



Guía de administración de Cisco Business Dashboard y Probe, Versión 2.2.x

Primera publicación: 2020-07-14

Última modificación: 2020-09-02

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. Todos los derechos reservados.



El logotipo de Java es una marca comercial o una marca comercial registrada de Sun Microsystems, Inc. en Estados Unidos u otros países.

© 2020 Cisco Systems, Inc. Todos los derechos reservados.



CONTENIDO

CAPÍTULO 1	Descripción general de Cisco Business Dashboard	1
	Acerca de Cisco Business Dashboard	1
	Público	2
	Documentos Relacionados	2
	Terminología	3
	Requisitos del sistema para Cisco Business Dashboard	4
	System Requirements for Cisco Business Dashboard Probe	5

CAPÍTULO 2	Uso de Cisco Business Dashboard y Probe	7
	Uso de la GUI de Cisco Business Dashboard	7
	Uso de la GUI de Cisco Business Dashboard Probe	10
	Actualización de Cisco Business Dashboard y Probe	13

CAPÍTULO 3	Panel de supervisión	15
	Acerca del panel de supervisión	15
	Agregar un widget	16
	Modificación de un widget	16
	Eliminación de un widget	16
	Modificación del diseño de Dashboard	16

CAPÍTULO 4	Red	19
	Acerca de Red	19
	Acerca de Network Detail (Detalles de la red)	21
	Acerca de la Vista de red	21
	Descripción general de las herramientas y el mapa Topología	22
	Visualización de la información básica del dispositivo	25

Acciones del dispositivo 27

Acceso a la interfaz de administración del dispositivo 29

Visualización de la información detallada del dispositivo 29

Uso de planos de plantas 32

CAPÍTULO 5 **Inventario 35**

Visualización del inventario de dispositivos 35

CAPÍTULO 6 **Administración de puertos 37**

Acerca de Administración de puertos 37

CAPÍTULO 7 **Configuración de red 39**

Acerca de Configuración de red 39

Uso del Asistente 39

Configuración de la administración del tiempo 40

Configuración de los Analizadores de DNS 41

Configuración de la autenticación 41

Configuración de LAN virtuales 42

Configuración de LAN inalámbricas 43

CAPÍTULO 8 **Plug and Play de red 45**

Acerca de Plug and Play de red 45

Requisitos de red 45

Configuración de la detección mediante Plug and Play Connect 47

Configuración del servicio Plug and Play de red 48

Supervisión de Plug and Play de red 55

CAPÍTULO 9 **Registro de eventos 57**

Acerca del registro de eventos 57

CAPÍTULO 10 **Informes 59**

Acerca de Informes 59

Visualización del Informe de ciclo de vida 59

Vista del informe de final de ciclo de vida útil 60

Visualización del informe de mantenimiento 62

Vista del informe de red inalámbrica 62

Vista del informe de clientes inalámbricos 65

CAPÍTULO 11

Administración 67

Acerca de Administración 67

Administración de las organizaciones 68

Administración de grupos de dispositivos 70

Administración de las credenciales del dispositivo 71

Cómo gestionar los usuarios 72

Cambio de los valores predeterminados de supervisión 75

Administración de los perfiles de supervisión 76

Visualización de los intentos de inicio de sesión 78

Administración de la configuración de los informes 78

CAPÍTULO 12

Sistema 79

Acerca de Sistema 79

Gestión de licencias 80

Gestión de certificados 82

Administración de la configuración del correo electrónico 84

Visualización del uso de la API 85

Copias de seguridad y restauración de la configuración de Dashboard 86

Administración de la configuración de la plataforma 86

Administración de la privacidad 89

Administración de la configuración de registro 91

Gestión de Probe local 93

CAPÍTULO 13

Notificaciones 95

Acerca de Notificaciones 95

Notificaciones admitidas 95

Visualización y filtrado de notificaciones actuales del dispositivo 97

Visualización y filtrado de notificaciones históricas del dispositivo 98

CAPÍTULO 14	Resolución de problemas	99
	Captura de la información de diagnóstico de red	99
	Administración de la configuración del registro de Probe	100

CAPÍTULO 15	Preguntas frecuentes	103
	Preguntas frecuentes generales	103
	Preguntas frecuentes sobre detección	103
	Preguntas frecuentes sobre configuración	104
	Preguntas frecuentes sobre consideraciones de seguridad	104
	Preguntas frecuentes sobre el acceso remoto	107
	Preguntas frecuentes sobre la actualización del software	108

CAPÍTULO 16	Apéndice A: Administración de plantillas de configuración	109
	Descripción general	109
	Sintaxis de configuración	109
	Creación de plantillas de configuración	112



CAPÍTULO 1

Descripción general de Cisco Business Dashboard

Este capítulo contiene las siguientes secciones:

- [Acerca de Cisco Business Dashboard](#) , en la página 1
- [Público](#), en la página 2
- [Documentos Relacionados](#), en la página 2
- [Terminología](#), en la página 3
- [Requisitos del sistema para Cisco Business Dashboard](#) , en la página 4
- [System Requirements for Cisco Business Dashboard Probe](#), en la página 5

Acerca de Cisco Business Dashboard

Cisco Business Dashboard proporciona herramientas que le ayudan a supervisar y administrar su red de las series de Cisco Business. Cisco Business Dashboard detecta automáticamente la red y permite configurar y controlar todos los dispositivos compatibles de Cisco Business, como, por ejemplo, puntos de acceso inalámbricos, routers y conmutadores. También notifica sobre la disponibilidad de las actualizaciones del firmware e informa sobre dispositivos que ya no están en garantía o bajo un contrato de soporte.

Cisco Business Dashboard es una aplicación distribuida que se compone de dos componentes o aplicaciones independientes: la aplicación principal Cisco Business Dashboard, también conocida como *Dashboard* y una o más instancias de Cisco Business Dashboard Probe, también conocido como *Probe*.

Se instala una única instancia de Cisco Business Dashboard en una ubicación adecuada de la red. Desde la interfaz de usuario de Dashboard, puede obtener una vista de alto nivel del estado de todos los sitios de la red o centrarse en un solo sitio o dispositivo para ver información específica al respecto.

Una instancia de Cisco Business Dashboard Probe se instala en cada sitio de la red y se asocia con Dashboard. La sonda realiza exploraciones de la red y se comunica directamente con cada dispositivo administrado en nombre de Dashboard.

Ciertos dispositivos de red admiten que se asocien directamente con Dashboard y que se manejen sin la presencia de una sonda. Cuando los dispositivos de red se administran directamente de esta manera, todas las funciones de administración están disponibles para el dispositivo, pero puede que el proceso de descubrimiento de la red no sea tan exhaustivo que cuando hay una sonda presente.

Público

Esta guía está destinada principalmente a administradores de red responsables de la administración e instalación del software Cisco Business Dashboard.

Documentos Relacionados

La documentación de Cisco Business Dashboard se compone de varias guías independientes. Estos son algunos de ellos:

- **Guía de administración (este documento):** en esta guía de referencia, se proporciona información sobre todas las funciones y opciones del software, así como la forma de configurarlas y utilizarlas.
- **Lista de compatibilidad de dispositivos:** esta lista proporciona información de los dispositivos admitidos por Cisco Business Dashboard y las funciones disponibles para cada tipo de dispositivo. Para obtener una lista de todos los dispositivos que Cisco Business Dashboard admite, consulte [Cisco Business Dashboard: lista de dispositivos admitidos](#).
- **Guía de inicio rápido:** facilita detalles sobre cómo realizar la configuración inicial de Cisco Business Dashboard mediante las opciones más usadas. Para conocer una descripción general de las tareas básicas necesarias para administrar una red, consulte la [guía de inicio rápido de Cisco Business Dashboard y Probe](#).
- **Guías de instalación**

En la siguiente tabla, se muestran todas las guías de instalación del software Cisco Business Dashboard , que puede implementarse en diferentes plataformas. Consulte la ruta facilitada en la columna de ubicación para obtener más detalles:

Plataformas admitidas	Ubicación
Amazon Web Services	Guía de instalación de Cisco Business Dashboard para Amazon Web Services
Oracle VirtualBox	Guía de instalación de Cisco Business Dashboard para Oracle VirtualBox
Microsoft Hyper-V	Guía de instalación de Cisco Business Dashboard para Microsoft Hyper-V
VMware vSphere, Workstation y Fusion	Guía de instalación de Cisco Business Dashboard para VMWare
Ubuntu Linux (Dashboard y Probe) y Raspbian Linux (solo Probe)	Guía de instalación de Cisco Business Dashboard para Linux

Terminología

Plazo	Descripción
□Hyper-V	Plataforma de virtualización proporcionada por Microsoft Corporation.
Archivo OVF (Open Virtualization Format)	Archivo TAR que contiene una o varias máquinas virtuales en formato OVF. Es un método independiente de la plataforma que permite empaquetar y distribuir máquinas virtuales (VM).
Archivo OVA (Open Virtual Appliance or Application)	Paquete que contiene los siguientes archivos usados para describir una máquina virtual. Se guarda como un único archivo con empaquetado .TAR: <ul style="list-style-type: none"> • Archivo descriptor (.OVF) • Archivos opcionales de certificado y de manifiesto (.MF).
Raspberry Pi	Un ordenador de placa única y muy bajo coste desarrollado por la Raspberry Pi Foundation. Para obtener más información, consulte https://www.raspberrypi.org/ .
Raspbian	Una distribución de Linux basada en Debian y optimizada para Raspberry Pi. Para obtener más información, consulte https://www.raspbian.org/ .
VirtualBox	Plataforma de virtualización proporcionada por Oracle Corporation.
Disco duro virtual (VHD)	Un disco duro virtual es un formato de archivo de imagen de disco donde se puede almacenar todo el contenido de un disco duro.
Máquina virtual (VM)	Entorno informático virtual en el que se puede ejecutar un sistema operativo invitado y el software de las aplicaciones asociadas. Se pueden operar varias máquinas virtuales en el mismo sistema host de forma simultánea.
<ul style="list-style-type: none"> • VMware ESXi • VMware Fusion • vSphere Server • VMware Workstation 	Plataforma de virtualización proporcionada por VMware Inc.
vSphere Client	Interfaz de usuario que permite a los usuarios conectarse de forma remota a vCenter Server o ESXi desde cualquier PC Windows. La interfaz principal de vSphere Client se puede usar para crear, administrar y supervisar las máquinas virtuales, sus recursos y los hosts. También proporciona acceso de consola a las máquinas virtuales.

Requisitos del sistema para Cisco Business Dashboard

Cisco Business Dashboard se distribuye como una imagen de máquina virtual, como un instalador para su uso con la distribución de Ubuntu Linux y, además, está disponible para Amazon Web Services (AWS) a través de AWS Marketplace (<https://aws.amazon.com/marketplace>).

Si ejecuta Cisco Business Dashboard en una máquina virtual, el hipervisor debe ser uno de los siguientes:

- Microsoft Hyper-V versión 10.0 o superior
- Oracle VirtualBox versión 6.1 o superior
- VMWare
 - ESXi versión 6.0 o superior
 - Fusion versión 11.5 o superior
 - Workstation versión 15.1 o superior

Para ejecutar Cisco Business Dashboard en Ubuntu Linux, el entorno debe contar con la versión 16.04.x (Xenial Xerus) de Ubuntu en una plataforma de arquitectura Intel de 64 bits. Cisco recomienda usar la distribución del servidor de Ubuntu y solo instalar los Cisco Business Dashboardpaquetes requeridos por.

En la tabla 1, se muestran los recursos informáticos necesarios para Cisco Business Dashboard según el número de dispositivos administrados.

Tabla 1: Cisco Business Dashboard Requisitos de recursos informáticos

N.º de dispositivos compatibles	N.º de vCPU	RAM	Espacio en disco
Hasta 300	2	4 GB	60 GB
Hasta 2500	12	24 GB	60 GB

Para ejecutar Cisco Business Dashboard en AWS, necesitará una cuenta de AWS. Se admiten los siguientes tipos de instancias de AWS:

- c5.large: hasta 300 dispositivos gestionados
- c5.4xlarge: hasta 2500 dispositivos gestionados

Cisco Business Dashboard se administra mediante una interfaz de usuario web. Para usar esta interfaz, el navegador debe ser uno de los siguientes:

- Apple Safari (solo macOS): las 2 principales versiones más recientes
- Google Chrome: última versión
- Microsoft Edge: las 2 principales versiones más recientes
- Mozilla Firefox: última versión



Nota Cuando use Safari, compruebe que el certificado de Cisco Business Dashboard Probe esté configurado como **Confiar siempre**. De lo contrario, se producirán fallos en determinadas funciones que dependen del uso de sockets web seguros. Se trata de una limitación del navegador web Safari.

La red debe permitir que todas las instancias de Cisco Business Dashboard Probe puedan establecer la conectividad TCP con Cisco Business Dashboard. Para obtener más detalles sobre los puertos y los protocolos usados, consulte la sección de [Preguntas frecuentes](#).

System Requirements for Cisco Business Dashboard Probe

Cisco Business Dashboard Probe se distribuye como una imagen de máquina virtual y como instaladores para su uso con los siguientes sistemas operativos:

- Distribución de Ubuntu Linux que se ejecuta en un PC
- Distribución de Raspbian Linux que se ejecuta en Raspberry Pi

Cisco Business Dashboard Probe también está disponible como una función integrada de determinados productos de las series 100 a 500 de Cisco.

Para ejecutar Cisco Business Dashboard Probe como máquina virtual, su entorno debe cumplir los siguientes requisitos:

- Hipervisor:
 - Microsoft Hyper-V versión 10.0 o superior
 - Oracle VirtualBox versión 6.1 o superior
 - VMWare
 - ESXi versión 6.0 o superior
 - Fusion versión 11.5 o superior
 - Workstation versión 15.1 o superior
- Requisitos de recursos de la máquina virtual:
 - CPU: arquitectura Intel 1x 64 bits
 - Memoria: 512 MB
 - Espacio en disco: 5 GB

Para ejecutar Cisco Business Dashboard en el sistema operativo Ubuntu Linux, su entorno debe cumplir los siguientes requisitos:

- Ubuntu versión 16.04.x (Xenial Xerus)
- CPU: arquitectura Intel 1x 64 bits
- Memoria: 512 MB

- Espacio en disco: 5 GB

Para ejecutar Cisco Business Dashboard Probe en un sistema operativo Raspberry Pi, su entorno debe cumplir los siguientes requisitos:

- Hardware: Raspberry Pi 3 modelo B/B+ o Raspberry Pi 4 modelo B
- Espacio en disco: 5 GB
- SO: Raspbian Buster

Para ejecutar Cisco Business Dashboard Probe como una aplicación integrada en un producto de Cisco Business, debe disponer de un producto compatible con una versión de firmware que admita la función de Cisco Business Dashboard Probe. Consulte la [lista de dispositivos compatibles de Cisco Business Dashboard](#) para obtener información sobre los requisitos de hardware y versiones. Asimismo, consulte la guía de administración del producto para determinar los requisitos adicionales específicos de la plataforma en cuestión.

Cisco Business Dashboard Probe se administra mediante una interfaz de usuario web. Para usar esta interfaz, el navegador debe ser uno de los siguientes:

- Apple Safari (solo macOS): las 2 principales versiones más recientes
- Google Chrome: última versión
- Microsoft Edge: las 2 principales versiones más recientes
- Mozilla Firefox: última versión

Cisco Business Dashboard Probe supervisa los dispositivos de red que cumplen los siguientes requisitos, además de acceder a ellos:

- Deben estar en la misma subred que el PC que está ejecutando Cisco Business Dashboard Probe. También pueden estar directamente conectados a un dispositivo administrado al que se pueda acceder a través de TCP/IP.
- Debe ser un dispositivo compatible de las series 100 a 500 de Cisco Business o Cisco Small Business



CAPÍTULO 2

Uso de Cisco Business Dashboard y Probe

Este capítulo contiene las siguientes secciones:

- [Uso de la GUI de Cisco Business Dashboard, en la página 7](#)
- [Uso de la GUI de Cisco Business Dashboard Probe, en la página 10](#)
- [Actualización de Cisco Business Dashboard y Probe, en la página 13](#)

Uso de la GUI de Cisco Business Dashboard

Descripción general de la GUI de Cisco Business Dashboard con descripción de los enlaces del panel de navegación.

Ventana Inicio

Figura 1: Página de inicio de Cisco Business Dashboard

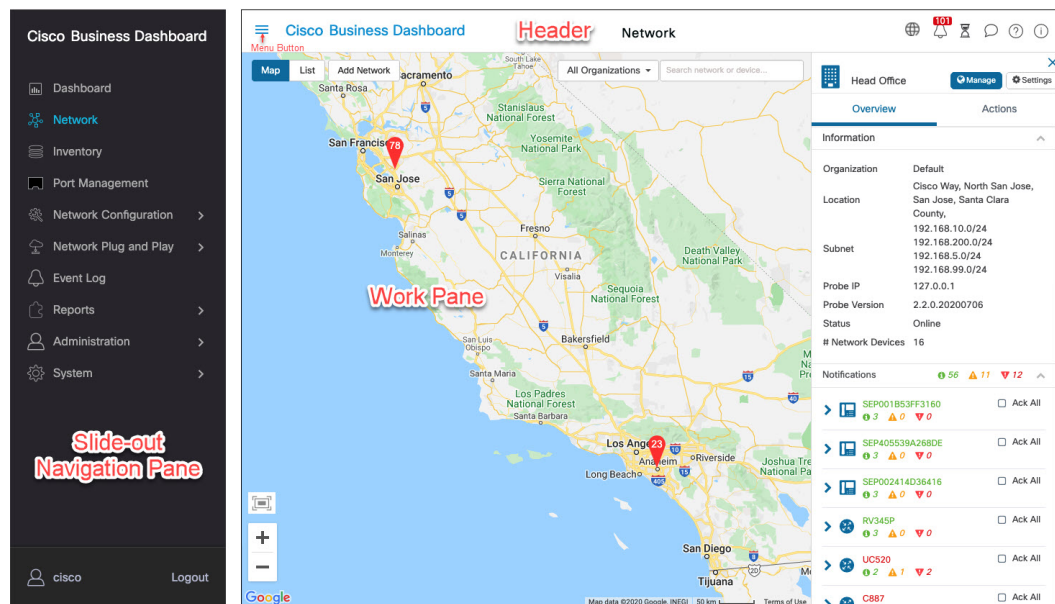






Tabla 2: Página de inicio de Cisco Business Dashboard








Nombre	Descripción
Panel Navegación	Proporciona acceso a las funciones de Cisco Business Dashboard. El panel de navegación se muestra cuando se hace clic en el icono Menú y desaparece cuando se realiza una selección. El usuario que ha iniciado sesión se muestra en la parte inferior del panel de navegación.
Panel Trabajo	Área en la que se presenta la interfaz de funciones Al hacer clic en una opción del panel Navegación , se abre la ventana correspondiente en esta área.
Barra de herramientas Encabezado	La barra de herramientas Encabezado incluye las siguientes opciones: <ul style="list-style-type: none"> • Un botón de menú para mostrar el panel de navegación • Texto del encabezado. • Una serie de iconos para funciones tales como selección de idioma, notificaciones, actividad de las tareas, comentarios, ayuda sensible al contexto e información de la versión.

