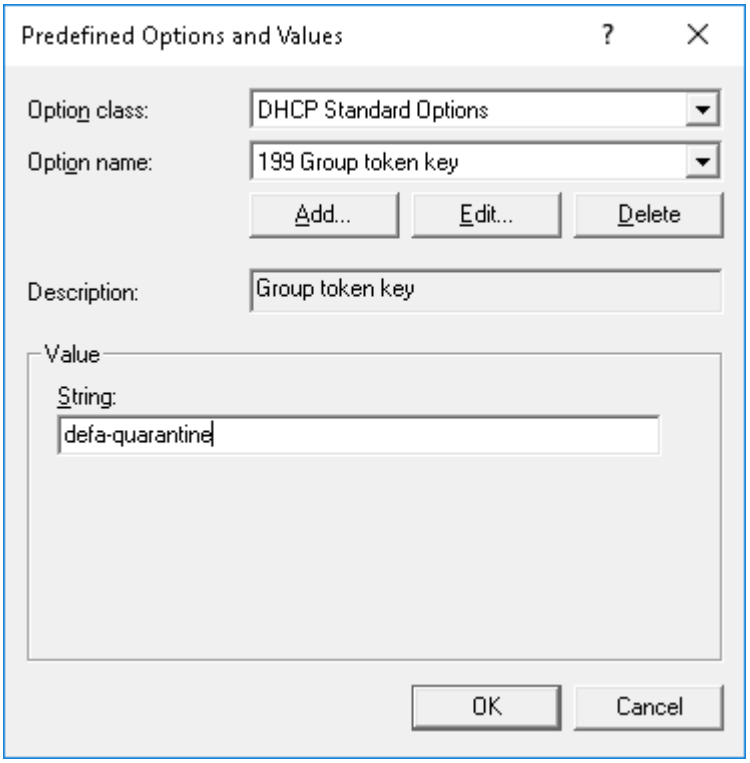

Ilustración 25. Etiqueta de opción de URL del servidor Wyse Management Suite 199

E

Creación y configuración de los registros DNS SRV

Sobre esta tarea

NOTA: Para obtener información sobre el entorno de seguridad del cliente, consulte Wyse Device Agent.

Para crear un registro SRV de DNS, haga lo siguiente:

Pasos

1. Abra el Administrador de servidores.
2. Vaya a **Herramientas** y haga clic en la **Opción DNS**.
3. Vaya a **DNS Nombre de host del servidor DNS Reenviar zonas de búsqueda Dominio _tcp** y haga clic con el botón derecho del mouse en la opción **_tcp**.

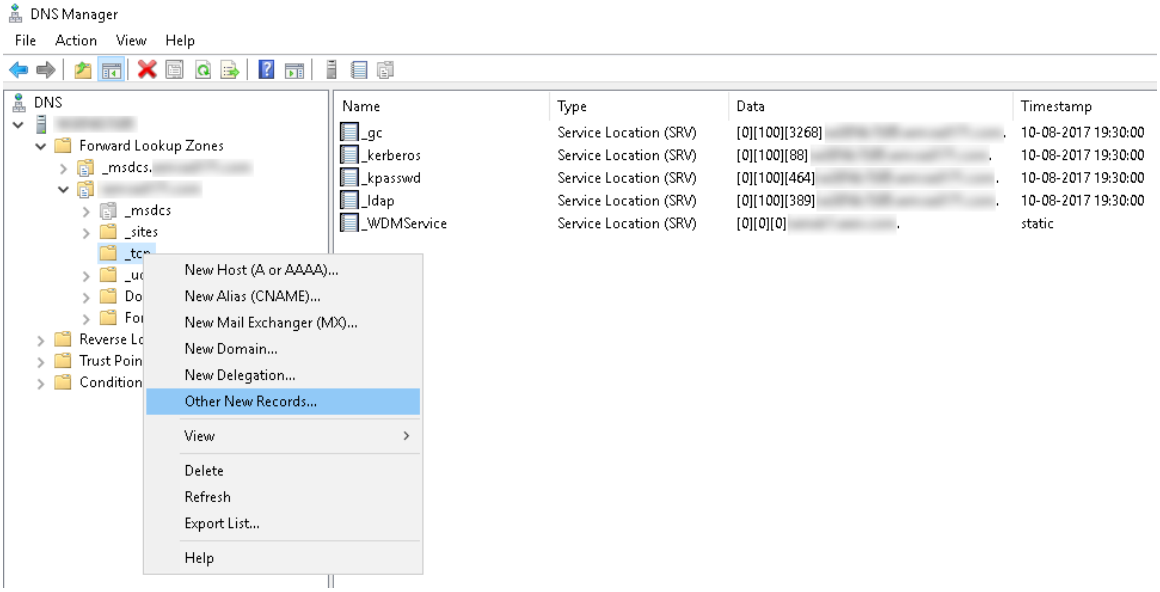

Ilustración 26. Administrador DNS

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:

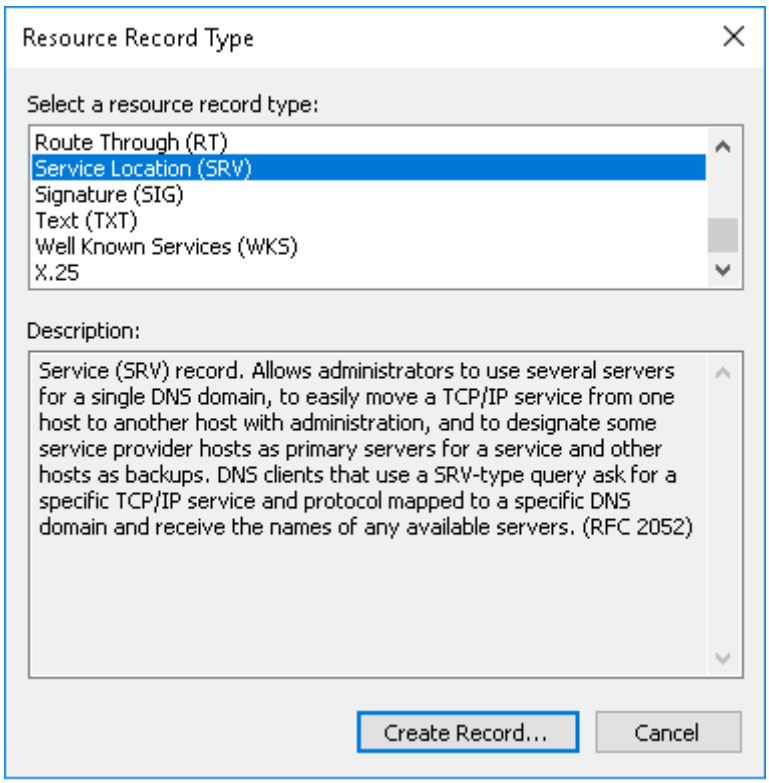

Ilustración 27. Tipo de registro de recursos

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

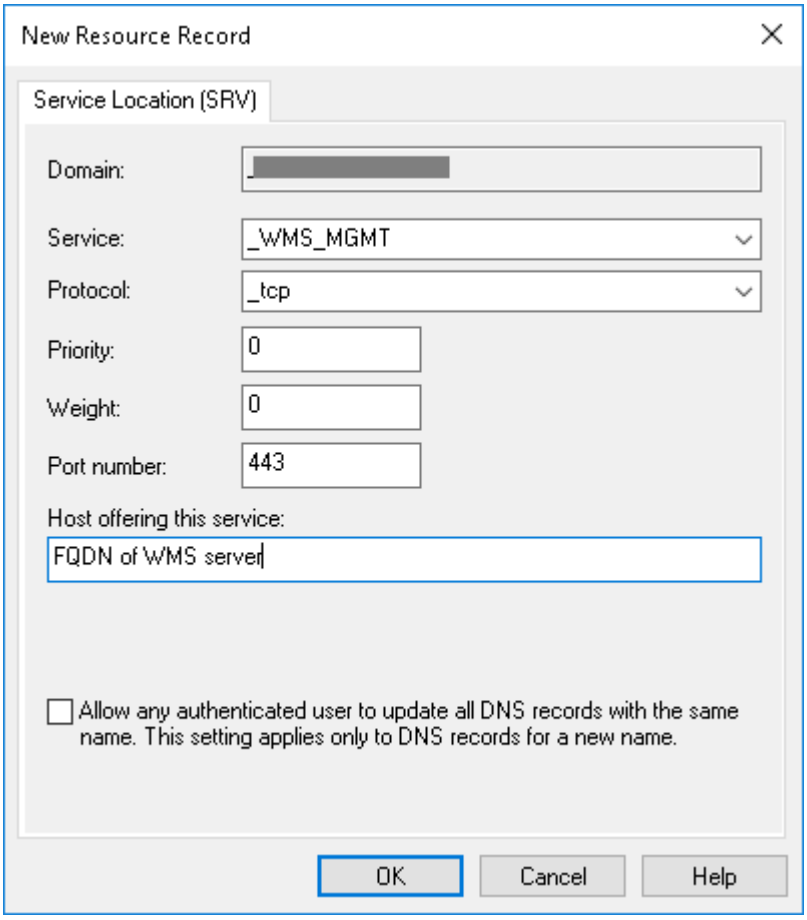

Ilustración 28. Servicio _WMS_MGMT