Opciones del panel Navegación

El panel **Navegación** ofrece opciones para acceder a las funciones principales de Cisco Business Dashboard

Tabla 3: Opciones del panel Navegación



Icono	Nombre	Descripción
	Panel	El Dashboard permite supervisar el rendimiento de la red a lo largo del tiempo. El panel de control permite controlar los niveles de tráfico, los recuentos de dispositivos conectados y otros detalles sobre la red.
	Red	Muestra una descripción general de todas las ubicaciones de la red en forma de mapa o de lista. Contiene distintas vistas de cada red y los dispositivos detectados. En las vistas, se muestra la topología de la red y un plano que permite controlar el diseño físico de la red.
	Inventario	La opción Inventario ofrece una lista de todos los dispositivos de la red y permite ver información detallada sobre los dispositivos y realizar acciones tales como actualizar el firmware, hacer copias de seguridad de las configuraciones y reiniciar.
	Administración de puertos	Administración de puertos ofrece una vista de panel frontal sobre los dispositivos de red, muestra información detallada sobre cada puerto y permite realizar cambios de configuración.






Icono	Nombre	Descripción
	Configuración de red	La página Configuración de red permite administrar los perfiles de configuración de su red.
	Plug and Play de red	Plug and Play de red habilita la implementación sin intervención del usuario de los dispositivos de red y permite que estos descarguen automáticamente archivos de configuración y de firmware de Cisco Business Dashboard en el momento de la instalación.
	Registro de eventos	La página Registro de eventos ofrece una lista de todos los eventos que han tenido lugar en la red y permite usar filtros para limitar los resultados únicamente a aquellos eventos que resulten de interés.
	Informes	Bajo el encabezado Informes, encontrará una serie de informes que ofrecen información sobre el ciclo de vida de los dispositivos de red, incluidos boletines de final de vida útil, datos sobre la garantía y detalles del contrato de servicios.
	Administración	Las páginas Administración permiten llevar a cabo el mantenimiento de Cisco Business Dashboard.
	Sistema	Las páginas de Sistema se emplean para administrar la aplicación de Cisco Business Dashboard.
	Opciones de usuario	El usuario que ha iniciado sesión se muestra en la parte inferior de la barra de navegación con una opción Cerrar sesión . Haga clic en el nombre de usuario para mostrar la página de perfil del usuario.

Opciones de la barra de herramientas Encabezado

La barra de herramientas **Encabezado** proporciona acceso a otras funciones y muestra notificaciones del sistema.

Tabla 4: Opciones de la barra de herramientas Encabezado

Icono	Opción	Descripción
	Botón de menú	Se encuentra en la parte superior izquierda del encabezado: al hacer clic en este botón se muestra el panel de navegación.
	Selección de idioma	Esta lista desplegable permite seleccionar el idioma de la interfaz de usuario.

Icono	Opción	Descripción
	Centro de notificaciones	Este icono muestra el número y la gravedad de las notificaciones pendientes en Cisco Business Dashboard. Haga clic en este icono para abrir el panel Notificación. En este panel, encontrará funciones para filtrar los eventos de notificación. Para obtener más información, consulte Visualización y filtrado de notificaciones actuales del dispositivo, en la página 97 en esta guía.
	Centro de trabajo	Muestra el estado de los trabajos en ejecución y el historial de trabajos pasados. Los trabajos incluyen cualquier acción realizada por Cisco Business Dashboard, incluidos los trabajos iniciados por el usuario y los trabajos del sistema. Haga clic en este icono para ver los trabajos que están pendientes, en curso y finalizados.
	Comentarios	Haga clic en esta opción para proporcionar comentarios sobre su experiencia con Cisco Business Dashboard y remitirnos cualquier sugerencia de mejora.
	Ayuda	Muestra documentación y ayuda en línea sobre Cisco Business Dashboard.
	Cisco Business Dashboard	Haga clic en este icono para ver información sobre Cisco Business Dashboard, incluida la versión actual. Si hay una nueva versión disponible, se mostrará un distintivo en el icono y un enlace en la ventana emergente para aplicar la actualización.

Uso de la GUI de Cisco Business Dashboard Probe

Una vez que haya iniciado la sesión en Cisco Business Dashboard Probe, aparecerá la página **Inicio**.

Figura 2: Página de inicio de Cisco Business Dashboard

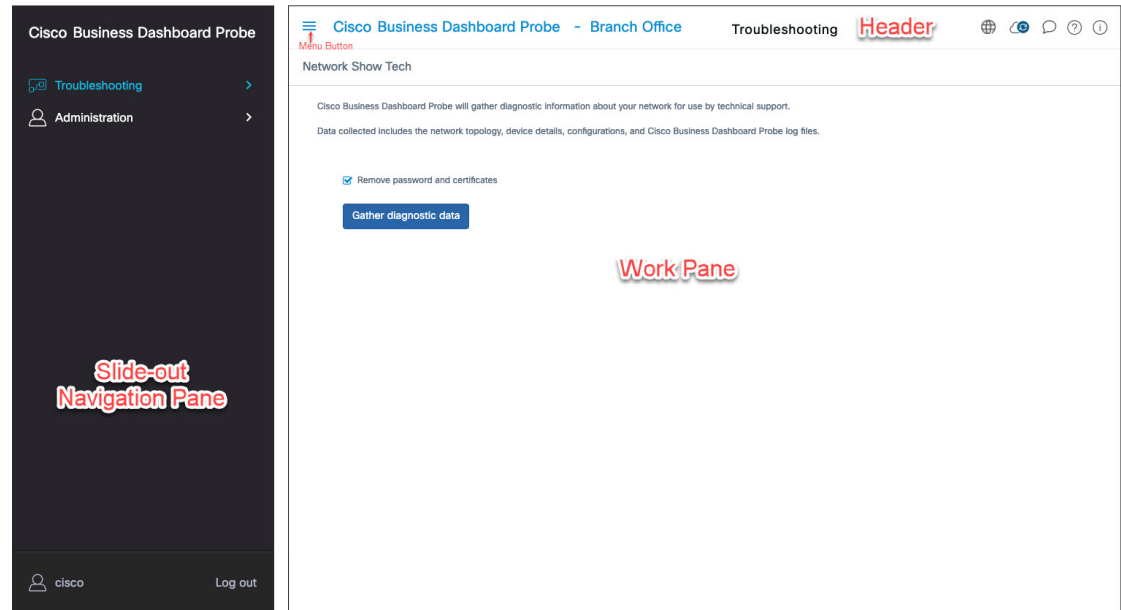





Tabla 5: Página de inicio de Cisco Business Dashboard

Nombre	Descripción
Panel Navegación	Proporciona acceso a las funciones de Cisco Business Dashboard Probe. El panel de navegación se muestra cuando se hace clic en el botón Menú y desaparece cuando se realiza una selección. El usuario que ha iniciado sesión se muestra en la parte inferior del panel de navegación.
Panel Trabajo	Área en la que se presenta la interfaz de funciones Al hacer clic en una opción del panel Navegación , se abre la ventana correspondiente en esta área.
Barra Encabezado	La barra de herramientas Encabezado incluye las siguientes opciones: <ul style="list-style-type: none"> • Un botón de menú para mostrar el panel de navegación • Texto del encabezado con el nombre de sitio de Probe. • Lista desplegable para seleccionar el idioma. • Una serie de iconos para funciones como notificaciones, comentarios y ayuda sensible al contexto

Opciones del panel Navegación

El panel **Navegación** ofrece opciones para acceder a las funciones principales de Cisco Business Dashboard Probe.







Tabla 6: Opciones del panel Navegación

Icono	Nombre	Descripción
	Resolución de problemas	En la sección Resolución de problemas , encontrará herramientas de diagnóstico que permiten identificar problemas con la red.
	Administración	La página Administración permite llevar a cabo el mantenimiento de las aplicaciones de red de Cisco Business Dashboard Probe.
	Opciones de usuario	El usuario que ha iniciado sesión se muestra en la parte inferior de la barra de navegación con una opción Cerrar sesión . Haga clic en el nombre de usuario para mostrar la página de perfil del usuario.

Opciones de la barra Encabezado

La barra **Encabezado** proporciona acceso a otras funciones y muestra notificaciones del sistema.

Tabla 7: Opciones de la barra Encabezado

Icono	Opción	Descripción
	Botón de menú	Se encuentra en la parte superior izquierda del encabezado: al hacer clic en este botón se muestra el panel de navegación.
	Selección de idioma	Esta lista desplegable permite seleccionar el idioma de la interfaz de usuario.
	Paneles de Dashboard	Muestra el estado de la conexión entre Cisco Business Dashboard y Probe. Haga clic en este icono para abrir la GUI de Dashboard.
	Comentarios	Haga clic en esta opción para proporcionar comentarios sobre su experiencia con Cisco Business Dashboard Probe y remitirnos cualquier sugerencia de mejora.
	Ayuda	Muestra documentación y ayuda en línea sobre Cisco Business Dashboard Probe.
	Acerca de Cisco Business Dashboard y Probe	Haga clic en este icono para ver información sobre Cisco Business Dashboard Probe, incluida la versión actual. Si hay una nueva versión disponible, se mostrará un distintivo en el icono y un enlace en la ventana emergente para aplicar la actualización.

Actualización de Cisco Business Dashboard y Probe

Cada cierto tiempo, Cisco lanza nuevas versiones y actualizaciones para Cisco Business Dashboard y Probe y las publica en el centro de software en cisco.com. Cisco Business Dashboard comprueba periódicamente el centro de software en busca de actualizaciones y, si encuentra una, muestra una señal en **Acerca de Cisco Business Dashboard**, en el panel de encabezado de la interfaz de usuario. Puede hacer clic para que Dashboard descargue y aplique la actualización o puede descargarla por su cuenta y aplicarla manualmente.

Para que Dashboard descargue y aplique la actualización, haga lo siguiente:

1. Haga clic en **Acerca de Cisco Business Dashboard** para abrir la ventana emergente **Acerca de Cisco Business Dashboard**. Si hay actualizaciones disponibles para Dashboard o Probes asociados, se enumerarán aquí.
2. Si hay disponible una actualización para Manager, seleccione el botón de opción correspondiente a dicha actualización y haga clic en **Actualizar**.

Manager descargará y aplicará la actualización; podrá ver el progreso en cualquier momento en la ventana emergente **Acerca de Cisco Business Dashboard**. Una vez finalizada la actualización, la aplicación de Dashboard se reiniciará.

Para aplicar manualmente una actualización de Dashboard, haga lo siguiente:

1. Descargue el archivo de instalación de Linux Cisco Business Dashboard en <https://cisco.com/go/cbd-sw> y seleccione la opción **Descargar software** en el panel de selección de productos en la parte inferior derecha.
2. Copie el archivo instalador al sistema de archivos de Dashboard.
3. Ejecute el instalador mediante el comando `sh <nombre de archivo del instalador>`. Por ejemplo, `sh cisco-business-dashboard-2.2-ubuntu-xenial-amd64.sh`. Si es necesario, introduzca su contraseña en la solicitud de `sudo`. La aplicación de Dashboard se reiniciará durante este proceso.

También puede aplicar actualizaciones a todos los Probes en la red de Dashboard. Puede actualizar todos los Probes de forma paralela o individualmente.

Para actualizar todos los Probes de forma paralela desde Dashboard, haga lo siguiente:

1. Haga clic en **Acerca de Cisco Business Dashboard** para abrir la ventana emergente **Acerca de Cisco Business Dashboard**. Si hay actualizaciones disponibles para Dashboard o cualquiera de las Probes asociadas, se enumerarán aquí.
2. Si hay disponible una actualización para Dashboard, ejecute la actualización antes de actualizar los Probes. Si trata de actualizar primero los Probe, recibirá un mensaje de error.
3. Seleccione el botón de opción junto a la actualización de Probe y haga clic en **Actualizar**.
4. Puede ver el progreso de la actualización en la interfaz de usuario de Probe.

Para actualizar un Dashboard de forma individual desde Manager, haga lo siguiente:

1. Si hay disponible una actualización para Dashboard, ejecute la actualización antes de actualizar cualquier sonda. Si trata de actualizar una sonda antes de actualizar Dashboard, recibirá un mensaje de error.

2. Seleccione **Red** en la navegación. Seleccione la red que se debe actualizar en la **Vista de mapa** o la **Vista de lista**.
3. En el panel **Información básica** de la red, seleccione la pestaña de **Acciones**.
4. Haga clic en **Actualizar**.

Puede ver el progreso de la actualización en el centro de trabajo.



Nota

Si utiliza una aplicación de Probe integrada en un dispositivo de red, debe consultar la documentación de ese dispositivo para realizar una actualización. Algunos dispositivos no admiten la actualización de la aplicación de Probe independientemente del firmware que tengan.



CAPÍTULO 3

Panel de supervisión

Este capítulo contiene las siguientes secciones:

- [Acerca del panel de supervisión, en la página 15](#)
- [Agregar un widget, en la página 16](#)
- [Modificación de un widget, en la página 16](#)
- [Eliminación de un widget, en la página 16](#)
- [Modificación del diseño de Dashboard, en la página 16](#)

Acerca del panel de supervisión

La página **Dashboard** de Cisco Business Dashboard permite ver en tiempo real el rendimiento de la red y sus dispositivos. Además, muestra los datos en un formato gráfico. Este panel de supervisión está formado por los widgets que seleccione el usuario. A continuación, se muestran los widgets incluidos en el panel de control de forma predeterminada:

- **Resumen del inventario:** este widget muestra un desglose de los dispositivos detectados en la red.
- **Estado del dispositivo:** este widget muestra el estado general de los dispositivos de la red.
- **Recuento de clientes de WLAN:** este widget muestra el número de dispositivos asociados con la red inalámbrica seleccionada.
- **Recuento de clientes del dispositivo:** este widget muestra el número de dispositivos asociados con el punto de acceso inalámbrico seleccionado.
- **Los diez inalámbricos más destacados:** este widget muestra las diez redes inalámbricas, los puntos de acceso o los clientes más destacados en función del tráfico o el recuento de clientes.
- **Tráfico:** este widget muestra un gráfico con el tráfico que pasa por la interfaz seleccionada.

Los controles de cada uno de los widgets permiten personalizar los datos mostrados. El menú desplegable de organizaciones, en la parte superior derecha de **Dashboard**, puede usarse para restringir a una organización concreta la información que aparece.

En los widgets gráficos, puede hacer clic en las etiquetas de la leyenda del gráfico para cambiar la visualización de cada conjunto de datos. Esto le permite ajustar aún más los datos visualizados.

Agregar un widget

Esta función permite agregar uno o varios widgets a los widgets existentes predeterminados que aparecen en el panel de control para supervisar las tareas específicas de un dispositivo o red que desee ver.

-
- Paso 1** Haga clic en el icono del engranaje situado en la parte superior derecha de la ventana del panel y seleccione **Añadir widget**.
 - Paso 2** En la lista desplegable, seleccione el tipo de widget que quiere agregar. El nuevo widget elegido aparecerá en el panel.
 - Paso 3** Arrastre el nuevo widget a la ubicación que desee del panel y cámbiele el tamaño si es necesario.
 - Paso 4** Vuelva a hacer clic en el icono del engranaje y seleccione **Modo de vista** para conservar los cambios.
-

Modificación de un widget

-
- Paso 1** Utilice las listas desplegables del nuevo widget para seleccionar los datos específicos que desea mostrar.
 - Paso 2** Haga clic en el icono del engranaje, en la parte superior derecha del widget, para modificar parámetros tales como el intervalo de ejemplos o los umbrales. También puede hacer clic en el icono Editar que aparece en el widget cuando el panel esté en **Modo de edición** para cambiar el título del widget.
-

Eliminación de un widget

-
- Paso 1** Haga clic en el icono del engranaje situado en la parte superior derecha de la ventana del panel y seleccione **Modo de edición**.
 - Paso 2** Haga clic en el icono **Eliminar widget**, situado en la esquina superior derecha del widget que se va a eliminar. Reorganice los demás widgets como desee.
 - Paso 3** Vuelva a hacer clic en el icono del engranaje y seleccione **Modo de vista** para conservar los cambios.
-

Modificación del diseño de Dashboard

El diseño de **Dashbaord** se puede personalizar fácilmente siguiendo estos pasos:

-
- Paso 1** Haga clic en el icono del engranaje situado en la parte superior derecha de la ventana del panel y seleccione **Modo de edición**.
 - Paso 2** Haga clic en el encabezado de un widget y arrástrelo para moverlo en **Dashboard**. Los demás widgets se ajustarán dinámicamente para dejar espacio. Haga clic en el borde o la esquina de un widget y arrástrelo para cambiarle el tamaño. A medida que reorganice el diseño, el panel cambiará dinámicamente de tamaño para ajustarse al ancho disponible.

Paso 3 Vuelva a hacer clic en el icono del engranaje y seleccione **Modo de vista** para conservar los cambios.



CAPÍTULO 4

Red

Este capítulo contiene las siguientes secciones:

- [Acerca de Red](#), en la página 19
- [Acerca de Network Detail \(Detalles de la red\)](#), en la página 21
- [Acerca de la Vista de red](#), en la página 21
- [Descripción general de las herramientas y el mapa Topología](#), en la página 22
- [Visualización de la información básica del dispositivo](#), en la página 25
- [Acciones del dispositivo](#), en la página 27
- [Acceso a la interfaz de administración del dispositivo](#), en la página 29
- [Visualización de la información detallada del dispositivo](#), en la página 29
- [Uso de planos de plantas](#), en la página 32

Acerca de Red

La página **Red** proporciona una descripción general de la red, bien en forma de mapa geográfico —con la ubicación y el estado de cada sitio en la red—, o bien como una lista de todos los sitios. En **Vista de mapa**, el número que aparece en cada icono de una red indica el número de notificaciones pendientes que existen para ese sitio. El color del icono señala el nivel de gravedad más alto pendiente. En **Vista de lista**, puede verse la misma información en la última columna de la tabla. Para obtener más información sobre una red, haga clic en el icono de la red o en la fila de la tabla de ese sitio.

Cuando dos o más iconos de red se colocan demasiado cerca en el mapa para distinguirse fácilmente, se reemplazarán por un único icono de clúster. Al hacer clic en el icono de clúster, se ampliará automáticamente el mapa a un nivel en el que puedan separarse las redes de ese clúster.

El **Mapa de red** ofrece los siguientes controles:

- Selección **Mapa/Lista**: use este control para ver las redes en un mapa o una tabla.
- Botón **Añadir red**: utilice este botón para crear un nuevo registro de red antes de implementar Probe para esa red.
- Menú desplegable **Organización**: seleccione una organización concreta del menú desplegable para limitar las redes que se muestran.
- Cuadro **Buscar**: introduzca el nombre o parte de este, la dirección o la dirección IP de una red para localizarla en el mapa. También puede introducir el nombre o parte de este, la dirección IP, el número de serie o la dirección MAC de un dispositivo para identificar la red donde está ubicado. A medida que

escriba, se mostrará una lista de resultados coincidentes. Pase el cursor por encima de una coincidencia y la red correspondiente se resaltará. Seleccione una coincidencia y la red correspondiente se seleccionará y se centrará en la vista.

- Controles de **Zoom**: use estos controles para acercar y alejar el mapa. Haga clic en el signo **+** (más) para acercar y en el signo **-** (menos) para alejar.
- Botón **Fit-to-view** (Ajustar vista): este botón aleja automáticamente el mapa para que se puedan mostrar todos los marcadores de red.

También puede hacer clic y arrastrar hasta cualquier lugar del área del mapa para mover el mapa al panel **Trabajo**.

En la **Vista de lista**, están disponibles los siguientes controles:

- Selección **Mapa/Lista**: use este control para ver las redes en un mapa o una tabla.
- Icono **Column Select** (Selección de columnas): este icono le permite seleccionar las columnas que se van a mostrar. Puede hacer clic en los encabezados de las columnas para ordenar la tabla.
- **Añadir red**: haga clic en el signo más (**+**) para añadir una nueva red antes de implementar Probe para esa red.
- **Actualizar**: haga clic en el botón Actualizar para actualizar la tabla y mostrar la información más reciente.
- Menú desplegable **Organización**: seleccione una organización concreta del menú desplegable para limitar las redes que se muestran.
- Cuadro **Buscar**: introduzca el nombre o parte de este, la dirección o la dirección IP de una red para mostrar únicamente las redes correspondientes en la tabla.

Al hacer clic en el icono o en la fila de una red, aparecerá el panel **Información básica** de la red en cuestión. El panel **Información básica** contiene la siguiente información:

- Nombre de la red
- La organización a la que pertenece la red
- La dirección física de la red
- La dirección IP de Probe para esta red y las subredes IP detectadas en ella
- La versión de software de Probe
- Estado de la conexión
- La cantidad de dispositivos gestionados de esta red
- Una lista de todas las notificaciones actuales de la red no reconocidas
- Una lista de eventos ocurridos en relación con esta red en las 24 horas previas

Desde el panel **Información básica** también puede realizar las siguientes acciones para una red:

- Haga clic en **Administrar** para ver información detallada sobre la red, incluida la topología de red y los planos de planta.

- Haga clic en **Configuración** para mostrar el panel **Network Detail** (Detalles de la red). Consulte [Acerca de Network Detail \(Detalles de la red\)](#), en la página 21 para obtener más información sobre el panel **Network Detail** (Detalles de la red).
- Haga clic en la pestaña **Acciones** para mostrar acciones adicionales disponibles para la red.
 - Haga clic en **Eliminar** para eliminar esta red y todos los datos asociados del panel.
 - Haga clic en **Actualizar** para actualizar el software de Probe en esta red.
 - Haga clic en **Mostrar información técnica** para generar un archivo de Mostrar información técnica de la red para esta red.

Acerca de Network Detail (Detalles de la red)

El panel **Network Detail** (Detalles de la red) permite ver y actualizar información específica de esa red. Esta información incluye lo siguiente:

- Parámetros clave de la red, como su nombre, la descripción, la organización y el grupo de dispositivos predeterminado.
- La ubicación de la red.
- Las credenciales que se van a utilizar para la red al cargar información del inventario en Cisco Active Advisor.
- Configuración de los registros de Probe en esta red. Consulte [Administración de la configuración del registro de Probe](#), en la página 100 para obtener más información sobre la configuración de los registros de Probe.

Acerca de la Vista de red

Haga clic en **Administrar** en el panel **Información básica** de la red para mostrar la **Vista de red** de esa red. La **Vista de red** ofrece varias vistas de la red:

- **Topología**: esta vista muestra una topología lógica de todos los dispositivos detectados en la red. Se muestra información sobre cada dispositivo y se pueden realizar acciones en los productos de Cisco seleccionados.
- **Plano de planta**: esta vista permite documentar la ubicación física de los dispositivos de red en su entorno.

A continuación, se indican los controles adicionales que están disponibles en común para todas las tareas que se realizan en **Vista de red**:

- Selección **Organization and Network** (Organización y red): estos menús desplegables permiten cambiar de red y organización sin necesidad de volver a la página principal de las redes. Para ver la topología o el plano de planta de una red diferente, basta con seleccionar esa red mediante el menú desplegable.
- **Acciones de red**: este menú desplegable permite realizar determinadas acciones en todos los dispositivos de la red que admiten esta acción. Por ejemplo, se puede hacer una copia de seguridad de todas las configuraciones del dispositivo con un solo clic. El menú desplegable **Acciones de red** también permite

reiniciar el proceso de detección de la red y cargar el inventario en Cisco Active Advisor mediante <https://www.ciscoactiveadvisor.com>. Para obtener más información sobre Cisco Active Advisor, consulte <https://help.ciscoactiveadvisor.com>.

Descripción general de las herramientas y el mapa Topología

Acerca del mapa Topología

Cisco Business Dashboard solicita información a los dispositivos detectados sobre la conectividad de la red y crea una representación gráfica o topología a partir de la información que ha recopilado. Entre los datos recopilados, podemos destacar información sobre los vecinos de protocolo de detección de capa de enlace (LLDP) y de protocolo de detección de Cisco (CDP), las tablas de direcciones MAC y las tablas de dispositivos asociados de los puntos de acceso inalámbricos, los routers y los conmutadores de las series Cisco Business. Esta información se utiliza para determinar cómo está construida la red. Cuando la red contiene dispositivos de infraestructura de red que no se pueden gestionar por alguna razón, Cisco Business Dashboard intentarán deducir la topología basándose en la información que se pueda recopilar.

Puede hacer clic en los dispositivos o enlaces en la topología para mostrar el panel **Información básica** del enlace o dispositivo. El panel **Información básica** ofrece información más detallada sobre el dispositivo o el enlace y permite llevar a cabo diferentes acciones en el dispositivo.

Al hacer clic en **Superposiciones**, en el mapa **Topología**, se muestra el panel **Superposiciones y filtros**. Este panel permite limitar los dispositivos que se muestran en la topología por tipo de dispositivo o por etiqueta. También permite mejorar la topología para mostrar información adicional como, por ejemplo, la carga de tráfico del enlace o cómo está configurada una VLAN concreta en la red.



Acceso al mapa Topología







Para acceder al mapa **Topología**, seleccione primero **Red** en **Navegación**, haga clic en el icono o la fila de tabla de la red que le interesa y, a continuación, haga clic en **Ver**. En el panel de trabajo, aparecerá el mapa **Topología** de esa red.

Controles de topología

Los controles de topología se encuentran en la parte superior izquierda del mapa **Topología**.

Tabla 8: Controles de topología





Icono	Nombre del icono	Descripción
	Acercar	Permite ajustar la vista de la ventana Topología . Haga clic en el icono + (más) de la barra de menús para aumentar el tamaño de la red en el área de visualización.
	Alejar	Permite ajustar la vista de la ventana Topología . Haga clic en el icono - (menos) para reducir el tamaño de la red en el área de visualización.




Icono	Nombre del icono	Descripción
	Volver a ajustar el diseño de la topología	Volver a habilitar el diseño automático de la topología después de se haya deshabilitado por cambios manuales. Rediseña la topología mediante el algoritmo de diseño automático.
	Acercar selección	Haga clic y arrastre para seleccionar un área a la que aplicar el zoom.
	Ajustar fase	Aplica el zoom hasta que la red entera encaje en el área de visualización.
	Acceder al modo de pantalla completa	Ocupa toda la pantalla con la interfaz de usuario de Cisco Business Dashboard.
	Exportar topología	Exportar la vista de topología actual como imagen en formato PNG. La imagen se guardará en la ubicación de descarga predeterminada del navegador.
	Ajustes de topología	Ajuste las etiquetas de los iconos de topología mostradas.

Iconos de topología

Los siguientes iconos aparecen en la ventana **Topología**:

Tabla 9: Iconos de topología

Icono	Elemento de red	Descripción
	Punto de acceso	Representación de un punto de acceso inalámbrico.
	Nube	Representa una red o parte de una red que no está administrada por Cisco Business Dashboard.
	Enlaces	Los enlaces son líneas de conexión entre dispositivos. Haga clic en un enlace para mostrar los nombres de los dispositivos de origen y de destino y otros detalles básicos como la velocidad, etc. El grosor del enlace representa su velocidad: una línea fina indica una velocidad de 100 Mbps o menos y una línea gruesa indica una velocidad de 1 Gbps o más. Una línea discontinua representa una conexión inalámbrica.
	Router	Representa un router.

Icono	Elemento de red	Descripción
	Switch	Representa un conmutador.
	Host	Representa un host conectado a la red mediante una conexión por cable.
	Host inalámbrico	Representa un host conectado a la red mediante una conexión inalámbrica.

Panel Superposiciones y filtros

Este panel aparece a la derecha del mapa de **Topología** cuando se hace clic en **Superposiciones**. **Superposiciones** se encuentra en la parte superior derecha de la Topología, junto al cuadro **buscar**.

Tabla 10: Panel Superposiciones y filtros

Elemento	Descripción
Seleccionar superposición	<p>Esta característica mejora el mapa Topología al ofrecer información adicional basada en la selección de la vista. Estos son algunos ejemplos:</p> <ul style="list-style-type: none"> • Vista de uso de enlace: identifica el rendimiento de la red actual al supervisar la cantidad de tráfico. Este tráfico se muestra mediante enlaces codificados con color en el mapa Topología. La codificación con color cambia según el porcentaje de utilización del enlace. El verde representa los enlaces que se cargan únicamente de forma moderada, mientras que el naranja y el rojo representan los enlaces que se aproximan a los límites de capacidad. Se proporcionan controles para ajustar los umbrales de los diferentes colores. • Vista de VLAN: muestra si hay una VLAN habilitada en la red. Este valor se puede usar para identificar una VLAN con particiones u otros errores de configuración. Al seleccionar Vista de VLAN en la lista desplegable Superposición, aparecerá un segundo cuadro desplegable debajo de este campo, donde se puede seleccionar el id. de VLAN que se debe mostrar. • Vista de POE: destaca los enlaces en el mapa Topología que indican dispositivos que se están alimentando actualmente mediante un conmutador habilitado para POE. • Traza de la ruta L2: muestra el tráfico de la ruta de la capa 2 entre dos dispositivos seleccionados en la red. Se pueden seleccionar los dispositivos escribiendo el nombre de host, la dirección IP o la dirección MAC en los campos provistos, o con Mayús + clic sobre dos dispositivos del mapa de topología.

Elemento	Descripción
Seleccionar etiqueta	Especifique una Etiqueta de dispositivo en el cuadro de texto debajo de la etiqueta Seleccionar etiqueta para filtrar la topología y mostrar los dispositivos que coincidan con la etiqueta indicada. Las etiquetas de dispositivos se asignan en el panel Detailed Info (Información detallada).
Mostrar solo: <ul style="list-style-type: none"> • Routers • Switches • Tecnología inalámbrica • Hosts • Otros 	Marque la casilla situada junto a los dispositivos de la lista que desee mostrar en el mapa Topología . Esta característica permite filtrar los dispositivos que desea ver en el mapa y elimina aquellos que no están marcados en la lista de dispositivos.

Visualización de la información básica del dispositivo

Haga clic en un dispositivo de red (por ejemplo, en un conmutador, un router o un enlace que conecte dos dispositivos) para ver la información básica sobre el dispositivo, incluidas las notificaciones pendientes y las acciones que se pueden realizar. El panel **Información básica** también proporciona acceso a información más detallada sobre un dispositivo y permite acceder directamente a la interfaz de administración del dispositivo.



Nota Para ver información detallada sobre el dispositivo, consulte [Visualización de la información detallada del dispositivo](#), en la página 29.

Para ver más información sobre cómo acceder a la interfaz de administración del dispositivo, consulte [Acceso a la interfaz de administración del dispositivo](#), en la página 29.

En la tabla de la siguiente sección, encontrará los detalles que se presentan sobre el tipo de dispositivo. Para ver la información básica del dispositivo, haga lo siguiente:

- Paso 1** En la página **Red**, seleccione una red y haga clic en **Administrar** para mostrar la topología.
- Paso 2** En el mapa Topología, haga clic en el dispositivo de red (por ejemplo, un conmutador o un router) cuyos detalles desee ver.
- Paso 3** En el panel **Información básica** aparecen los detalles del dispositivo debajo de la pestaña **Descripción general**. Estos elementos se describen en la siguiente tabla:

Tabla 11: Información básica del dispositivo

Nombre de elemento	Descripción
Panel de información	
Modelo	Nombre de modelo del dispositivo.

Nombre de elemento	Descripción
Descripción	Descripción del producto o dispositivo.
Versión del firmware	Versión del firmware del dispositivo.
PID VID	Id. de versión y del producto.
Dirección MAC	La dirección <i>MAC</i> (<i>control de acceso a medios</i>) es una dirección de capa de enlace de datos estandarizada que se requiere para ciertos tipos de interfaces de red. Estas direcciones son específicas y únicas para cada dispositivo y no las utilizan otros dispositivos de la red.
Número de serie	El número de serie del dispositivo.
Estado	Estado en línea o sin conexión del dispositivo.
Dominio	El nombre de dominio del dispositivo.
Proveedor	El fabricante del dispositivo.
Red	El nombre de la red en la que se encuentra el dispositivo.
Organización	La organización a la que pertenece el dispositivo.
Panel de notificaciones	
<p>Encabezado del panel de notificaciones: el encabezado del panel de notificaciones muestra recuentos resumidos de las notificaciones pendientes del dispositivo.</p> <p>Cuerpo del panel de notificaciones: el cuerpo del panel de notificaciones enumera las notificaciones pendientes del dispositivo. Para ver y filtrar una lista completa de todas las notificaciones del dispositivo, consulte Visualización y filtrado de notificaciones actuales del dispositivo, en la página 97. Marque la casilla situada junto a una notificación para confirmarla y eliminarla de la lista de notificaciones. Si lo desea, puede usar el filtrado de notificaciones para mostrar las notificaciones confirmadas.</p>	
Panel de eventos	
El panel de eventos muestra una lista de todas las notificaciones y de otros eventos ocurridos en este dispositivo en las últimas 24 horas. Para ver y filtrar una lista completa de todos los eventos de todos los dispositivos, visite el registro de eventos.	
Panel POE	
El panel POE se muestra en conmutadores habilitados para POE y ofrece un resumen del uso de energía en cada uno de los puertos del dispositivo.	
Panel de información de la pila	
El panel de información de la pila se muestra para pilas de conmutadores y muestra los detalles de hardware de cada miembro de la pila, entre ellos la información de modelo, el número de serie y la dirección MAC.	
Servicio	
Muestra los servicios de red identificados en el dispositivo.	

Nombre de elemento	Descripción
Dispositivo conectado	
Los dispositivos de host incluyen el panel Dispositivo conectado . En este panel, se indica cómo se conecta el host a la red y se muestra el dispositivo de red anterior y, en su caso, el puerto al que el host está conectado.	

Además de la pestaña **Descripción general**, el panel **Información básica** también cuenta con una pestaña de **Acciones** que permite llevar a cabo varias tareas operacionales en el dispositivo. Para obtener más detalles, consulte [Acciones del dispositivo, en la página 27](#).

Acciones del dispositivo

Es muy fácil realizar acciones en los dispositivos de la red, por ejemplo, actualizaciones de firmware, copias de seguridad y restauraciones de configuraciones, y reinicios. Para realizar estas acciones, haga lo siguiente:

Paso 1 En el mapa **Topología** o la página **Inventario**, haga clic en un dispositivo de red (como un conmutador o un router) en el que desee realizar la acción.

Paso 2 En el panel **Información básica**, seleccione la pestaña de **Acciones**. En función de las capacidades del dispositivo, se muestran una o varias de las siguientes acciones:

Actualizar firmware a la última versión	Le permite aplicar la última actualización de firmware al dispositivo. Cisco Business Dashboard descargará la actualización de Cisco y la cargará en el dispositivo. El dispositivo se reiniciará al finalizar la actualización.
Actualizar desde local	Le permite cargar un archivo de actualización de firmware desde su unidad local. Cisco Business Dashboard cargará el archivo en el dispositivo y el dispositivo se reiniciará cuando se complete la actualización.
Configuración de copia de seguridad	<p>Permite guardar una copia de la configuración del dispositivo actual en Dashboard.</p> <ol style="list-style-type: none"> Haga clic en Configuración de copia de seguridad. En la ventana Configuración de copia de seguridad, si lo desea, puede agregar una nota en el cuadro de texto para la copia de seguridad que desee realizar. <p>Nota Esta nota verá cada vez que la copia de seguridad aparezca en la GUI.</p> Haga clic en Guardar copia de seguridad para completar esta acción. Haga clic en Cancelar si no desea continuar. <p>Se creará un trabajo de configuración de copia de seguridad que se podrá ver en el Centro de tareas.</p>

Restaurar configuración	<p>Permite restaurar en el dispositivo una configuración de la que se haya realizado previamente una copia de seguridad.</p> <p>Haga clic en Restaurar configuración.</p> <p>Se ofrecen las siguientes opciones de configuración para las copias de seguridad:</p> <ul style="list-style-type: none"> • Copias de seguridad de nombre de dispositivo: muestra una lista de todas las copias de seguridad disponibles para configurar un dispositivo específico. • Copia de seguridad para otro dispositivo: muestra una lista de todas las copias de seguridad disponibles para configurar otros tipos de dispositivos del mismo tipo o con el mismo id. de producto. • Copia de seguridad para otro dispositivo compatible: muestra una lista de todas las copias de seguridad disponibles para configurar otros dispositivos de la serie compatibles con el dispositivo seleccionado. <p>Para realizar una configuración de copia de seguridad, haga lo siguiente:</p> <ol style="list-style-type: none"> 1. En la ventana Restaurar configuración, seleccione la copia de seguridad que desee restaurar en el dispositivo. Use la barra de desplazamiento para ver todas las copias de seguridad disponibles y haga clic en el botón de opción que desee. Esta acción habilita el botón Restaurar configuración. Otro procedimiento consiste en cargar un archivo de configuración. Para ello, arrastre y suelte el archivo de configuración en el área de destino concreta o haga clic en el área de destino para seleccionar un archivo del sistema de archivos. 2. Haga clic en Restaurar configuración para completar la acción. Se creará un trabajo de configuración de restauración que se podrá ver en el Centro de tareas.
Reiniciar	<p>Permite reiniciar el dispositivo.</p> <p>Nota Al hacer clic en este botón, se le pedirá que haga clic de nuevo para confirmar la acción.</p>
Guardar configuración en ejecución	<p>Para los dispositivos que admiten configuraciones de inicio y de ejecución separadas, esta acción copia la configuración de ejecución actual en la configuración de inicio. Esto garantiza que cualquier cambio de configuración se conserve cuando el dispositivo se reinicie la próxima vez.</p>
Eliminar	<p>Elimine un dispositivo sin conexión de la Topología y el Inventario.</p>

Acceso a la interfaz de administración del dispositivo

En algunas circunstancias, es posible que necesite acceder directamente a la interfaz de administración de un dispositivo de red. Para acceder a la interfaz de administración, haga lo siguiente:

Paso 1 En la página **Topología** o **Inventario**, haga clic en el dispositivo de red (por ejemplo, un conmutador o un router) a cuya interfaz de administración desee acceder.