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

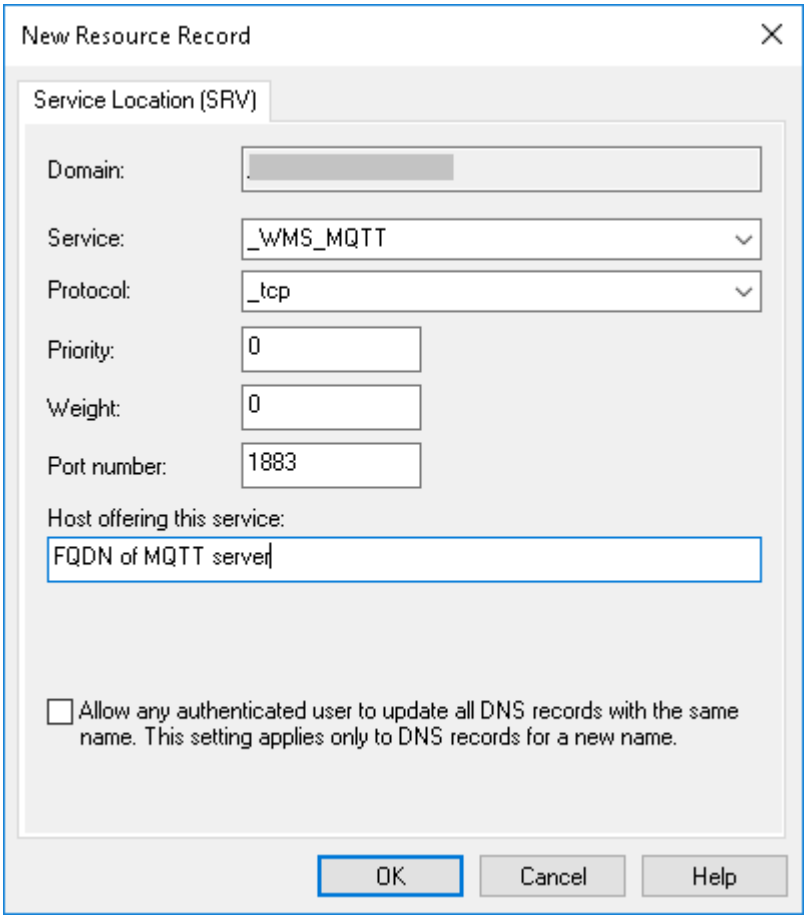

Ilustración 29. Servicio _WMS_MQTT

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:

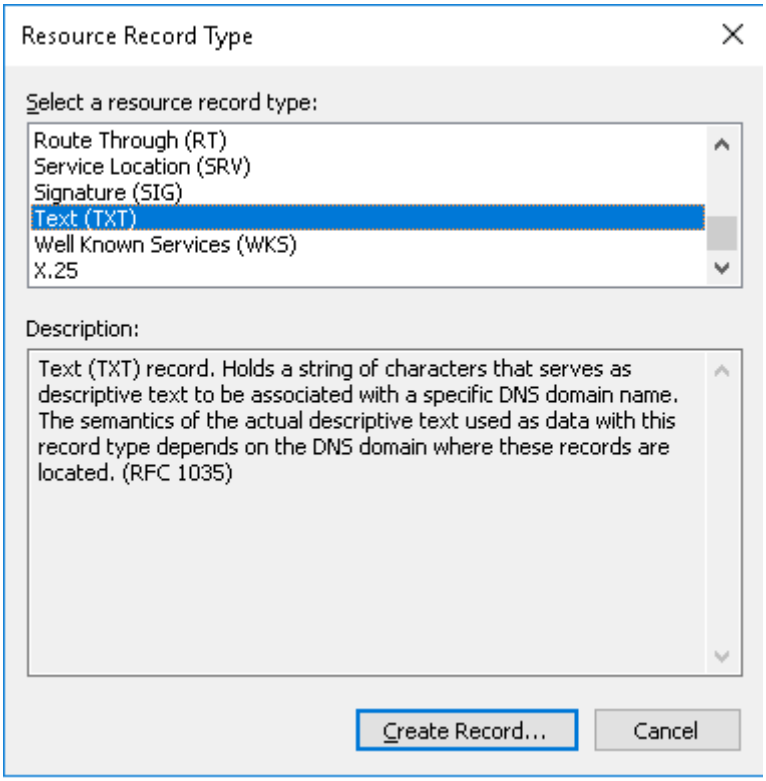

Ilustración 30. Tipo de registro de recursos

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 de WMS

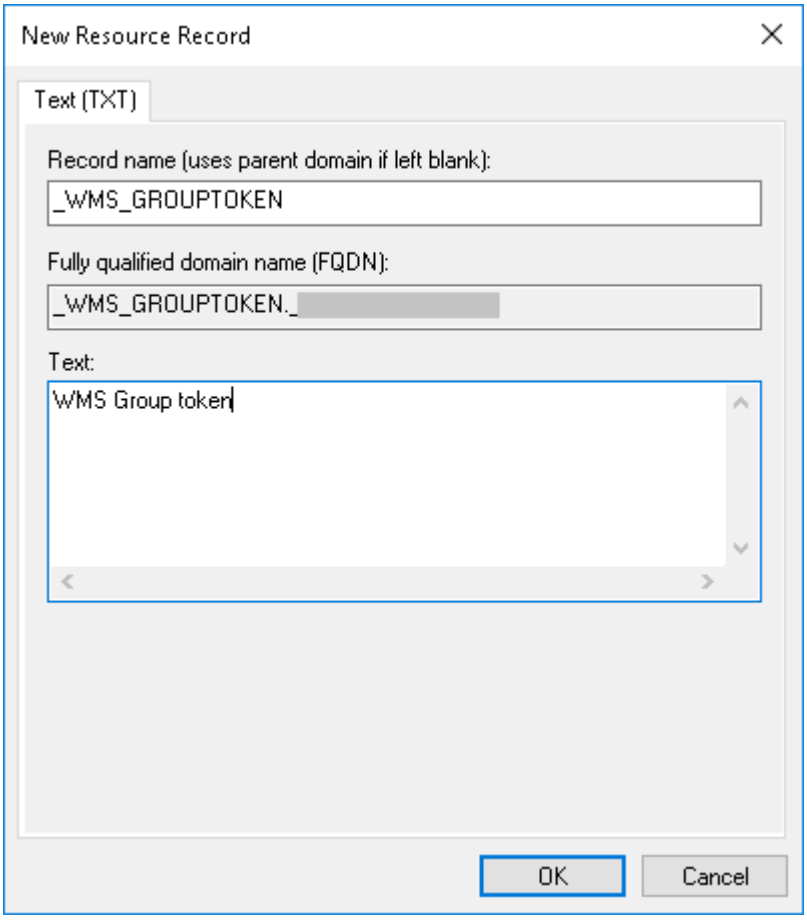

Ilustración 31. Nombre de registro _WMS_GROUPTOKEN

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

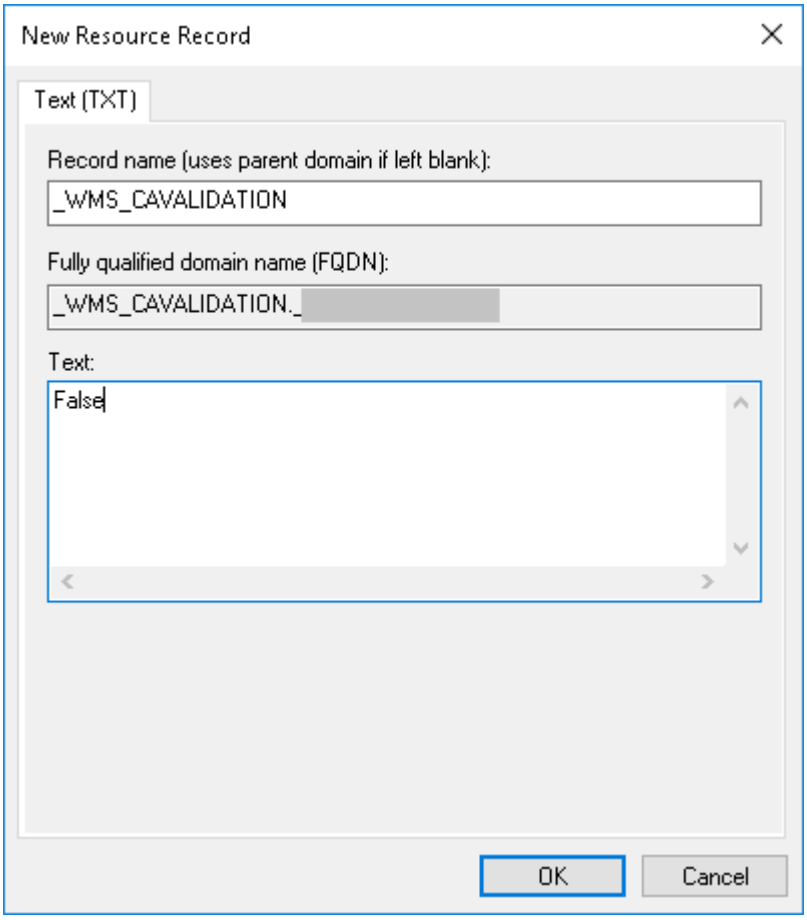

Ilustración 32. Nombre de registro _WMS_CAVALIDATION

F

Creación e implementación de políticas de aplicaciones estándar en clientes delgados

Sobre esta tarea

Para implementar una política de aplicaciones estándar en clientes ligeros, haga lo siguiente:

Pasos

1. En el repositorio local, vaya a **thinClientApps** y copie la aplicación a la carpeta.
2. Asegúrese de que la aplicación está registrada; para ello, vaya a la pestaña **Aplicaciones y datos** y seleccione **Cliente delgado** en **Inventario de aplicaciones**.

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

3. En **Políticas de la aplicación**, haga clic en **Cliente ligero**.
4. Haga clic en **Agregar política**.
5. Para crear una política de aplicaciones, ingrese la información apropiada en la ventana **Agregar política de la aplicación estándar**.
   - Seleccione **Nombre de la política**, **Grupo**, **Tarea**, **Tipo de dispositivo** y **Aplicación TC**.
   - Para implementar esta política en un sistema operativo o una plataforma en específico, seleccione **Filtro del subtipo de SO**, **Filtro de la plataforma** o **Filtro del fabricante**. El tiempo de espera muestra un mensaje en el cliente que le dará tiempo para guardar su trabajo antes de que comience la instalación. Especifique la cantidad de minutos que debe mostrarse en el cliente el cuadro de diálogo.
   - Para aplicar automáticamente esta política a un dispositivo que se ha registrado con Wyse Management Suite, seleccione **Aplicar la política a nuevos dispositivos** desde la lista desplegable **Aplicar política automáticamente**.