Paso 2 En el panel **Información básica**, haga clic en **Ver**, en la esquina superior derecha. Se abrirá una nueva ventana en el navegador, donde aparecerá la interfaz de administración del dispositivo.

Nota Al acceder a la interfaz de administración al hacer clic en **Ver**, el navegador se conectará con el dispositivo mediante Dashboard. Esto significa que si accede a la red de forma remota, solo Dashboard debe estar accesible directamente desde el exterior del sitio.

Como todas estas conexiones se realizan mediante el mismo host (o sea, Dashboard), las cookies de un dispositivo se presentarán a los demás dispositivos y estos podrían actualizarlas si el nombre es el mismo. Un síntoma claro de esto es que la sesión del navegador del primer dispositivo se cierre inmediatamente después de conectarse a un segundo dispositivo debido a la actualización de la cookie de sesión.

Visualización de la información detallada del dispositivo

Paso 1 En la página **Topología** o **Inventario**, haga clic en un dispositivo de red (por ejemplo, un conmutador o un router) para ver la información detallada.

Paso 2 En el panel **Información básica**, haga clic en **Más**, en la esquina superior derecha.

Paso 3 En el panel **Detailed Info** (Información detallada), a la izquierda encontrará una lista detallada de información sobre el dispositivo, así como funciones adicionales en las siguientes pestañas:

- **Dashboard:** muestra una serie de widgets del panel específicos del dispositivo.
- **Administración de puertos:** permite administrar la configuración de los puertos de conmutador.

Nota Esta información está disponible solo para los dispositivos con puertos de conmutador.

- **LAN inalámbricas:** permite ver las LAN inalámbricas configuradas en el dispositivo.

Nota Esta información está disponible solo para dispositivos inalámbricos.

- **Registro de eventos:** proporciona una lista de notificaciones y acciones pasadas de este dispositivo.

- **Copias de seguridad de la configuración:** permite ver una lista de configuraciones de copias de seguridad de los dispositivos y realizar acciones como restaurar, guardar o eliminar la configuración.

Nota Esta información está disponible solo para dispositivos compatibles con la operación de Configuración de copia de seguridad.

- **Configuración pendiente:** compara la configuración deseada en función de los perfiles de configuración definidos con la configuración actual en el dispositivo y destaca las diferencias.

Nota Este panel solo se muestra con los dispositivos compatibles para las operaciones de configuración en las que la configuración actual no coincida con la configuración deseada.

Estos elementos se describen en los siguientes pasos:

Paso 4

A la izquierda se muestra una lista detallada de información sobre el dispositivo. Esta lista contiene la siguiente información:

Tabla 12: Información detallada sobre el dispositivo

Nombre de elemento	Descripción
Nombre de host	Haga clic en la opción Editar , situada junto al nombre del dispositivo, para modificar el nombre de host del dispositivo. Haga clic en Guardar para guardar los cambios.
Modelo	Nombre de modelo del dispositivo.
Dirección MAC	La dirección <i>MAC (control de acceso a medios)</i> es una dirección de capa de enlace de datos estandarizada que se requiere para ciertos tipos de interfaces de red. Estas direcciones son específicas y únicas para cada dispositivo y no las utilizan otros dispositivos de la red.
Estado	Muestra el estado actual del dispositivo. Por ejemplo, conectado o desconectado.
Acciones	El menú desplegable Acciones y el icono Abrir GUI del dispositivo permiten actuar sobre el dispositivo desde el panel Detailed Info (Información detallada).
IP	La dirección IP del dispositivo.
Dominio	El nombre de dominio del dispositivo.
PID VID	Id. de versión y del producto.
Número de serie	El número de serie del dispositivo.
Proveedor	El fabricante del dispositivo.
Descripción	Descripción del producto o dispositivo.
Grupo de dispositivos	El grupo de dispositivos al que pertenece este dispositivo.
Red	La red a la que pertenece este dispositivo.
Organización	La organización a la que pertenece este dispositivo.
Parámetros de PnP	La imagen y el archivo de configuración que se proporcionarán al dispositivo mediante la función Plug and Play de red. Haga clic en el icono Editar para realizar cambios y, a continuación, en el icono Guardar para aplicarlos o Cancelar para salir sin guardar.

Nombre de elemento	Descripción
Etiquetas	En el campo Etiquetas, escriba caracteres alfanuméricos y pulse Intro si desea crear etiquetas nuevas para este dispositivo. Para eliminar una etiqueta existente, haga clic en la ✕ de la etiqueta. Haga clic en Guardar para guardar los cambios. Se pueden usar etiquetas para identificar dispositivos con características comunes. Las etiquetas se pueden usar en cualquier lugar de Cisco Business Dashboard Probe para restringir las vistas de la red a fin de mostrar un subconjunto de dispositivos.
Versión del firmware	La versión del firmware que se está ejecutando actualmente en el dispositivo. Si hay disponible una versión posterior, dicha versión se mostrará entre paréntesis junto a la versión actual. También se proporcionan iconos para ver las notas de la versión de una actualización y para aplicar la actualización al dispositivo.
Método de descubrimiento	Muestra los protocolos y dispositivos con los que se detectó este dispositivo.
Configuración pendiente	Muestra el estado de la configuración del dispositivo y si hay diferencias entre la configuración actual y la esperada.

Paso 5 Haga clic en **Dashboard** para mostrar un conjunto de widgets que indican el estado actual del dispositivo. Para obtener más información, consulte [Acerca del panel de supervisión](#).

Paso 6 Haga clic en **Administración de puertos** para ver y administrar la configuración de los puertos de conmutador del dispositivo. Se muestra una representación visual del dispositivo, parecida a la que se muestra en la página **Administración de puertos**.

En esta ventana, se especifican los detalles de los puertos del dispositivo con una representación visual. Encima de la imagen aparecen el modelo y el número de serie del dispositivo, y debajo se muestra una vista de los puertos en forma de tabla. Para obtener más detalles sobre las operaciones, consulte [Acerca de Administración de puertos, en la página 37](#).

Paso 7 Haga clic en **WLAN** para ver la configuración de radio y las LAN inalámbricas configuradas en este dispositivo.

Paso 8 Haga clic en **Registro de eventos** para ver una lista de notificaciones históricas y otros eventos registrados para este dispositivo. Puede usar filtros para limitar las entradas mostradas. Para obtener más información, consulte [Acerca del registro de eventos](#).

Paso 9 Haga clic en **Copias de seguridad de la configuración** para ver y administrar las copias de seguridad de la configuración de este dispositivo. En esta ficha, verá una tabla donde aparecen las copias de seguridad almacenadas en Probe, con los siguientes detalles:

Tabla 13: Copias de seguridad de la configuración

Elemento	Descripción
Marca de tiempo	La fecha y la hora en la que se realizó la copia de seguridad de la configuración.
Comentario	Las notas que especifica el usuario en el momento de realizar la copia de seguridad.
Copia de seguridad realizada por	El usuario que realizó la configuración.

Elemento	Descripción
Acciones	<p>Elija una de las siguientes acciones de copia de seguridad:</p> <ul style="list-style-type: none"> • Restaurar configuración en el dispositivo: permite restaurar la copia de seguridad seleccionada en el dispositivo. • Guardar configuración en el PC: permite guardar la copia de seguridad como un archivo zip en una unidad local del PC. • Eliminar configuración: elimina la copia de seguridad • Ver configuración: ayuda a ver el contenido de la copia de seguridad de configuración en el navegador.

También puede activar una copia de seguridad de configuración desde la pestaña haciendo clic en **Configuración de copia de seguridad**.

Paso 10 Haga clic en **Configuración pendiente** para ver una comparación en paralelo entre la configuración actual del dispositivo y la esperada en función de los perfiles de configuración aplicados al dispositivo. Las configuraciones se representan en un formato independiente del dispositivo; asimismo, se resaltan las diferencias. Puede utilizar los botones de la parte superior de la página para aplicar los cambios pendientes, aceptar la configuración actual del dispositivo o volver a leer dicha configuración.

Uso de planos de plantas

La vista Plano de planta permite realizar un seguimiento de las ubicaciones físicas de su equipo de red. Se puede cargar un plano para cada planta del edificio y situar cada dispositivo de red en el plano. Esto facilita la localización de los dispositivos en caso de que sea necesario realizar labores de mantenimiento. El Plano de planta funciona de forma parecida al mapa Topología y los dispositivos ubicados en el Plano de planta se utilizan del mismo modo que los dispositivos del mapa Topología.

Creación de un nuevo plano de planta

1. Acceda a **Vista de red** y haga clic en **Plano de planta**. Si se muestra un plano de planta existente, haga clic en el icono **Inicio** en la parte superior izquierda del plano.
2. Si el edificio al que desea agregar un plano de planta ya se ha creado, continúe con el paso siguiente. De lo contrario, especifique el nombre del edificio que alberga la planta en el campo **Nuevo edificio**. Haga clic en el icono **Guardar**.
3. Arrastre un archivo de imagen que contenga el plano de planta y suéltelo en el área de destino de la nueva planta. También puede hacer clic en el área de destino para especificar un archivo a fin de cargarlo. Los formatos de imágenes admitidos son png, gif y jpg. Los archivos de imagen pueden tener un tamaño máximo de 500 KB.
4. Especifique un nombre para la planta en el campo **Nueva planta**. Haga clic en el icono **Guardar**.
5. Repita los pasos del 2 al 4 para cada edificio y planta en los que haya dispositivos de red.

Ubicación de los dispositivos de red en un plano de planta

1. Acceda a **Vista de red** y haga clic en **Plano de planta**. Si no se muestra el plano de planta que le interesa, haga clic en el plano de planta.
2. Haga clic en **Agregar dispositivos** y, a continuación, use el cuadro de búsqueda situado en la parte inferior izquierda para encontrar el dispositivo que desea colocar. Puede buscar por nombre de host, tipo de dispositivo o dirección IP. A medida que escriba, los dispositivos coincidentes se mostrarán debajo del cuadro de búsqueda. Los iconos grises representan los dispositivos que ya se han ubicado en un plano de planta.
3. Haga clic en un dispositivo y arrástrelo para agregarlo al plano de planta en la ubicación correspondiente. Si selecciona un dispositivo que ya estaba ubicado en otro plano de planta, se eliminará de dicho plano y se agregará al nuevo.
4. Repita los pasos 2 y 3 hasta que todos los dispositivos se hayan agregado al plano de planta.

Eliminación de un dispositivo del plano de planta

1. Acceda a **Vista de red** y haga clic en **Plano de planta**. Si no se muestra el plano de planta que le interesa, haga clic en el plano de planta.
2. Identifique el dispositivo que desea eliminar y haga clic para seleccionarlo.
3. Haga clic en la cruz roja que se muestra para eliminar el dispositivo del plano de planta.

Cambio del plano de planta

1. Acceda a **Vista de red** y haga clic en **Plano de planta**. Si se muestra un plano de planta existente, haga clic en el icono **Inicio** en la parte superior izquierda del plano.
2. Para cambiar el nombre de un edificio, haga clic en el icono **Editar** situado junto al nombre. Una vez que los cambios estén completos, haga clic en el icono **Guardar**.
3. Para modificar un plano de planta, haga clic en el icono **Editar** situado junto al nombre del plano de planta. Puede modificar un plano de planta arrastrando un archivo de imagen nueva hasta el área de destino. También puede hacer clic en el área de destino para cargar un archivo nuevo desde un PC. Si lo desea, también puede cambiar el nombre del plano de planta. Una vez que los cambios estén completos, haga clic en el icono **Guardar**.

Eliminación de un plano de planta

1. Acceda a **Vista de red** y haga clic en **Plano de planta**. Si se muestra un plano de planta existente, haga clic en el icono **Inicio** en la parte superior izquierda del plano.
2. Identifique el plano de planta que desee eliminar y haga clic en el icono **Eliminar** en la esquina superior derecha del área de destino de la imagen.
3. Si desea eliminar el edificio entero que contiene todas las plantas de plano, haga clic en el icono **Eliminar** situado junto al nombre del edificio.



CAPÍTULO 5

Inventario

Este capítulo contiene las siguientes secciones:

- [Visualización del inventario de dispositivos, en la página 35](#)

Visualización del inventario de dispositivos

La página **Inventario** muestra una lista completa de los dispositivos y su información en forma de tabla. Además, también se proporcionan botones de acción para realizar tareas de configuración y aplicar el firmware más reciente para dispositivos compatibles. En la siguiente tabla, se proporcionan detalles sobre la información que se presenta:

Tabla 14: Detalles del inventario

Elemento	Descripción
Nombre de host	Muestra el nombre del dispositivo.
Tipo	El tipo de dispositivo, por ejemplo, conmutador, router o punto de acceso inalámbrico (WAP).
Etiquetas	Muestra las etiquetas asociadas con el dispositivo.
IP	Direcciones de protocolo de Internet (IP) del dispositivo.
MAC (oculto de forma predeterminada)	La dirección de control de acceso a medios (MAC) es una dirección de capa de enlace de datos estandarizada que se requiere para ciertos tipos de interfaces de red. Estas direcciones son específicas y únicas para cada dispositivo y no las utilizan otros dispositivos de la red.
Número de serie	Número de serie del dispositivo.
Versión	La versión del firmware actual del dispositivo.
Proveedor (oculto de forma predeterminada)	El proveedor que fabricó el dispositivo.
Modelo	Nombre de modelo del dispositivo.
Organización	La organización a la que pertenece el dispositivo.

Elemento	Descripción
Red	La red a la que pertenece el dispositivo.
Notificación	Un recuento de las notificaciones pendientes del dispositivo.
PnP Status (Estado de PnP) (oculto de forma predeterminada)	El estado actual de la función Plug and Play de red del dispositivo. Para obtener más información, consulte las páginas de Plug and Play de red .

En la página **Inventario**, están disponibles los siguientes controles adicionales:

- Botón **Seleccionar columnas**: utilice este botón situado en la parte superior izquierda de la tabla para elegir qué columnas mostrar.
- Cuadro **Filtrar**: puede usar el cuadro **Filtrar** para limitar la visualización al escribir nombres de dispositivos, tipos de dispositivos, números de serie, etc. De forma predeterminada, el inventario está filtrado para mostrar solo los dispositivos de red.
- Icono **Agregar**: haga clic en el icono más (+) para añadir nuevos dispositivos al inventario antes de que se detecte el dispositivo. Al añadir manualmente un dispositivo al inventario, puede proporcionar información básica acerca de él, como la identidad, la organización, el grupo de dispositivos y la configuración de PnP. El hecho de ofrecer esta información con antelación garantiza que el dispositivo se administre correctamente cuando esté conectado a la red.
- Botón **Actualizar**: haga clic en este botón para actualizar la tabla y mostrar la información más reciente.
- Botones **Acciones**: los siguientes botones permiten realizar acciones en uno o varios dispositivos seleccionados.
 - **Descargar el firmware más reciente**
 - **Aplicar actualización de firmware local**
 - **Configuración de copia de seguridad**
 - **Restaurar configuración**
 - **Reiniciar dispositivo**
 - **Guardar configuración en ejecución**
 - **Eliminar**

Los botones de acción solo se muestran cuando se seleccionan uno o varios dispositivos que admiten acciones.



Nota Para obtener más información sobre estas acciones, consulte [Acciones del dispositivo](#).



CAPÍTULO 6

Administración de puertos

Este capítulo contiene las siguientes secciones:

- [Acerca de Administración de puertos, en la página 37](#)

Acerca de Administración de puertos

Administración de puertos ofrece una vista de panel frontal de cada dispositivo que incluye los puertos de conmutador que Cisco Business Dashboard puede configurar. Esta página permite ver el estado de los puertos, incluidos los contadores de tráfico, y realizar cambios en la configuración de puertos. Esta página permite ver y configurar la función de los Smartports para los puertos de dispositivos compatibles con esta función. Puede usar la casilla de búsqueda para restringir los dispositivos mostrados. Escriba total o parcialmente el nombre de un dispositivo, el id. del producto o el número de serie para buscar el dispositivo deseado.

También se proporciona una vista de lista de la misma información para mostrar todos los puertos de switch en forma de tabla. La vista de panel frontal de **Administración de puertos** presenta dos vistas diferentes del dispositivo:

- **Físico:** esta vista muestra el estado y los cambios de configuración del puerto en la capa física. Se pueden ver o cambiar diversas configuraciones, como la velocidad, la función dúplex, el Ethernet de eficiencia energética (EEE), la alimentación por Ethernet (PoE) y las VLAN. Cada puerto cuenta con un LED verde que indica un enlace y un LED amarillo que indica que se está suministrando alimentación al dispositivo conectado.
- **Smartports:** esta vista permite ver la función actual Smartport para cada puerto y cambiar la función. Cada puerto tiene un icono superpuesto que indica la función actual.



Nota

Un Smartport es una interfaz a la que se puede aplicar una plantilla integrada (o definida por el usuario). Estas plantillas están diseñadas para configurar rápidamente el dispositivo de forma que cumpla los requisitos de comunicación y utilice las características de los distintos tipos de dispositivos de red.

Para ver el estado de un puerto, haga clic en el puerto en la vista del panel frontal o en la de lista. Aparece el panel **Información básica** del puerto, que muestra los siguientes paneles:

- **General:** el panel **General** muestra el estado de la capa física del puerto y le permite activar el puerto o apagarlo
- **Ethernet:** permite controlar la velocidad y la configuración dúplex.

- **VLAN:** el panel **VLAN** muestra las VLAN configuradas actualmente en el puerto. Haga clic en los botones **Seleccionar VLAN** o **Crear una VLAN** para modificar esta configuración.
- **POE:** el panel **POE** solo se muestra con puertos habilitados para POE y permite configurar sus ajustes de POE. También puede reiniciar un dispositivo POE asociado haciendo clic en el botón **Cambiar alimentación**.
- **Green Ethernet:** el panel **Green Ethernet** permite administrar la configuración de Ethernet de eficiencia energética (EEE) del puerto.
- **Smartports:** el panel **Smartports** muestra las funciones Smartports disponibles para el puerto. Haga clic en una función para aplicar dicha configuración al puerto. Se destaca la función configurada en ese momento.

Para realizar cambios en la configuración del puerto, haga clic en el icono **Editar**, en la parte superior derecha del panel que contiene esa configuración. Una vez realizados los cambios, haga clic en el icono **Guardar**.



CAPÍTULO 7

Configuración de red

Este capítulo contiene las siguientes secciones:

- [Acerca de Configuración de red](#), en la página 39
- [Uso del Asistente](#), en la página 39
- [Configuración de la administración del tiempo](#), en la página 40
- [Configuración de los Analizadores de DNS](#), en la página 41
- [Configuración de la autenticación](#), en la página 41
- [Configuración de LAN virtuales](#), en la página 42
- [Configuración de LAN inalámbricas](#), en la página 43

Acerca de Configuración de red

Las páginas de **Configuración de red** permiten definir diversos parámetros de configuración que se suelen aplicar a algunos de los dispositivos de la red o a todos ellos. Entre estos parámetros, se incluyen configuraciones como los ajustes de hora, los servicios de nombre de dominio, la autenticación de administrador y las LAN virtuales e inalámbricas. Puede crear perfiles de configuración para cada una de estas áreas por separado. El asistente también permite crear perfiles para cada área en un único flujo de trabajo. Los perfiles de configuración se aplican a uno o varios grupos de dispositivos y, a continuación, se distribuyen a los dispositivos.

Uso del Asistente

El asistente le permite crear perfiles de configuración para cada uno de los elementos de Configuración de red y asignar dichos perfiles a uno o varios grupos de dispositivos en un único flujo de trabajo.

Uso del Asistente

1. Acceda a **Configuración de red > Asistente**.
2. En la pantalla **Selección de grupo de dispositivos**, especifique un nombre de perfil para esta configuración, elija una organización y seleccione uno o varios grupos de dispositivos para configurarlos. Haga clic en **Siguiente**.
3. En cada una de las pantallas que aparecen a continuación, seleccione las configuraciones que procedan. Para obtener más detalles sobre estos parámetros, consulte las siguientes secciones.

4. Complete las opciones de configuración en cada pantalla y haga clic en **Siguiente**. Si no desea definir los ajustes de una pantalla concreta para un perfil determinado, haga clic en **Omitir**. Haga clic en **Atrás** para acceder a las pantallas anteriores. También puede hacer clic en los encabezados de la izquierda.
5. Finalice la configuración y revísela en la pantalla final. Haga clic en **Finalizar** para aplicar la configuración a los dispositivos seleccionados.

Configuración de la administración del tiempo

La página **Administración del tiempo** permite configurar las zonas horarias, el horario de verano y los servidores NTP para la red. En las siguientes secciones, se proporciona información sobre cómo crear, modificar y eliminar el perfil de configuración de los ajustes de hora.

Creación de un perfil de configuración para la administración del tiempo

1. Acceda a **Configuración de red > Administración del tiempo**.
2. Haga clic en el icono **+** (más) para agregar un perfil nuevo.
3. En la sección **Selección de grupo de dispositivos**, especifique un nombre de perfil para esta configuración, elija una organización y seleccione uno o varios grupos de dispositivos para configurarlos.
4. En la sección **Ajuste de hora**, seleccione la zona horaria que desee en la lista desplegable.
5. También puede habilitar **Horario de verano** marcando la casilla de verificación. A continuación, especifique los parámetros correspondientes en los campos proporcionados. Puede especificar fechas fijas o un patrón recurrente. También puede especificar la diferencia que se debe usar.
6. Si lo desea, habilite el Protocolo de tiempo de red (NTP) en la sección **Usar NTP** para sincronizar el reloj marcando la casilla de verificación correspondiente. En los cuadros correspondientes, especifique una dirección de servidor NTP como mínimo.
7. Haga clic en **Guardar**.

Modificación de un perfil de configuración para la administración del tiempo

1. Seleccione el botón de opción situado junto al perfil que desea modificar y haga clic en el icono **Editar**.
2. Efectúe los cambios oportunos en la configuración del perfil y haga clic en **Actualizar**.

Eliminación de un perfil de configuración para la administración del tiempo

1. Seleccione el botón de opción situado junto al perfil que se debe eliminar.
2. Haga clic en el icono **Eliminar**.

Configuración de los Analizadores de DNS

La página **Analizadores de DNS** permite configurar el nombre de dominio y los servidores de nombres de dominio para la red. En las siguientes secciones, se proporciona información sobre cómo crear, modificar y eliminar un perfil de configuración de los analizadores de DNS.

Creación de un perfil de configuración para el Analizador de DNS

1. Acceda a **Configuración de red > Analizadores de DNS**.
2. Haga clic en el icono **+** (más) para agregar un perfil nuevo.
3. En la sección **Selección de grupo de dispositivos**, especifique un nombre de perfil para esta configuración, elija una organización y seleccione uno o varios grupos de dispositivos para configurarlos.
4. Especifique el nombre de dominio para la red.
5. Especifique al menos una dirección de servidor DNS.
6. Haga clic en **Guardar**.

Modificación de un perfil de configuración para el Analizador de DNS

1. Seleccione el botón de opción situado junto al perfil que desea modificar y haga clic en el icono **Editar**.
2. Efectúe los cambios oportunos en la configuración del perfil y haga clic en **Actualizar**.

Eliminación de un perfil de configuración para el Analizador de DNS

1. Seleccione el botón de opción situado junto al perfil que se va a eliminar.
2. Haga clic en el icono **Eliminar**.

Configuración de la autenticación

La página **Autenticación** permite configurar el acceso de usuario administrativo a los dispositivos de red. En las siguientes secciones, se proporciona información sobre cómo crear, modificar y eliminar un perfil de configuración de autenticación.

Creación de un perfil de configuración de autenticación

1. Acceda a **Configuración de red > Autenticación**.
2. Haga clic en el icono **+** (más) para agregar un perfil nuevo.
3. En la sección **Selección de grupo de dispositivos**, especifique un nombre de perfil para esta configuración, elija una organización y seleccione uno o varios grupos de dispositivos para configurarlos.
4. Especifique como mínimo una combinación de nombre de usuario y contraseña para la autenticación del usuario local. Se pueden agregar más usuarios haciendo clic en el icono **+** (más).
5. También puede exigir el uso de contraseñas complejas.

6. Haga clic en **Guardar**.

Modificación de un perfil de configuración de autenticación

1. Seleccione el botón de opción situado junto al perfil que desea modificar y haga clic en el icono **Editar**.
2. Efectúe los cambios oportunos en la configuración del perfil y haga clic en **Actualizar**.

Eliminación de un perfil de configuración de autenticación

1. Seleccione el botón de opción situado junto al perfil que se debe eliminar.
2. Haga clic en el icono **Eliminar**.

Configuración de LAN virtuales

La página **LAN virtuales** permite dividir la red de conmutadores en varias redes virtuales o VLAN. Las VLAN de la red que no se hayan configurado con Cisco Business Dashboard también se pueden ver en esta página en una tabla aparte. En las siguientes secciones, se proporciona información sobre cómo crear, modificar y eliminar un perfil de configuración de LAN virtuales.

Creación de una LAN virtual

1. Acceda a **Configuración de red > LAN virtuales**.
2. Haga clic en el icono **+** (más) para agregar una VLAN nueva.
3. En la sección **Selección de grupo de dispositivos**, especifique un nombre de perfil para esta configuración, elija una organización y seleccione uno o varios grupos de dispositivos para configurarlos.
4. Especifique un nombre descriptivo para la VLAN y el id. de VLAN que se debe usar. El ID de la VLAN debe ser un número entre 1 y 4094.
5. Puede crear varias VLAN usando un solo perfil. Si quiere generar VLAN adicionales en este perfil, haga clic en **Agregar otro** y vuelva al paso 4.
6. Haga clic en **Guardar**. La nueva VLAN se creará en todos los dispositivos compatibles con VLAN de los grupos seleccionados.

Si el ID de la VLAN recién creada coincide con una VLAN ya presente en los dispositivos del grupo de dispositivos, Cisco Business Dashboard adoptará esa VLAN y, a su vez, esta se eliminará de la tabla de LAN virtuales detectadas.

Modificación de una VLAN

1. Marque el botón de opción situado junto a la VLAN que desee modificar y haga clic en el icono **Editar**.
2. Efectúe los cambios oportunos en la configuración de la VLAN y haga clic en **Actualizar**.

Eliminación de una VLAN

Marque el botón de opción situado junto a la VLAN que desee eliminar y haga clic en el icono **Eliminar**.

Eliminación de una VLAN no creada en Cisco Business Dashboard

En la tabla de VLAN detectadas, haga clic en el icono **Eliminar** situado junto a las VLAN que desee eliminar.



Nota Es posible que la VLAN 1 no se pueda eliminar.

Configuración de LAN inalámbricas

La página **LAN inalámbricas** permite administrar las redes inalámbricas de su entorno. Las LAN inalámbricas de la red que no se hayan configurado con Cisco Business Dashboard también se pueden ver en una tabla separada. En las siguientes secciones, se proporciona información sobre cómo crear, modificar y eliminar un perfil de configuración de LAN inalámbricas.

Creación de una LAN inalámbrica

1. Acceda a **Configuración de red > LAN inalámbricas**.
2. Haga clic en el icono **+** (más) para agregar una nueva LAN inalámbrica.
3. En la sección **Selección de grupo de dispositivos**, especifique un nombre de perfil para esta configuración, elija una organización y seleccione uno o varios grupos de dispositivos para configurarlos.
4. Especifique un nombre de SSID para la LAN inalámbrica y el ID de VLAN con el que se debe asociar. El id. de VLAN debe ser un número entre 1 y 4095. Si no existe en la red, se creará automáticamente una VLAN nueva.
5. Si lo desea, cambie la configuración de **Habilitar, Difusión, Seguridad y Radio** para que se ajusten a sus requisitos.
6. Puede crear varias LAN inalámbricas usando un solo perfil. Si quiere generar LAN inalámbricas adicionales en este perfil, haga clic en **Agregar otro** y vuelva al paso 3.
7. Según el modo de seguridad seleccionado (**Empresarial** o **Personal**), especifique el servidor RADIUS con el que se debe realizar la autenticación o una clave precompañada.
8. Haga clic en **Guardar**. La nueva WLAN se creará en todos los dispositivos con funciones de punto de acceso inalámbrico de los grupos seleccionados.

Si la configuración de LAN inalámbrica del perfil recién creado coincide con una LAN inalámbrica ya presente en los dispositivos del grupo de dispositivos, Cisco Business Dashboard adoptará esa LAN inalámbrica y, a su vez, esta se eliminará de la tabla de LAN inalámbricas detectadas.

Modificación de una LAN inalámbrica

1. Marque el botón de opción situado junto a la LAN inalámbrica que desee modificar y haga clic en el icono **Editar**.
2. Efectúe los cambios oportunos en la configuración de la LAN inalámbrica y haga clic en **Actualizar**.

Eliminación de una LAN inalámbrica

Seleccione el botón de opción situado junto a las LAN inalámbricas que desee eliminar y haga clic en el icono **Eliminar**.



Nota Si se generó automáticamente una LAN virtual al crear la LAN inalámbrica, la LAN virtual no se eliminará cuando se quite la inalámbrica. La LAN virtual se puede eliminar en la página **LAN virtuales**.

Eliminación de una LAN inalámbrica creada en Cisco Business Dashboard

En la tabla de LAN inalámbricas detectadas, haga clic en el botón de opción de la LAN inalámbrica que se vaya a eliminar y, a continuación, en el icono **Eliminar**. En algunos casos, es posible que una WLAN no se pueda eliminar de determinados dispositivos. En estos casos, habrá que hacer cambios en la configuración del dispositivo directamente.



CAPÍTULO 8

Plug and Play de red

Este capítulo contiene las siguientes secciones:

- [Acerca de Plug and Play de red, en la página 45](#)
- [Requisitos de red, en la página 45](#)
- [Configuración de la detección mediante Plug and Play Connect, en la página 47](#)
- [Configuración del servicio Plug and Play de red, en la página 48](#)
- [Supervisión de Plug and Play de red, en la página 55](#)

Acerca de Plug and Play de red

Plug and Play de red es un servicio que funciona junto con dispositivos habilitados a tal fin para permitir la gestión centralizada del firmware y la configuración, y la implementación sin intervención del usuario de nuevos dispositivos de red. Los dispositivos se pueden implementar directamente mediante el protocolo Plug and Play de red o indirectamente si los detecta una sonda asociada a Dashboard.

Cuando se instala, un dispositivo habilitado para Plug and Play de red identifica el servidor de Plug and Play de red a través de uno de configuración manual, DHCP, DNS o el servicio Plug and Play Connect. En las siguientes secciones, se proporcionan más detalles sobre la configuración del servicio Plug and Play de red de Cisco Business Dashboard.

Requisitos de red

Un dispositivo Plug and Play de red encontrará automáticamente la dirección del servidor Plug and Play de red mediante uno de los siguientes métodos. Se usará cada método de forma consecutiva hasta encontrar una dirección o hasta que todos ellos fallen. Los métodos usados (en orden) son los siguientes:

- **Configuración manual:** un dispositivo habilitado para Plug and Play de red puede configurarse manualmente con la dirección del servidor a través de la interfaz de administración.
- **DHCP:** puede suministrarse la dirección del servidor al dispositivo en la opción de información específica del proveedor.
- **DNS:** si no se ha suministrado la opción de información específica del proveedor DHCP, el dispositivo realizará una búsqueda DNS del servidor usando un nombre de host conocido.
- **Servicio Plug and Play Connect:** si, finalmente, ningún método tiene éxito, el dispositivo tratará de conectar con el servicio Plug and Play Connect. Dicho servicio redireccionará el dispositivo a su servidor.

Una vez que el dispositivo haya identificado el servidor, conectará con él y actualizará el firmware y la configuración según las especificaciones del servidor.

Configuración de detección mediante DHCP

Para detectar la dirección del servidor mediante DHCP, el dispositivo enviará un mensaje de detección DHCP con opción 60 que contiene la cadena “ciscopnp”. El servidor DHCP debe enviar una respuesta que contenga la opción de información específica del proveedor (opción 43). El dispositivo extrae la dirección del servidor de dicha opción y la utiliza para conectar con el servidor. Un ejemplo de cadena de opción 43 con la dirección de un servidor Plug and Play de red sería “5A1N;B2;K4;I172.19.45.222;J80”.

La cadena de opción 43 contiene los siguientes elementos delimitados por punto y coma:

- 5A1N: especifica la opción secundaria DHCP para Plug and Play, operación activa, versión 1, sin información de depuración. No es necesario modificar esta parte de la cadena.
- B2 = tipo de dirección IP:
 - B1 = nombre de host
 - B2 = IPv4
- Ixxx.xxx.xxx.xxx: dirección IP o nombre de host del servidor (tras una i mayúscula). En este ejemplo, la dirección IP es 172.19.45.222.
- Jxxxx: nombre del puerto utilizado para conectar con el servidor. En este ejemplo, el número de puerto es 80. El puerto predeterminado para HTTP es el 80 y para HTTPS el 443.
- K4 = protocolo de transporte que se usa entre el agente de Cisco Plug and Play y el servidor:
 - K4 = HTTP (predeterminado)
 - K5 = HTTPS
- *TrustpoolBundleURL*: parámetro opcional que especifica la URL externa del paquete de trustpool si se va a obtener de una ubicación distinta al servidor. Por ejemplo, para descargar el paquete de un servidor TFTP en 10.30.30.10, especificaría el parámetro de esta forma: `Tftp://10.30.30.10/ca.p7b`
- Si utiliza seguridad de trustpool y no especifica el parámetro T, el dispositivo obtiene el paquete de trustpool del servidor.
- Zxxx.xxx.xxx.xxx: dirección IP del servidor NTP. Este parámetro es obligatorio cuando se usa seguridad de trustpool para garantizar que todos los dispositivos estén sincronizados.

Consulte la documentación de su servidor DHCP para obtener detalles sobre la configuración de opciones de DHCP.

Configuración de detección mediante DNS

Si la detección mediante DHCP no puede obtener la dirección IP del servidor, el dispositivo vuelve a un método de búsqueda mediante DNS. En función del nombre de dominio de red devuelto por el servidor DHCP, el dispositivo crea un nombre de dominio completo (FQDN) para el servidor usando el nombre de host preestablecido “pnpserver”.

Por ejemplo: si el servidor DHCP devuelve el nombre de dominio “ejemplo.com”, el dispositivo crea el FQDN “pnpserver.ejemplo.com”. Después, utiliza el servidor de nombre local para averiguar la dirección IP de este FQDN.

Requisitos de certificación

Al establecer una conexión con un servidor de Plug and Play de red, el cliente comprueba si el certificado presentado por el servidor es válido y se puede confiar en él. Para que el certificado sea aceptable y la conexión pueda realizarse, el certificado debe cumplir las siguientes condiciones:

- El certificado debe estar firmado por una entidad de certificación (CA) de confianza, o bien el cliente debe confiar en el propio certificado. Un certificado descargado del parámetro TrustpoolBundleURL obtenido de DHCP, o bien del servicio Plug and Play Connect es de confianza para el cliente.
- Si la identidad del servidor se detecta mediante la configuración manual, DHCP o Plug and Play Connect y es una dirección IP, los campos **Nombre común** o **Nombre alternativo del asunto** deben contener esa dirección IP.
- Si la identidad del servidor se detecta mediante la configuración manual, DHCP o Plug and Play Connect y es un nombre de host, los campos **Nombre común** o **Nombre alternativo del asunto** deben contener ese nombre de host.
- Si la identidad del servidor se detecta mediante DNS, los campos **Nombre común** o **Nombre alternativo del asunto** deben contener la dirección IP correspondiente al nombre de host conocido `pnpserver.<dominio local>`.



Nota Algunas de las implementaciones de cliente antiguas de Plug and Play de red no verifican la presencia de la identidad del servidor en el certificado.

Configuración de la detección mediante Plug and Play Connect

Plug and Play Connect es un servicio proporcionado por Cisco y el último recurso para detectar el servidor usado por dispositivos habilitados para Plug and Play de red. Para usar Plug and Play Connect para la detección del servidor, primero debe crear un perfil de controlador que represente al servidor PnP y, a continuación, registrar cada uno de sus dispositivos en el servicio Plug and Play Connect.

Acceso al servicio Plug and Play Connect

Para acceder al servicio Plug and Play Connect, haga lo siguiente:

1. En su navegador web, vaya a <https://software.cisco.com>
2. Haga clic en el botón **Log In** (Iniciar sesión) de la parte superior derecha de la pantalla. Inicie sesión con un ID cisco.com asociado a su Cisco Smart Account.
3. Seleccione el enlace **Plug and Play Connect** situado debajo del encabezado **Plug and Play de red**. Aparecerá la página principal del servicio **Plug and Play Connect**.

Creación de un perfil de controlador

Para crear un perfil de controlador para servidor PnP, haga lo siguiente:

1. Abra la página Web de Plug and Play Connect en su navegador. Si es necesario, seleccione la cuenta virtual adecuada.

2. Seleccione el enlace de perfiles de controladores y haga clic en el botón **Añadir perfil**.
3. Seleccione un tipo de controlador de SERVIDOR PNP en el menú desplegable. Después, haga clic en **Siguiente**.
4. Escriba un nombre y, opcionalmente, una descripción para el perfil.
5. Debajo del encabezado del controlador principal, use el menú desplegable para seleccionar si se va a especificar el servidor por nombre o por dirección IP. Introduzca el nombre o las direcciones del servidor en los campos provistos.
6. Seleccione qué protocolo usar para la comunicación con el servidor. Se recomienda encarecidamente usar HTTPS para garantizar la integridad del servicio de aprovisionamiento.
7. Si el protocolo seleccionado es HTTPS, el certificado empleado por el servidor debería cargarse mediante los controles proporcionados. Consulte [Gestión de certificados, en la página 82](#) para obtener detalles sobre la descarga del certificado de Cisco Business Dashboard.
8. También puede especificar un controlador secundario.
9. Haga clic en **Siguiente** y repase la configuración antes de hacer clic en **Enviar**.