   NOTA: Cuando algún dispositivo se mueve al grupo definido o se registra directamente a dicho grupo, se aplica la política de aplicación. Si selecciona **Aplicar la política a los dispositivos durante registro**, la política se aplica automáticamente en el dispositivo tras registrarse en el servidor de Wyse Management Suite.

6. Para permitir un retraso en la ejecución de la política, seleccione la casilla de verificación **Permitir retraso de la ejecución de la política**. Si se selecciona esta opción, se activarán los siguientes menús desplegables:
   - Desde el menú desplegable **Máx. de horas por retraso**, seleccione la cantidad máxima de horas (de 1 a 24 horas) que puede retrasar la ejecución de la política.
   - Desde el menú desplegable **Máx. de retrasos**, seleccione la cantidad de veces (de 1 a 3) que puede retrasar la ejecución de la política.
7. 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**.
8. Haga clic en **Guardar** para crear una política.
   Se muestra un mensaje para permitir que el administrador programe esta política en los dispositivos según el grupo.
9. Seleccione **Sí** para programar un trabajo en la misma página. El trabajo de política de aplicación/imagen se puede ejecutar:
   - **Inmediatamente**: el servidor ejecuta el trabajo inmediatamente.
   - **En zona horaria del dispositivo**: el servidor crea un trabajo para cada zona horaria de dispositivo y programa el trabajo en la fecha y hora seleccionadas de la zona horaria del dispositivo.
   - **En zona horaria seleccionada**: el servidor crea un trabajo para que se ejecute en la fecha y hora de la zona horaria designada.
10. Para crear el trabajo, haga clic en **Vista previa**; los programas se mostrarán en la página siguiente.
11. Puede revisar el estado del trabajo en la página **Trabajos**.