Registro de dispositivos

En el momento del pedido, algunos productos adquiridos directamente a Cisco pueden estar asociados a su Cisco Smart Account y se añadirán automáticamente a Plug and Play Connect. Sin embargo, la mayoría de productos habilitados para Plug and Play de Cisco Business deberán registrarse manualmente. Para registrar dispositivos en Plug and Play Connect, haga lo siguiente:

1. Abra la página Web de Plug and Play Connect en su navegador. Si es necesario, seleccione la cuenta virtual adecuada.
2. Seleccione el enlace **Dispositivos** y haga clic en **Añadir dispositivos**. Puede que necesite aprobación para añadir manualmente dispositivos a su cuenta. Se trata de un proceso que solo se realiza una vez y, si es necesario, se le notificará por correo electrónico cuando se conceda la aprobación.
3. Elija si se añadirán dispositivos manualmente o si se añadirán varios dispositivos cargando los detalles en formato CSV. Haga clic en el enlace proporcionado para descargar un archivo CSV de muestra. Si decide cargar un archivo CSV, haga clic en el botón **Examinar** para seleccionar el archivo. Después, haga clic en **Siguiente**.
4. Si ha elegido añadir dispositivos manualmente, haga clic en **Identificar dispositivo**. Especifique el número de serie y el ID de producto del dispositivo que va a añadirse. Seleccione un perfil de controlador del menú desplegable. También puede introducir una descripción del dispositivo.
5. Repita el paso 4 hasta que se hayan añadido todos sus dispositivos. A continuación, haga clic en **Siguiente**.
6. Revise los dispositivos añadidos y haga clic en **Enviar**.

Configuración del servicio Plug and Play de red

Puede que sea necesario llevar a cabo diversas tareas a la hora de configurar el servicio Plug and Play de red para su entorno. Entre ellas, cargar configuraciones e imágenes, agregar y configurar dispositivos para que

usen el servicio Plug and Play de red, y administrar los dispositivos que se conectan al servicio cuando no se han registrado previamente en él. Las siguientes secciones describen estas tareas en detalle.

Uso del panel de Plug and Play de red

El panel de control de **Plug and Play de red** da una visión general de los dispositivos que se están aprovisionando actualmente usando Plug and Play de red. Se muestran tres gráficos donde aparece el estado del dispositivo desglosado por grupo de dispositivos, dispositivo habilitado para PnP y dispositivos que no están definidos en el inventario de Cisco Business Dashboard (dispositivos no reclamados). Cada tabla muestra el número de dispositivos o grupos en cada uno de los estados enumerados. Puede hacer clic en el encabezado de estado de cualquiera de las tablas para ver una lista detallada de dispositivos o grupos incluidos en esa categoría. La siguiente tabla proporciona un desglose de los diferentes estados:

Tabla 15: Dashboard Plug and Play de la red: definiciones de estados

Estado	Descripción
Grupos	
Preaprovisionado	Grupos de dispositivos con dispositivos habilitados para PnP solo con estado pendiente.
En curso	Grupos de dispositivos con dispositivos habilitados para PnP con estado Pendiente y algunos con el estado Aprovisionando o Aprovisionado
Aprovisionado	Grupos de dispositivos en los que los dispositivos habilitados para PnP con estado Aprovisionado
Error	Grupos de dispositivos con uno o más dispositivos habilitados para PnP con estado Error
Dispositivos habilitados	
Pendiente	Dispositivos del inventario que se han habilitado para PnP, pero que aún no se han puesto en contacto con el servidor de PnP
Aprovisionamiento	Dispositivos que se han puesto en contacto con el servidor PnP y han comenzado el aprovisionamiento pero no han completado el proceso
Aprovisionado	Dispositivos que se han aprovisionado correctamente con PnP
Error	Dispositivos en los que el proceso de aprovisionamiento PnP ha fallado
Dispositivos no reclamados	
No reclamado	Dispositivos que se han puesto en contacto con el servidor de PnP pero no están definidos en el inventario
Ignorado	Dispositivos no reclamados que el usuario ha ignorado explícitamente

Puede restringir a una organización concreta los datos mostrados mediante el menú desplegable de organizaciones, en la parte superior derecha de la página. Al ver grupos de dispositivos, escriba todo el nombre del grupo o parte de él en el cuadro de búsqueda para limitar los grupos que aparecen en la tabla. Del mismo modo, puede introducir el nombre, el ID de producto o el número de serie del dispositivo en el cuadro de búsqueda al ver las reglas de aprovisionamiento para mostrar el estado actual de un dispositivo concreto.



Nota El gráfico de los dispositivos no reclamados solo se muestra a los **Administradores** que visualizan datos de **Todas las organizaciones**.

Administración de dispositivos habilitados

Los dispositivos habilitados son dispositivos del inventario que se han configurado para aprovisionar un archivo de configuración o imagen o que Cisco Business Dashboard detectó anteriormente y que han intentado conectarse mediante el protocolo Plug and Play de red. Un dispositivo habilitado que se ha configurado con un archivo de configuración o imagen tendrá esa imagen o configuración aplicada al dispositivo en la próxima oportunidad. Si el dispositivo está conectado y gestionado por Dashboard, los cambios se aplicarán inmediatamente. De lo contrario, los cambios se aplicarán la próxima vez que se conecte el dispositivo, ya sea a través de una sonda o gestión directa, o cuando se registre utilizando el protocolo Plug and Play de red.

Para crear un nuevo dispositivo habilitado, siga estos pasos:

1. Acceda a **Plug and Play de red > Dispositivos habilitados**.
2. Haga clic en el icono **+** (más) para añadir un nuevo dispositivo habilitado al inventario.
3. Rellene el formulario **Añadir nuevo dispositivo** con los parámetros solicitados, incluidos los detalles de identificación del dispositivo, la organización, la red y el grupo de dispositivos al que debe pertenecer y después haga clic en **Siguiente**.
4. Si lo desea, seleccione una imagen de firmware que aplicar al dispositivo. Si elige **Predeterminado** para la imagen, el dispositivo usará la imagen que está designada como predeterminada para la ID de producto cuando el dispositivo se conecte al servidor.
5. Si lo desea, seleccione una configuración que aplicar al dispositivo, junto con la versión de la configuración si existe más de una versión. Si la configuración es una plantilla con marcadores de posición, aparecerá un formulario que solicitará los valores que deben usarse para este dispositivo. Complete estos campos según sea necesario. Si la plantilla hace uso de los parámetros definidos por el sistema, puede marcar la casilla de verificación para mostrar los valores que se utilizarán.
6. Haga clic en **Siguiente** para pasar a la pantalla **Resumen**. Revise los datos introducidos para asegurarse de que sean correctos. También puede revisar la configuración del dispositivo final en la ventana de vista previa de la parte inferior. Cuando haya terminado, haga clic en **Siguiente**.

Para editar un dispositivo existente, siga estos pasos:

1. Acceda a **Plug and Play de red > Dispositivos habilitados**.
2. Marque la casilla de verificación del dispositivo que desea modificar y haga clic en **Editar**. Si lo desea, puede hacer clic en el nombre del dispositivo.
3. Haga clic en **Siguiente** para pasar a la pantalla **Aprovisionar dispositivo**. Cambie la imagen o el archivo de configuración si es necesario y realice cambios en los valores de los parámetros asociados con la configuración.
4. Haga clic en **Siguiente** para pasar a la pantalla **Resumen**. Revise los datos introducidos para asegurarse de que sean correctos. También puede revisar la configuración del dispositivo final en la ventana de vista previa de la parte inferior. Cuando haya terminado, haga clic en **Siguiente**.



Nota Si se modifica la configuración de un archivo de configuración o imagen de un dispositivo que ya se ha provisionado, el estado de ese dispositivo se restablecerá como pendiente y el dispositivo se volverá a provisionar la próxima vez que se registre con Dashboard.

Para eliminar un dispositivo habilitado, siga estos pasos:

1. Acceda a **Plug and Play de red > Dispositivos habilitados**.
2. Marque una o más casillas de verificación para los dispositivos que desee quitar y haga clic en el icono **eliminar**.



Nota Si se elimina un dispositivo habilitado cuando Dashboard lo conoce y el dispositivo está en línea, solo se quitará la configuración de los archivos de configuración e imagen de dicho dispositivo. El dispositivo permanecerá en el inventario de forma similar a cualquier otro dispositivo administrado. Si un dispositivo se conecta posteriormente a Dashboard mediante PnP, se añadirá una nueva entrada a la tabla de dispositivos habilitados.

Dispositivos no reclamados



Nota La página **Dispositivos no reclamados** solo está disponible para los administradores.

Un dispositivo no reclamado es aquel que se ha conectado al servicio, pero no hay ningún registro en el inventario que coincida con el dispositivo. Para ver una lista de dispositivos no reclamados y reclamarlos para poder gestionarlos usando Plug and Play de red, haga lo siguiente:

1. Vaya a **Plug and Play de red > Dispositivos no reclamados** y seleccione la pestaña **No reclamado**.
2. Haga clic en el botón de reclamación del dispositivo que desee administrar.
3. Rellene el formulario Dispositivo no reclamado con los parámetros solicitados, incluidos la organización, la red y el grupo de dispositivos a los que debe pertenecer; después, haga clic en **Siguiente**.
4. Si lo desea, seleccione una imagen de firmware que aplicar al dispositivo. Si elige **Predeterminado** para la imagen, el dispositivo usará la imagen que está designada como predeterminada para la ID de producto cuando el dispositivo se conecte al servidor.
5. También puede seleccionar una configuración que aplicar al dispositivo, junto con la versión de la configuración si existe más de una versión. Si la configuración es una plantilla con marcadores de posición, aparecerá un formulario que solicitará los valores que deben usarse para este dispositivo. Complete estos campos según sea necesario.

Si la plantilla hace uso de los parámetros definidos por el sistema, puede marcar la casilla de verificación para mostrar los valores que se utilizarán.

6. Haga clic en **Siguiente** para pasar a la pantalla **Resumen**. Revise los datos introducidos para asegurarse de que sean correctos. También puede revisar la configuración del dispositivo final en la ventana de vista previa de la parte inferior. Cuando haya terminado, haga clic en **Siguiente**.

Para eliminar un dispositivo de la lista No reclamado sin aprovisionarlo, haga lo siguiente:

1. Vaya a **Plug and Play de red > Dispositivos no reclamados** y seleccione la pestaña **No reclamado**.
2. Haga clic en **Omitir** en el caso del dispositivo que desea eliminar de la lista.

Los dispositivos pasarán a la lista **Omitido** y no se llevarán a cabo más acciones. Para reclamar un dispositivo omitido, haga lo siguiente:

1. Vaya a **Plug and Play de red > Dispositivos no reclamados** y seleccione la pestaña **Omitido**.
2. Haga clic en el botón **No omitir** del dispositivo que desee reclamar.

Los dispositivos pasarán a la lista **No reclamado** y podrá reclamarlos como se ha descrito anteriormente.

Autorreclamación de dispositivos



Nota La página **Auto Claim** (Reclamación automática) solo está disponible para los administradores.

El servidor puede reclamar y aprovisionar automáticamente los dispositivos no reclamados creando una regla de autorreclamación para ese ID de producto. Para crear una regla de autorreclamación, haga lo siguiente:

1. Vaya a **Plug and Play de red > Dispositivos autorreclamados**.
2. Haga clic en el icono **+** (más) para crear una nueva regla de **autorreclamación**.
3. Rellene el formulario Reclamación automática de dispositivo con los parámetros solicitados, incluida la ID del producto (PID) que se asociará y la organización, la red y el grupo de dispositivos a los que debe pertenecer el dispositivo que se acaba de reclamar; después, haga clic en **Siguiente**.
4. Si lo desea, seleccione una imagen de firmware que aplicar al dispositivo. Si elige **Predeterminado** para la imagen, el dispositivo usará la imagen que está designada como predeterminada para la ID de producto cuando el dispositivo se conecte al servidor.
5. También puede seleccionar una configuración que aplicar al dispositivo, junto con la versión de la configuración si existe más de una versión. Si la configuración es una plantilla con marcadores de posición, aparecerá un formulario que solicitará los valores que deben usarse para este dispositivo. Complete estos campos según sea necesario.

Si la plantilla hace uso de los parámetros definidos por el sistema, puede marcar la casilla de verificación para mostrar los valores que se utilizarán.
6. Haga clic en **Siguiente** para pasar a la pantalla **Resumen**. Revise los datos introducidos para asegurarse de que sean correctos. También puede revisar la configuración del dispositivo final en la ventana de vista previa de la parte inferior. Cuando haya terminado, haga clic en **Siguiente**.

Los nuevos dispositivos que no estén presentes en el inventario se cotejarán con la lista de reglas de autorreclamación. Si se da una coincidencia, se creará un nuevo registro del dispositivo en el inventario con la imagen y el archivo de configuración definidos por la regla de **autorreclamación**. Después, el dispositivo se aprovisionará como corresponda. Si el dispositivo no coincide con una regla de **autorreclamación**, se agregará a la lista No reclamado y no se llevarán a cabo más acciones.

Imágenes de firmware de dispositivos

La página **Imágenes** permite cargar imágenes de firmware que después pueden implementarse en los dispositivos. Las imágenes de firmware pueden designarse como imagen predeterminada para diferentes plataformas, lo que permite actualizar el firmware en toda una familia de dispositivos de forma muy sencilla. Las imágenes de firmware son específicas de una organización y solo pueden utilizarse con dispositivos de aprovisionamiento asociados a la misma organización.

Para cargar una imagen de firmware, haga lo siguiente:

1. Vaya a **Plug and Play de red > Imágenes**.
2. Haga clic en el icono **+** (más).
3. Seleccione la organización de la imagen en el menú desplegable.
4. Arrastre una imagen de firmware desde su PC y suéltela en la zona de destino de la ventana **Cargar archivo**. También puede hacer clic en la zona de destino y seleccionar una imagen de firmware para cargarla.
5. Haga clic en **Cargar**.

Puede designar una imagen como imagen predeterminada para uno o varios tipos de dispositivo. Para designar una imagen como imagen predeterminada, haga lo siguiente:

1. Vaya a **Plug and Play de red > Imágenes**.
2. Seleccione el botón de opción de la imagen en la tabla **Imágenes** y haga clic en **Editar**.
3. Introduzca una lista de ID de producto separados por comas en el campo **Imagen predeterminada para los id. de productos**. Los ID de producto pueden contener caracteres comodín “?”, que representa un único carácter, y “*”, que representa una cadena de caracteres.
4. Haga clic en **Guardar**.

Para eliminar una imagen, haga lo siguiente:

1. Vaya a **Plug and Play de red > Imágenes**.
2. Seleccione el botón de opción de la imagen que desea eliminar y haga clic en **Eliminar**.

Archivos de configuración de dispositivos

La página Configuraciones permite cargar o crear archivos de configuración que después pueden implementarse en los dispositivos. Los archivos de configuración son específicos de una organización y solo pueden utilizarse con dispositivos de aprovisionamiento asociados a la misma organización.

Los archivos de configuración pueden ser archivos de texto sencillos o pueden contener marcadores de posición y metadatos asociados para permitir que el mismo archivo de configuración se use con varios dispositivos, a la vez que permite que los parámetros únicos se establezcan en un dispositivo por dispositivo. Por ejemplo, una sola plantilla de configuración se podría aplicar a varios dispositivos, pero permitir que el nombre de host se especifique individualmente para cada dispositivo. Para obtener más detalles sobre las plantillas de configuración, consulte [Administración de plantillas de configuración](#) en el Apéndice A.

Se incluye una selección de plantillas de configuración para diferentes tipos de dispositivos con la aplicación Dashboard. Estas plantillas pueden utilizarse tal cual o pueden modificarse o copiarse y utilizarse como base para nuevas plantillas.

Para crear una nueva configuración manualmente, haga lo siguiente:

1. Vaya a **Plug and Play de red > Configuraciones**.
2. Haga clic en el icono **+** (más).
3. El editor de plantillas se abre con un área en blanco para la configuración a la izquierda y un formulario a la derecha para administrar los metadatos asociados con la plantilla.

Introduzca un nombre para la configuración en el campo en la esquina superior izquierda. Seleccione una organización e ingrese una lista separada por comas de ID de productos que admitan esta configuración en los campos de la derecha. Si lo desea, puede introducir una descripción. Los ID de producto pueden contener caracteres comodín "?", que representa un único carácter, y "*", que representa una cadena de caracteres.

4. Cree la configuración escribiendo o pegando texto en el área de texto a la izquierda. Si es necesario, realice los cambios correspondientes en los metadatos mediante los controles de la derecha. Para obtener más detalles sobre la sintaxis y los metadatos de la plantilla, consulte [Administración de plantillas de configuración](#).

Puede utilizar el botón **Vista previa** para ver cómo aparecerá la plantilla de configuración cuando esté asignada a un dispositivo.

5. Cuando esté conforme con la configuración, haga clic en **Guardar**.

Para cargar un archivo de configuración, haga lo siguiente:

1. Vaya a **Plug and Play de red > Configuraciones**.
2. Haga clic en el icono **Cargar**.
3. Seleccione la organización de la configuración en el menú desplegable. Escriba un nombre para la configuración y, opcionalmente, añada una descripción.
4. Arrastre un archivo de configuración desde su PC y suéltelo en la zona de destino de la ventana **Cargar archivo**. También puede hacer clic en la zona de destino y seleccionar un archivo de configuración para cargarlo.
5. Haga clic en **Cargar**.

Si lo desea, puede hacer clic en el nombre del archivo de configuración cargado para ver el contenido en el editor de plantillas.

Para eliminar una configuración, haga lo siguiente:

1. Vaya a **Plug and Play de red > Configuraciones**.
2. Marque una o más casillas de verificación para las configuraciones que desee quitar y haga clic en el icono **eliminar**.

Gestión de configuraciones

La página de configuración de Plug and Play de red permite controlar la operación del protocolo de dicho servicio. El **Check In Time Interval** (Intervalo de comprobación) controla la frecuencia con la que un dispositivo se conecta al servicio Plug and Play de red tras el aprovisionamiento inicial. Para modificar este parámetro, haga lo siguiente:

1. Vaya a **Plug and Play de red > Configuración**.

2. Introduzca en el campo provisto el intervalo deseado entre conexiones. El tiempo se expresa en minutos y el valor predeterminado es 2880 minutos (dos días).
3. Haga clic en **Guardar**.

El **Check In Time Interval** (Intervalo de comprobación) se establece para el sistema en su conjunto, pero se puede anular en el nivel de organización. Si no se define ningún intervalo para la organización, se utiliza el valor del sistema.

Configuración del certificado

El certificado que Cisco Business Dashboard genera automáticamente durante el primer inicio es un certificado autofirmado. En la mayoría de los casos, esto no bastará para que el cliente de Plug and Play de red acepte el certificado; será necesario generar uno nuevo. Al generar un nuevo certificado autofirmado o una solicitud de firma de certificado (CSR), Dashboard incluirá el contenido del campo **Nombre común** en el campo **Nombre alternativo del asunto**, además de los valores especificados en el campo **Nombre alternativo del asunto** en la GUI.

Para obtener más información sobre cómo configurar el certificado de Dashboard, consulte [Gestión de certificados, en la página 82](#).

Supervisión de Plug and Play de red

Todos los dispositivos conocidos del servicio Plug and Play de red se muestran en las páginas **Dispositivos activados** o **Dispositivos no reclamados** con su respectivo estado. Este estado también se puede ver en la página **Inventario**. Para ello, se debe habilitar la visualización de la columna **PnP Status** (Estado de PnP). El campo de estado muestra el estado actual del dispositivo y contiene uno de los valores enumerados en la siguiente tabla. Haciendo clic en el campo de estado puede ver más detalles, entre ellos un historial de los cambios de estado de este dispositivo a lo largo del tiempo.

Tabla 16: Plug and Play de red - Estado de los dispositivos

Estado	Descripción
PENDIENTE	El dispositivo está definido pero no se ha conectado al servicio.
APROVISIONAMIENTO	El dispositivo ha realizado la conexión inicial al servicio.
APROVISIONANDO_IMAGEN	Se está aplicando una imagen de firmware al dispositivo.
APROVISIONADO_IMAGEN_REINICIANDO	Se está reiniciando el dispositivo para ejecutar el nuevo firmware.
APROVISIONADO_IMAGEN	El nuevo firmware se ha aplicado correctamente.
APROVISIONANDO_CONFIG	Se está aplicando un archivo de configuración al dispositivo.

Estado	Descripción
APROVISIONADO_CONFIG	Se ha aplicado correctamente el archivo de configuración al dispositivo. En función del tipo de dispositivo, este puede reiniciarse para aplicar la configuración.
ERROR	Se ha producido un error. Compruebe los archivos de registro para obtener más detalles.
APROVISIONADO	Se ha completado el proceso de aprovisionamiento del dispositivo.



CAPÍTULO 9

Registro de eventos

Este capítulo contiene las siguientes secciones:

- [Acerca del registro de eventos, en la página 57](#)

Acerca del registro de eventos

El Registro de eventos proporciona una interfaz de búsqueda y clasificación de los eventos generados a través de la red. Puede usar los controles de filtrado para limitar los eventos mostrados en función de cualquier combinación de estos parámetros:

- **Hora:** especifique las horas de inicio y fin del periodo deseado. Solo se mostrarán los eventos sucedidos en este intervalo.
- **Gravedad:** seleccione el nivel de gravedad de los eventos que desea que se muestren. También puede marcar la casilla *Mayor* para incluir eventos con un nivel de gravedad mayor.
- **Tipo:** seleccione uno o varios tipos de eventos que mostrar. Los tipos se disponen en una estructura de árbol y, al seleccionar uno, se incluyen automáticamente todos los tipos incluidos debajo en el árbol.
- **Red:** seleccione una o varias redes cuyos eventos desee mostrar. A medida que escriba se mostrarán los sitios que coincidan.
- **Dispositivo:** seleccione uno o varios dispositivos cuyos eventos desee mostrar. A medida que escriba se mostrarán los dispositivos que coincidan. Puede indicar dispositivos por nombre, dirección IP o dirección MAC.

Los eventos que reúnan las condiciones de filtrado se mostrarán en la tabla de debajo. La tabla puede organizarse haciendo clic en los encabezados de columna.



CAPÍTULO 10

Informes

Este capítulo contiene las siguientes secciones:

- [Acerca de Informes, en la página 59](#)
- [Visualización del Informe de ciclo de vida, en la página 59](#)
- [Vista del informe de final de ciclo de vida útil, en la página 60](#)
- [Visualización del informe de mantenimiento, en la página 62](#)
- [Vista del informe de red inalámbrica, en la página 62](#)
- [Vista del informe de clientes inalámbricos, en la página 65](#)

Acerca de Informes

La opción **Informes** de Cisco Business Dashboard ofrece una serie de informes sobre la red. Entre los informes, se incluyen los siguientes:

- **Informe de ciclo de vida:** proporciona un resumen del estado de ciclo de vida de los dispositivos de la red.
- **Informe de final de ciclo de vida útil:** muestra los dispositivos que tengan publicado un boletín de final del ciclo de vida útil.
- **Informe de mantenimiento:** muestra una lista con todos los dispositivos, junto con su estado de garantía, e indica si el dispositivo tiene un contrato de soporte activo.
- **Red inalámbrica:** muestra información sobre el entorno inalámbrico, incluidos SSID, puntos de acceso y uso del espectro.
- **Cliente inalámbrico:** muestra detalles sobre los clientes inalámbricos vistos en la red.

Visualización del Informe de ciclo de vida

El **Informe de ciclo de vida** proporciona una vista general sobre el estado de los dispositivos de red, teniendo en cuenta el estado del ciclo de vida del software y el hardware. En la siguiente tabla, se describe la información que se proporciona:

Tabla 17: Informe de ciclo de vida

Campo	Descripción
Número de red	El nombre de la red en la que se encuentra el dispositivo.
Organización	La organización a la que pertenece el dispositivo.
Nombre de host	Nombre de host del dispositivo.
Tipo de appliance	El tipo de dispositivo.
Modelo	El número de modelo del dispositivo.
Semana de fabricación	La fecha de fabricación del dispositivo, que se muestra como número de semana y año.
Actualiz. de firmware disp.	Muestra cuál es la versión del firmware más reciente que está disponible para el dispositivo. También puede indicar que el firmware del dispositivo está actualizado.
Versión del firmware	Muestra la versión del firmware que se está ejecutando actualmente en el dispositivo.
Estado de fin de vida	Especifica si se ha publicado un boletín de final del ciclo de vida útil para el dispositivo y la próxima fecha importante en el proceso de final del ciclo de vida útil.
Estado de mantenimiento	Especifica si el dispositivo está actualmente en garantía bajo un contrato de soporte.

Si una fila de la tabla de un dispositivo requiere atención, aparecerá en color rojo para indicar la urgencia. Por ejemplo, un dispositivo con un boletín de final del ciclo de vida útil publicado aparecerá en color naranja si la fecha de finalización de soporte no se ha alcanzado todavía. Si el dispositivo ya no recibe soporte de Cisco, aparecerá en rojo.

El cuadro Buscar, situado en la parte superior del informe, se puede usar para filtrar los resultados. Escriba el texto que desee en el cuadro Buscar para limitar el número de entradas que se muestran con el texto coincidente. Los resultados pueden limitarse a una organización específica mediante el menú desplegable Organización.

El icono de selección de columna, ubicado en la parte superior izquierda del informe, se puede usar para personalizar la información mostrada. Haga clic en el icono y use las casillas que aparecen para seleccionar las columnas que desee incluir en el informe.

Vista del informe de final de ciclo de vida útil

El **Informe de final de ciclo de vida útil** muestra una lista con los dispositivos que tienen un boletín de **Final del ciclo de vida útil** publicado junto con las fechas claves de dicho proceso. Asimismo, informa sobre la plataforma de sustitución recomendada. En la siguiente tabla, se describe la información que se proporciona:

Tabla 18: Informe de final de ciclo de vida útil

Campo	Descripción
Número de red	El nombre de la red en la que se encuentra el dispositivo.
Organización	La organización a la que pertenece el dispositivo.
ID de producto	Id. de producto o número de referencia del dispositivo.
Nombre de host	Nombre de host del dispositivo.
Tipo de appliance	El tipo de dispositivo.
Estado actual	Estado del proceso de final del ciclo de vida útil del producto
Fecha de anuncio	Fecha en que se publicó el boletín de final del ciclo de vida útil.
Fecha límite de venta	Fecha tras la cual Cisco ya no venderá el producto.
Fecha límite de versiones del software	Fecha tras la cual no se lanzarán más versiones de software para el producto.
Fecha límite de nuevo contrato de servicio	Fecha final para firmar un nuevo contrato de soporte para el dispositivo.
Fecha límite de renovación de servicio	Fecha final para renovar un contrato de soporte existente para el dispositivo.
Fecha final de soporte técnico	Fecha tras la cual Cisco no proporcionará ningún soporte para el producto.
Sustitución recomendada	Producto de sustitución recomendado.
Boletín de producto	Número del boletín de productos y enlace al boletín en el sitio web de Cisco.

Cada fila de la tabla está codificada con un color para indicar el estado del proceso de final del ciclo de vida útil del dispositivo. Por ejemplo, si un dispositivo ha pasado ya la Fecha límite de venta, pero todavía no ha alcanzado la Fecha límite de soporte, tendrá el color naranja. Si ha pasado también la Fecha límite de soporte, tendrá el color rojo.

El cuadro Buscar, situado en la parte superior del informe, se puede usar para filtrar los resultados. Escriba el texto que desee en el cuadro Buscar para limitar el número de entradas que se muestran con el texto coincidente. Los resultados pueden limitarse a una organización específica mediante el menú desplegable Organización.

El icono de selección de columna, ubicado en la parte superior izquierda del informe, se puede usar para personalizar la información mostrada. Haga clic en el icono y use las casillas que aparecen para seleccionar las columnas que desee incluir en el informe.

Visualización del informe de mantenimiento

En el **Informe de mantenimiento** aparecen todos los dispositivos de red con información sobre el estado del contrato de soporte y la garantía respectiva. En la siguiente tabla, se describe la información que se proporciona:

Tabla 19: Informe de mantenimiento

Campo	Descripción
Número de red	El nombre de la red en la que se encuentra el dispositivo.
Organización	La organización a la que pertenece el dispositivo.
Nombre de host	Nombre de host del dispositivo.
Tipo de appliance	El tipo de dispositivo.
Modelo	Número de modelo del dispositivo.
Número de serie	Número de serie del dispositivo.
Estado	Estado de soporte actual del dispositivo.
Fecha de finalización de la cobertura	Fecha en la que caducará el contrato de soporte actual.
Fecha de finalización de la garantía	Fecha en la que caducará la garantía del dispositivo.

Cada fila de la tabla está codificada con un color para indicar el estado de soporte del dispositivo. Por ejemplo, si el dispositivo se está aproximando a la fecha de caducidad del contrato de soporte o de la garantía, aparecerá de color naranja. Si el dispositivo está fuera de garantía y no cuenta con un contrato de soporte, aparecerá en rojo.

El cuadro Buscar, situado en la parte superior del informe, se puede usar para filtrar los resultados. Escriba el texto que desee en el cuadro Buscar para limitar el número de entradas que se muestran con el texto coincidente. Los resultados pueden limitarse a una organización específica mediante el menú desplegable Organización.

El icono de selección de columna, ubicado en la parte superior izquierda del informe, se puede usar para personalizar la información mostrada. Haga clic en el icono y use las casillas que aparecen para seleccionar las columnas que desee incluir en el informe.

Vista del informe de red inalámbrica

El **Informe de red inalámbrica** muestra detalles sobre la red inalámbrica clasificados por SSID, uso del espectro inalámbrico y punto de acceso e incluye una lista de puntos de acceso fraudulentos detectados. Los informes pueden generarse por intervalos de tiempo, desde diariamente hasta anualmente, usando los controles de la parte superior de la página.

Varios de los conjuntos de datos incluyen un gráfico donde figura un desglose a lo largo del tiempo de la fila seleccionada. Puede hacer clic en las etiquetas de la leyenda del gráfico para cambiar la visualización de cada conjunto de datos.

En la siguiente tabla, se describe la información que se proporciona en las distintas secciones del informe:

Tabla 20: Informe de red inalámbrica

Campo	Descripción
Tabla de redes inalámbricas	
SSID	El nombre de la red inalámbrica.
Red (oculto de forma predeterminada)	La red en la que se encuentra el SSID.
Organización (oculto de forma predeterminada)	La organización a la que pertenece el SSID.
Invitado	Si el SSID está configurado o no para acceso de invitados.
Seguridad	El método de seguridad configurado para el SSID.
Recuento de clientes (máximo)	El máximo número de clientes asociados al SSID durante el periodo abarcado por el informe.
Recuento de clientes (media)	El promedio de clientes asociados al SSID durante el periodo abarcado por el informe.
Tráfico (máximo)	La máxima tasa de tráfico total en el SSID durante el periodo abarcado por el informe.
Tráfico (media)	La media de la tasa de tráfico total en el SSID durante el periodo abarcado por el informe.
Tabla de uso del espectro	
Radiofrecuencia	La banda de radiofrecuencia usada (2,4 GHz o 5 GHz).
Segmentación	La red a la que se refieren los datos de uso del espectro visualizados.
Organización	La organización a la que se refieren los datos de uso del espectro.
Recuento de clientes (máximo)	El máximo número de clientes que usaron la banda de frecuencia durante el periodo abarcado por el informe.
Recuento de clientes (media)	El promedio de clientes que usaron la banda de frecuencia durante el periodo abarcado por el informe.
Tráfico (máximo)	La máxima tasa de tráfico total en la banda de frecuencia durante el periodo abarcado por el informe.
Tráfico (media)	La media de la tasa de tráfico total en la banda de frecuencia durante el periodo abarcado por el informe.
Tabla de puntos de acceso inalámbricos	
Punto de acceso	El nombre del punto de acceso.

Campo	Descripción
Red (oculto de forma predeterminada)	La red en la que se encuentra el punto de acceso.
Organización (oculto de forma predeterminada)	La organización a la que pertenece el punto de acceso.
Modelo	El modelo del punto de acceso.
Versión	La versión de firmware del punto de acceso.
Recuento de clientes (máximo)	El máximo número de clientes asociados al punto de acceso durante el periodo abarcado por el informe.
Recuento de clientes (media)	El promedio de clientes asociados al punto de acceso durante el periodo abarcado por el informe.
Tráfico (máximo)	La máxima tasa de tráfico total en el punto de acceso durante el periodo abarcado por el informe.
Tráfico (media)	La media de la tasa de tráfico total en el punto de acceso durante el periodo abarcado por el informe.
Tabla de puntos de acceso fraudulentos	
SSID	El SSID detectado.
Red (oculto de forma predeterminada)	La red en la que se encuentra el punto de acceso de detección.
Organización (oculto de forma predeterminada)	La organización a la que pertenece el punto de acceso de detección.
MAC	La dirección MAC del punto de acceso fraudulento.
Visto por primera vez	La hora a la que se detectó el punto de acceso fraudulento por primera vez.
Visto por última vez	La hora a la que se detectó el punto de acceso fraudulento por última vez.
Tiempo total de visibilidad	El tiempo total de conexión del punto de acceso fraudulento.
CANAL	El canal inalámbrico usado por el punto de acceso fraudulento.
Intensidad media de la señal	La intensidad media de la señal del punto de acceso fraudulento observada por el punto de acceso que lo detectó.
Visto por	Los puntos de acceso que detectó el punto de acceso fraudulento.

Vista del informe de clientes inalámbricos

El **Informe de clientes inalámbricos** muestra detalles sobre los clientes inalámbricos de la red. Los informes pueden generarse por intervalos de tiempo, desde diariamente hasta anualmente, usando los controles de la parte superior de la página.

Cada conjunto de datos incluye gráficos donde figura un desglose a lo largo del tiempo de la fila seleccionada. Puede hacer clic en las etiquetas de la leyenda del gráfico para cambiar la visualización de cada conjunto de datos.

En la siguiente tabla, se describe la información que se proporciona:

Tabla 21: Tabla de clientes inalámbricos

Tabla de clientes inalámbricos	
MAC	La dirección MAC del cliente.
Nombre de host	El nombre de host del cliente, si está disponible.
Organización	La organización en la que se detectó el cliente por última vez.
Segmentación	La red donde se detectó el cliente por última vez.
SSID	El SSID al que el cliente estuvo asociado por última vez.
Tipo 802.11	La variante 802.11 usada por el cliente.
Frecuencia	La banda de frecuencia usada por el cliente.
Velocidad de datos máxima	La máxima velocidad de datos usada por el cliente.
Cargar	El volumen de datos cargados por el cliente.
Descargar	El volumen de datos descargados por el cliente.
Total	El volumen total de datos enviados y recibidos por el cliente.
Visto por primera vez	La hora a la que se detectó el cliente por primera vez.
Visto por última vez	La hora a la que se detectó el cliente por última vez.
Tiempo de conexión	El tiempo total de conexión del cliente.
Porcentaje de tiempo de conexión	El porcentaje de tiempo de conexión del cliente respecto de todo el tiempo durante el cual el cliente ha sido detectado por la red.

Tabla 22: Tabla de invitados inalámbricos

Tabla de invitados inalámbricos	
MAC	La dirección MAC del cliente.
Nombre de host	El nombre de host del cliente, si está disponible.

Tabla de invitados inalámbricos	
Nombre del usuario	El nombre de usuario introducido por el cliente en el portal invitado.
Organización	La organización en la que se detectó el cliente por última vez.
Segmentación	La red donde se detectó el cliente por última vez.
SSID	El SSID al que el cliente estuvo asociado por última vez.
Tipo 802.11	La variante 802.11 usada por el cliente.
Frecuencia	La banda de frecuencia usada por el cliente.
Velocidad de datos máxima	La máxima velocidad de datos usada por el cliente.
Cargar	El volumen de datos cargados por el cliente.
Descargar	El volumen de datos descargados por el cliente.
Total	El volumen total de datos enviados y recibidos por el cliente.
Visto por primera vez	La hora a la que se detectó el cliente por primera vez.
Visto por última vez	La hora a la que se detectó el cliente por última vez.
Tiempo de conexión	El tiempo total de conexión del cliente.
Porcentaje de tiempo de conexión	El porcentaje de tiempo de conexión del cliente respecto de todo el tiempo durante el cual el cliente ha sido detectado por la red.



Nota

Las marcas de tiempo **Visto por primera vez** y **Visto por última vez** representan la hora notificada por el punto de acceso. Se recomienda que todos los dispositivos de red implementen la sincronización del reloj mediante un mecanismo como el protocolo de tiempo de red (NTP).