G

Registrar manualmente un cliente híbrido Dell

Requisitos previos

Antes de registrar el dispositivo, asegúrese de que este tenga conectividad a una red para comunicarse con el servidor de Wyse Management Suite.

NOTA: Puede registrar o anular el registro del dispositivo solo desde la cuenta de usuario invitado.

Pasos

1. Inicie sesión en el cliente híbrido como usuario invitado.
2. En la barra superior, haga clic en el ícono de **Dell Client Agent**.

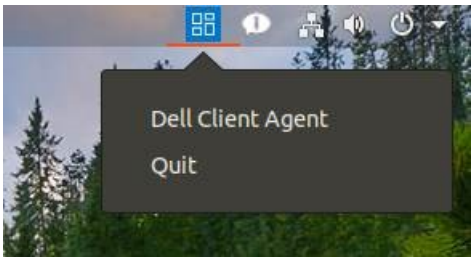

Ilustración 33. Ícono de DCA

3. Haga clic en **Dell Client Agent**.
   Aparecerá el cuadro de diálogo **Dell Client Agent**.
4. Haga clic en **Registro**.
   El estado predeterminado aparece como **Descubrimiento en curso**.
5. Para registrarse manualmente, haga clic en el botón **Cancelar**.
6. En el campo **Servidor WMS**, ingrese la URL del servidor de Wyse Management Server.
7. En el campo **Token de grupo**, ingrese su clave de registro de grupo. El token de grupo es una clave única para registrar sus dispositivos directamente en grupos.

   NOTA: Si los campos Grupo y Grupo de usuarios están vacíos, el dispositivo se registra en el grupo no administrado. Sin embargo, el token de grupo es obligatorio para registrar el dispositivo en una nube pública.

8. Haga clic en el botón **Encendido/Apagado** para activar o desactivar la opción **Validar CA de certificado del servidor**. Active esta opción para realizar la validación del certificado del servidor para todas las comunicaciones entre el dispositivo y el servidor.

   La opción Validación de CA se habilita automáticamente y no se puede deshabilitar si ingresa una dirección URL de nube pública.
9. Haga clic en **Registrar** para registrar el cliente híbrido en el servidor Wyse Management Suite.

   Cuando el cliente híbrido se registra correctamente, el estado se muestra como **Registrado** con la marca de color verde junto a la etiqueta **Estado de registro**. El título del botón **Registrar** cambia a **Anular registro**.

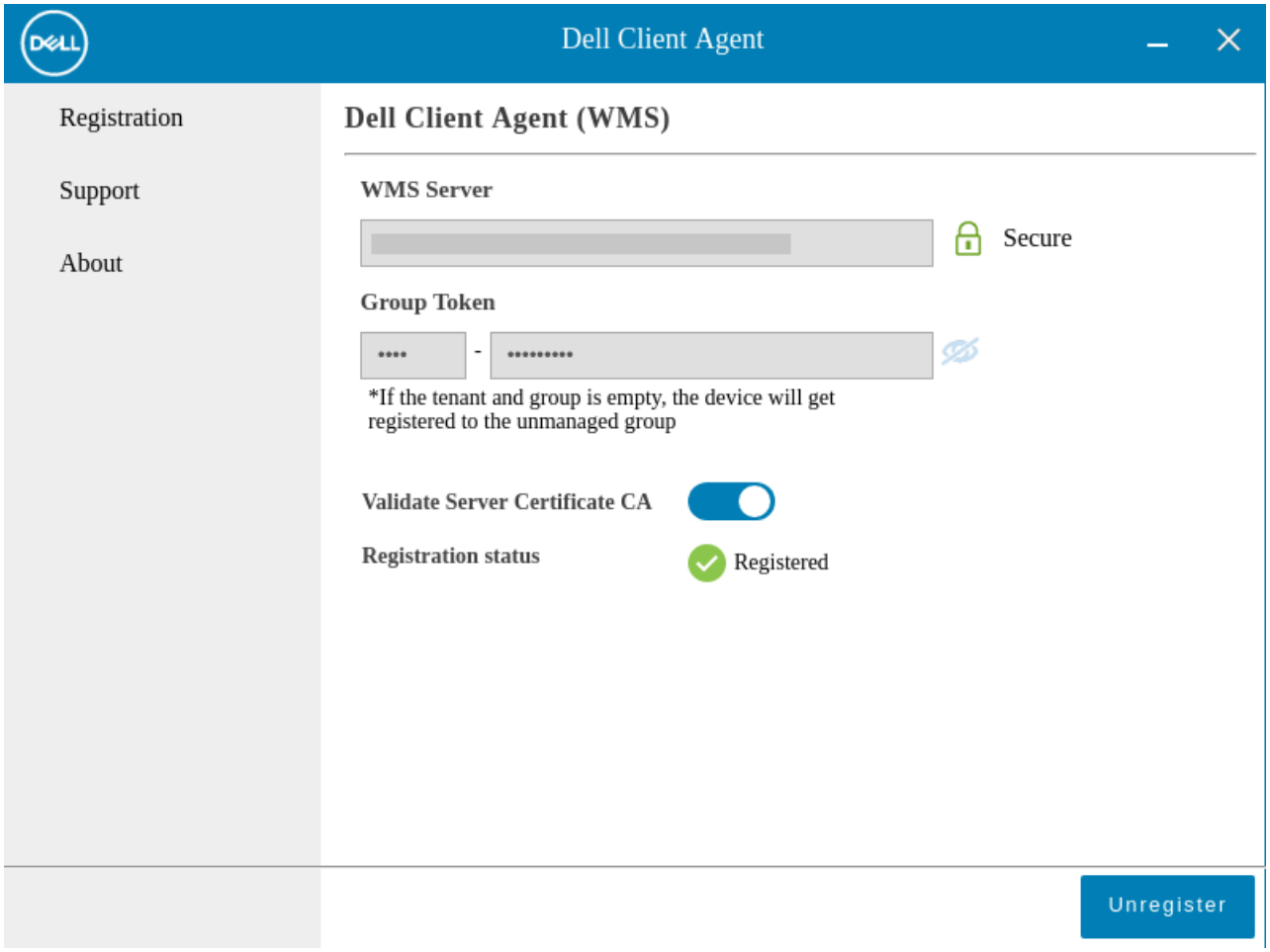

Ilustración 34. Dell Client Agent

H

Registrar dispositivos Windows Embedded Standard de forma manual

Los dispositivos Windows Embedded Standard se pueden registrar manualmente ejecutando el ícono **UI de WDA** en la barra de tareas.

1. Seleccione **Wyse Management Suite-WMS** como el servidor de administración.
2. Ingrese un inquilino y un nombre de grupo adecuados. Si este campo queda en blanco, los dispositivos se registran en un grupo no administrado. (Opcional)
3. Haga clic **Registrar**.

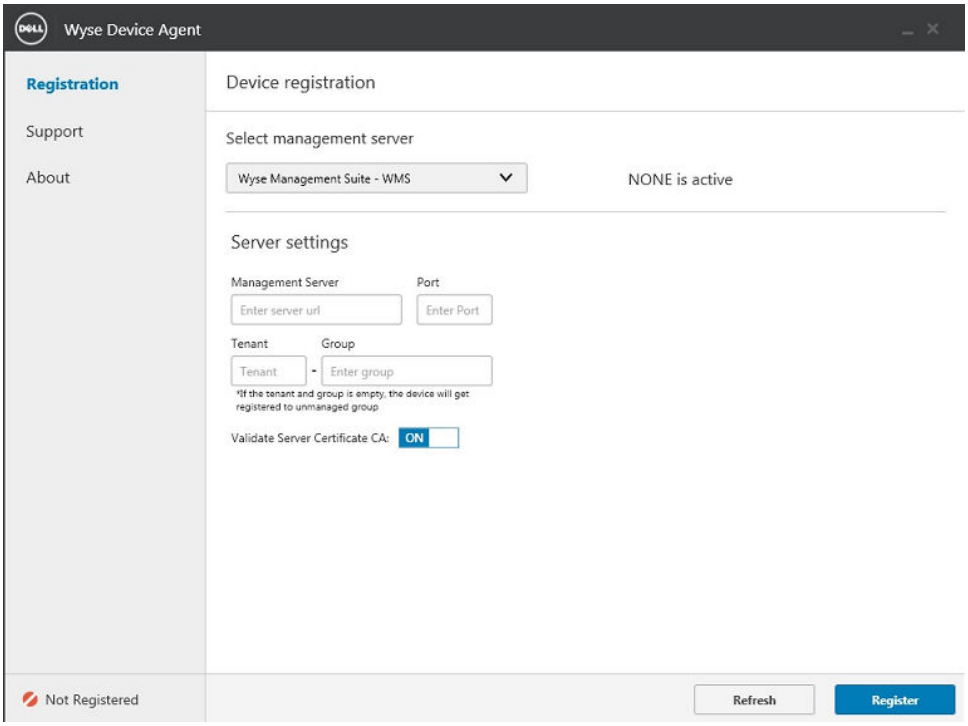

Ilustración 35. Registro de dispositivo

Registrar dispositivo ThinOS 8.x manualmente

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.

   El dispositivo está registrado en Wyse Management Suite.

J

Registrar dispositivo ThinOS 9.x manualmente

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: 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.

   El dispositivo está registrado en Wyse Management Suite.

K

Registrar dispositivo Linux de forma manual

Los dispositivos Linux se pueden registrar manualmente ejecutando el ícono **UI de WDA** desde **Configuración del sistema**.

1. Ingrese los detalles del **servidor WMS**.
2. Ingrese un inquilino y un nombre de grupo adecuados. Si este campo queda en blanco, los dispositivos se registran en un grupo no administrado. (Opcional)
3. Haga clic **Registrar**.

   El dispositivo se registra en la consola de Wyse Management Suite.

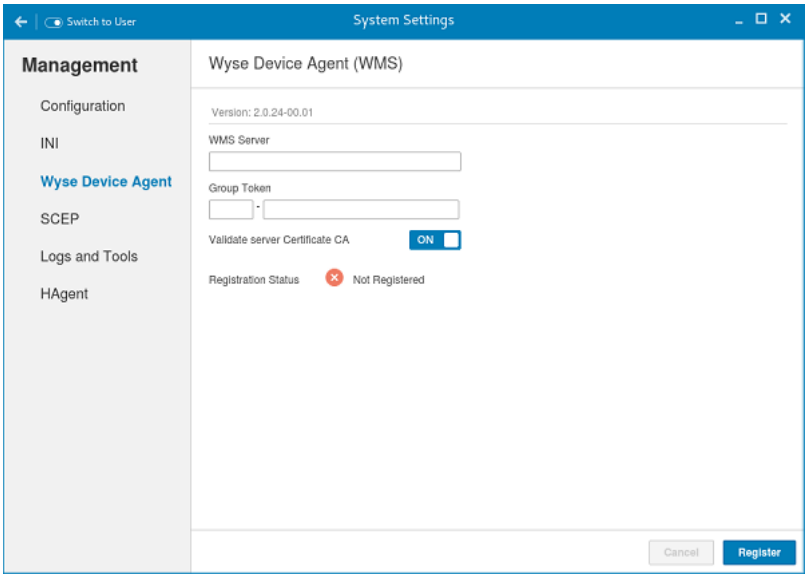

Ilustración 36. Registro de dispositivo

L

Términos y definiciones

En la siguiente tabla, se muestran los términos utilizados en este documento y sus definiciones:

Tabla 7. Términos y definiciones

Terminología	Definición
Nube privada	Servidor de Wyse Management Suite instalado en la nube que está reservado para su centro de datos principal.
WDA	Wyse Device Agent; reside en el dispositivo y actúa como agente para la comunicación entre el servidor y el cliente.
Repositorio local	Wyse Device Agent; reside en el dispositivo y actúa como agente para la comunicación entre el servidor y el cliente.
Repositorio remoto	Repositorios de aplicaciones, imágenes de sistema operativo y archivos que se pueden instalar opcionalmente para obtener escalabilidad y confiabilidad a través de zonas geográficas para transferir contenido.
Nube pública	Wyse Management Suite alojado en una nube pública con la comodidad y el ahorro de costos de no tener que configurar y mantener la infraestructura y el software.
Complemento/Aplicación	Cualquier componente o paquete que no forme parte de la compilación base y se proporciona como un componente opcional. El componente o paquete se puede implementar desde el software de administración. Por ejemplo: los agentes de conexión más recientes de VMware y Citrix.
Local	Servidor Wyse Management Suite instalado de forma local que está reservado para el centro de datos de su organización.
Inquilino	Un grupo de usuarios que comparten un acceso común con privilegios específicos a Wyse Management Suite. Es una clave única asignada a clientes específicos para acceder al conjunto de administración.
Usuarios	Los usuarios pueden ser administradores locales, administradores globales y visores. Se puede asignar a los usuarios locales y los usuarios importados desde Active Directory roles de administrador global, administrador de grupo y visor para iniciar sesión en Wyse Management Suite. Los usuarios reciben permisos para realizar operaciones según las funciones que se les asignan.