CAPÍTULO 11

Administración

Este capítulo contiene las siguientes secciones:

- [Acerca de Administración](#), en la página 67
- [Administración de las organizaciones](#), en la página 68
- [Administración de grupos de dispositivos](#), en la página 70
- [Administración de las credenciales del dispositivo](#), en la página 71
- [Cómo gestionar los usuarios](#), en la página 72
- [Cambio de los valores predeterminados de supervisión](#), en la página 75
- [Administración de los perfiles de supervisión](#), en la página 76
- [Visualización de los intentos de inicio de sesión](#), en la página 78
- [Administración de la configuración de los informes](#), en la página 78

Acerca de Administración

La opción **Administración** de Cisco Business Dashboard permite controlar el funcionamiento de la aplicación en el nivel de organización. Esta opción se divide en las siguientes páginas:

- **Organizaciones:** permite crear organizaciones y mantenerlas en Cisco Business Dashboard.
- **Grupos de dispositivos:** permite organizar los dispositivos de red en grupos para facilitar su administración.
- **Credenciales del dispositivo:** permite especificar las credenciales que se deben usar para acceder a los dispositivos de red.
- **Usuarios:** permite definir el acceso de los usuarios a Cisco Business Dashboard.
- **Valores predeterminados de notificación:** permite cambiar el comportamiento predeterminado de las notificaciones de Cisco Business Dashboard.
- **Intentos de inicio de sesión:** proporciona un registro del acceso de todos los usuarios a Cisco Business Dashboard.
- **Configuración de informes:** permite cambiar la configuración que controla la forma en que se generan los informes.

No todas las páginas están visibles para todas las funciones. Los operadores no pueden administrar la configuración de los usuarios. Las páginas **Valores predeterminados de notificación** y **Configuración de informes** solo están visibles para los administradores.

Administración de las organizaciones

En Cisco Business Dashboard, las organizaciones se emplean para dividir redes, usuarios y dispositivos en grupos que normalmente se administran por separado. Cada red o dispositivo pertenece a una organización y cada usuario puede administrar una o más organizaciones. Una organización puede representar a un cliente, un departamento o una región, lo que resulte más adecuado para su empresa; no obstante, en todos los casos, el uso de las organizaciones posibilita un control más granular sobre quién puede ver y administrar las distintas partes de la red. Cuando se instala Cisco Business Dashboard, se crea una sola organización de forma predeterminada.

Creación de una nueva organización

Para crear una nueva organización, siga estos pasos:

1. Acceda a **Administración > Organizaciones**.
2. Haga clic en el icono **+** (más) situado en la parte superior de la tabla.
3. Especifique un nombre para la organización e introduzca los detalles necesarios.
4. Escriba un nombre para un nuevo grupo de dispositivos que deberá convertirse en el predeterminado para los dispositivos recién detectados. El nuevo grupo de dispositivos se creará junto con la organización.
5. Haga clic en **Guardar**.
6. Repita los pasos anteriores con cada organización que desee crear.

Modificación de una organización existente

Para modificar una organización, haga lo siguiente:

1. Acceda a **Administración > Organizaciones**.
2. Seleccione el botón de opción de la organización que desea modificar y haga clic en el icono **Editar**.
3. Realice los cambios oportunos y haga clic en **Guardar**.

Eliminación de una organización

Para eliminar una organización, siga estos pasos:

1. Acceda a **Administración > Organizaciones**.
2. Seleccione el botón de opción de la organización que desea modificar y haga clic en el icono **Eliminar**.

Administración de los perfiles de supervisión para una organización

Los perfiles de supervisión le permiten controlar cómo la supervisión de dispositivos se realiza en toda la organización. Los perfiles seleccionados a nivel de organización también afectarán a todas las redes que se encuentren en ella.

Para cambiar los perfiles de supervisión de una organización, haga lo siguiente:

1. Acceda a **Administración > Organizaciones**.
2. Haga clic en el nombre de la organización que desea modificar y seleccione la pestaña **Perfiles de supervisión**.
3. Utilice los menús desplegables para seleccionar el perfil de supervisión adecuado que se aplicará a los dispositivos del tipo correspondiente. Consulte [Administración de los perfiles de supervisión, en la página 76](#) para obtener más información sobre la creación de perfiles de supervisión.

También puede optar por seguir el comportamiento definido en el nivel de sistema. Para ello, marque las casillas de verificación **Valores predeterminados de supervisión** para los tipos de dispositivos concretos para toda la organización.

4. Haga clic en **Guardar**.



Nota Consulte [Administración de los perfiles de supervisión](#) para obtener más información sobre los tipos de supervisión que se pueden llevar a cabo y cómo administrarlos. Consulte [Cambio de los valores predeterminados de supervisión, en la página 75](#) para obtener más información sobre el cambio de los perfiles de supervisión a nivel de sistema.

Administración de usuarios asociados a una organización

Los usuarios con la función **Administrador de la organización** u otra inferior deben asociarse explícitamente a una organización para poder ver o administrar los dispositivos que se encuentren en ella.

Para asociar un usuario a la organización, siga estos pasos:

1. Acceda a **Administración > Organizaciones**.
2. Haga clic en el nombre de la organización que desea modificar y seleccione la pestaña **Usuarios**.
3. Haga clic en el icono **+** (más). Seleccione un usuario de la lista desplegable.



Nota Los usuarios del nivel **Administrador** están asociados implícitamente a todas las organizaciones y no aparecerán en la lista desplegable.

Para eliminar un usuario de la organización, realice lo siguiente:

1. Acceda a **Administración > Organizaciones**.
2. Haga clic en el nombre de la organización que desea modificar y seleccione la pestaña **Usuarios**.
3. Haga clic en el icono **Eliminar** situado junto al usuario en la tabla.

Administración de redes asociadas a una organización

Cada red de Cisco Business Dashboard pertenece a una sola organización. Para ver una lista de las redes asociadas a una organización, seleccione la pestaña **Redes** en la página **Organization Detail** (Detalles de la organización).

La asociación de una red a una organización se realiza cuando se crea la red. Para cambiar la organización a la que está asociada una red, siga estos pasos:

1. Acceda a **Red** y seleccione la red que desea cambiar. Haga clic en **Más** para mostrar el panel **Network Detail** (Detalles de la red).
2. Haga clic en el icono **Editar** situado junto al nombre de la red.
3. Seleccione la nueva organización de la lista desplegable.
4. Haga clic en **Aceptar**.

Puede crear nuevas redes para una organización desde esta vista. Haga clic en el icono **+** (más) para crear una nueva red y rellene los valores correspondientes en el formulario que aparezca.

Administración de grupos de dispositivos

Cisco Business Dashboard usa grupos de dispositivos para llevar a cabo la mayoría de las tareas de configuración. Se agrupan varios dispositivos de red para poder configurarlos en una única acción.

Cada grupo de dispositivos puede incluir dispositivos de varios tipos. Cuando una configuración se aplica a un grupo de dispositivos, esta solo se aplica a los dispositivos del grupo que admitan esa función. Por ejemplo, si un grupo de dispositivos contiene routers, conmutadores y puntos de acceso inalámbricos, la configuración para un nuevo SSID inalámbrico se aplicará a los puntos de acceso inalámbricos, no se aplicará a los conmutadores y se aplicará a los routers solo si son inalámbricos.

Los grupos de dispositivos pueden incluir dispositivos de varias redes, pero todos ellos deben pertenecer a una sola organización. Un grupo de dispositivos puede designarse como el grupo predeterminado de una organización o red; los dispositivos recién detectados de esa red u organización se ubicarán en el grupo de dispositivos predeterminado.

Creación de un nuevo grupo de dispositivos

Para crear un nuevo grupo de dispositivos, haga lo siguiente:

1. Acceda a **Administración > Grupos de dispositivos**.
2. Haga clic en el icono **+** (más) para crear un grupo nuevo.
3. Introduzca una organización, un nombre y una descripción para el grupo. Haga clic en **Guardar**.
4. De manera opcional, puede añadir dispositivos al grupo haciendo clic en el icono **+** (más) y usando el cuadro de búsqueda para seleccionar los dispositivos que deben agregarse. Puede añadir dispositivos de forma individual o por red. Si el dispositivo seleccionado ya es miembro de un grupo diferente, se eliminará de dicho grupo. Los dispositivos deben pertenecer a un único grupo.

Modificación del grupo de dispositivos

Para modificar un grupo de dispositivos existente, haga lo siguiente:

1. Acceda a **Administración > Grupos de dispositivos**.
2. Seleccione el botón de opción situado junto al grupo que desea cambiar y haga clic en el icono **Editar**.
3. Cambie el nombre y la descripción si es necesario. Haga clic en **Guardar**.

4. Agregue dispositivos al grupo o elimínelos de este según se requiera. Para eliminar un dispositivo que se haya agregado previamente al grupo, haga clic en el icono **Papelera de reciclaje** situado junto al dispositivo. El dispositivo pasará a formar parte del grupo **Predeterminado** de la red u organización.



Nota No es posible eliminar los dispositivos del grupo **Predeterminado**. Para eliminar un dispositivo del grupo **Predeterminado**, deberá asignarlo a un grupo nuevo.

Eliminación de un grupo de dispositivos

Para eliminar un grupo de dispositivos, haga lo siguiente:

1. Acceda a **Administración > Grupos de dispositivos**.
2. Haga clic en el botón de opción para que se elimine el grupo de dispositivos y, a continuación, en el icono **Eliminar**.



Nota El grupo **Predeterminado** no se puede eliminar.

Administración de las credenciales del dispositivo

Para que Cisco Business Dashboard detecte y administre la red por completo, debe tener credenciales de autenticación para los dispositivos de red. Cuando un dispositivo se detecte por primera vez, Probe intentará autenticarse con el dispositivo usando el nombre de usuario predeterminado (`cisco`), la contraseña predeterminada (`cisco`) y la comunidad SNMP predeterminada (`public`). Si se produce un fallo, se generará una notificación y el usuario deberá proporcionar credenciales válidas. Para suministrar credenciales válidas, haga lo siguiente:

1. Acceda a **Administración > Credenciales del dispositivo**. En la primera tabla de esta página, aparecen todos los dispositivos detectados que requieren credenciales.
2. Especifique credenciales válidas en algunos de los campos **Nombre de usuario/Contraseña**, **Comunidad SNMP** y **SNMPv3** (o en todos ellos). Puede hacer clic en el icono **+** (más) situado junto al campo correspondiente para introducir hasta tres credenciales de cada tipo. Las contraseñas deben especificarse como texto sin formato.



Nota En el caso de las credenciales **SNMPv3**, los protocolos de autenticación son Ninguno, MD5, y SHA. Los protocolos de cifrado admitidos son Ninguno, DES y AES.

3. Haga clic en **Apply** (Aplicar). Probe probará cada credencial con cada uno de los dispositivos que requieran ese tipo de credencial. Si la credencial es válida, se almacenará para usarla posteriormente en el dispositivo.
4. Repita los pasos del 2 al 3 las veces que sea necesario hasta que cada dispositivo tenga almacenadas unas credenciales válidas.

Para especificar una única credencial para un dispositivo específico, haga lo siguiente:

1. Haga clic en el icono **Editar** que aparece junto al dispositivo en la tabla de dispositivos detectados. Aparecerá una ventana emergente en la que se le solicita que especifique las credenciales que correspondan al tipo de credencial seleccionado.
2. Especifique un nombre de usuario y una contraseña o una credencial de SNMP en los campos correspondientes.
3. Haga clic en **Apply** (Aplicar). Para cerrar la ventana sin aplicar los cambios, haga clic en ✕, en la esquina superior derecha de la ventana emergente.

Debajo de la sección **Agregar nuevas credenciales**, encontrará una tabla que muestra la identidad de cada dispositivo para el que Probe tiene credenciales válidas almacenadas, junto con la hora en la que se usó la credencial por última vez. Para ver las credenciales almacenadas de un dispositivo, puede hacer clic en el icono **Mostrar contraseña** ubicado junto al dispositivo. Para ocultar las credenciales de nuevo, haga clic en el icono **Ocultar contraseña**. También puede mostrar y ocultar las credenciales de todos los dispositivos mediante el botón situado en la parte superior de la tabla. También puede eliminar credenciales que ya no sean necesarias. Para eliminar credenciales almacenadas, haga lo siguiente:

1. Acceda a **Administración > Credenciales del dispositivo**.
2. En la tabla **Credenciales guardadas**, seleccione la casilla situada junto a uno o varios conjuntos de credenciales para eliminarlos. También puede seleccionar la casilla situada en la parte superior de la tabla para seleccionar todas las credenciales.
3. Haga clic en **Eliminar las credenciales seleccionadas**.

Para eliminar las credenciales de un solo dispositivo, también puede hacer clic en el icono **Eliminar**, ubicado junto al dispositivo.

Cómo gestionar los usuarios

La página **Administración de usuarios** permite controlar cómo se les puede conceder a los usuarios acceso a Cisco Business Dashboard. También permite cambiar ajustes que afectan al modo en que dichos usuarios interactúan con Dashboard.

Cisco Business Dashboard admite cuatro tipos de usuarios:

- **Administrador**: los administradores tienen acceso total a las funciones de Dashboard, incluida la capacidad de mantener el sistema.
- **Administrador de la organización**: los administradores de la organización se limitan a gestionar una o más organizaciones, pero no pueden realizar cambios en el sistema.
- **Operador**: los operadores tienen capacidades similares a las de los administradores de la organización, pero no pueden administrar usuarios.
- **Solo lectura**: un usuario de solo lectura únicamente puede ver información de red, no puede realizar modificaciones.

Cisco Business Dashboard permite a los usuarios autenticarse en la base de datos de usuarios local. A partir de la versión 2.2.1, los usuarios también pueden autenticarse en una instancia de Microsoft Azure Active Directory.

Al instalar Cisco Business Dashboard por primera vez, se crea un **Administrador** predeterminado en la base de datos del usuario local con el nombre de usuario y la contraseña `cisco`.



Nota Únicamente los **Administradores** y los **Administradores de la organización** pueden administrar la configuración de los usuarios.

Adición de un nuevo usuario a la base de datos de usuarios local

Para agregar un nuevo usuario, haga lo siguiente:

1. Acceda a **Administración** > **Usuarios** y seleccione la pestaña **Usuarios**.
2. Haga clic en el icono **+** (más) para crear un usuario nuevo.
3. En los campos proporcionados, escriba un nombre de usuario, un nombre que mostrar, una dirección de correo electrónico y una contraseña, y especifique el tipo de usuario. También puede facilitar datos de contacto para el usuario.
4. Haga clic en **Guardar**.

Si el usuario no es un **Administrador**, debe añadirlo a una o varias organizaciones. Para ello, seleccione la pestaña **Organizaciones** y haga clic en el icono **+** (más). Seleccione la organización deseada de la lista desplegable.

Modificación de un usuario

Para modificar un usuario, haga lo siguiente:

1. Acceda a **Administración** > **Usuarios** y seleccione la pestaña **Usuarios**.
2. Seleccione el botón de opción situado junto al usuario que debe cambiarse y haga clic en el icono **Editar**.
3. Realice las modificaciones según sea necesario.
4. Haga clic en **Guardar**.

Para añadir al usuario a una nueva organización, seleccione la pestaña **Organizaciones** y haga clic en el icono **+** (más). Seleccione la organización deseada de la lista desplegable. Para eliminarlo de una organización, haga clic en el icono **Eliminar** ubicado junto a la organización en la tabla.

Eliminación de un usuario

Para eliminar un usuario, haga lo siguiente:

1. Acceda a **Administración** > **Usuarios** y seleccione la pestaña **Usuarios**.
2. Seleccione el botón de opción situado junto al usuario que debe eliminarse y haga clic en **Eliminar** en la parte superior de la tabla.

Modificación de la complejidad de la contraseña

Para habilitar o cambiar los requisitos de complejidad de la contraseña, haga lo siguiente:

1. Acceda a **Administración** > **Usuarios** y seleccione la pestaña **Configuración de usuario**.

2. Seleccione la pestaña **Local** en **Origen de autenticación**, modifique la configuración **Complejidad de la contraseña del usuario** según sea necesario y haga clic en **Guardar**.



Nota Al autenticarse en una instancia de Azure Active Directory, la complejidad de la contraseña se administra en Active Directory.

Activación de la autenticación de Azure Active Directory

Cisco Business Dashboard admite la autenticación de usuarios con una instancia de Microsoft Azure Active Directory. A los usuarios de Active Directory se les asignan funciones y listas de organizaciones en función de los grupos de Active Directory a los que pertenece el usuario.

Para habilitar Azure Active Directory como origen de autenticación, haga lo siguiente:

1. En **Azure Active Directory**, cree un nuevo registro de aplicación para Cisco Business Dashboard, asígnele permisos delegados de User.Read y Domain.Read.All desde la **API de Microsoft Graph** y cree un **secreto de cliente**. Tenga en cuenta la ID de la aplicación (cliente), el secreto del cliente y la ID del directorio (arrendatario).
2. Abra la GUI web de Cisco Business Dashboard y acceda a **Administración > Usuarios**. Seleccione la pestaña **Configuración de usuario** y, a continuación, seleccione la pestaña **Azure AD** en **Origen de autenticación**.
3. Haga clic en la casilla de verificación **Activar**.
4. Introduzca la **ID de cliente**, el **Secreto de cliente** y la **ID de arrendatario** recopilados en el paso 1 en el campo proporcionado.
5. Opcionalmente, especifique una lista de dominios separados por comas a los que se debe permitir acceder al panel. Haga clic en **Guardar**.
6. Haga clic en el icono del signo más (+) del encabezado **Asignaciones de grupos de usuarios** para crear una nueva asignación de grupos. Introduzca la **ID de objeto** para el grupo de Active Directory en el campo proporcionado y, a continuación, seleccione una función y una lista de organización que aplicar a los usuarios de este grupo. Repita este paso para todos los grupos que se deben asignar.
7. Tome nota de la **URL de redireccionamiento** que se muestra debajo de la casilla de verificación **Habilitar**. Vuelva a Azure Active Directory y agregue la URL a la lista de URI de redireccionamiento para el registro de la aplicación.



Nota El host y el puerto que se muestran en la URL de redireccionamiento deben ser accesibles desde los navegadores web de los usuarios que acceden al panel. Si no se puede acceder a los valores actuales que se muestran, actualice los campos correspondientes en la pestaña **Variables de sistema** de la página **Configuración de plataforma > del sistema**.

Administración de la autenticación local

La autenticación en la base de datos del usuario local está habilitada de forma predeterminada. Para deshabilitar la autenticación local, haga lo siguiente:

1. Asegúrese de que la autenticación en Azure Active Directory se haya configurado como se describe anteriormente. Inicie sesión en el panel con una cuenta de administrador autenticada por Active Directory.
2. Acceda a **Administración > Usuarios** y seleccione la pestaña **Configuración de usuario**. En **Origen de la autenticación**, seleccione la pestaña **Local**.
3. Anule la selección de la casilla de verificación **Habilitar** y haga clic en **Guardar**.

Para habilitar la autenticación local de nuevo, haga lo siguiente:

1. Acceda a **Administración > Usuarios** y seleccione la pestaña **Configuración de usuario**. En **Origen de la autenticación**, seleccione la pestaña **Local**.
2. Seleccione de la casilla de verificación **Habilitar** y haga clic en **Guardar**.

Restauración del acceso cuando se haya perdido todo el acceso administrativo

Si se pierde el acceso administrativo a la aplicación Cisco Business Dashboard, haga lo siguiente para recuperarla:

1. Inicie sesión en el sistema operativo del host usando SSH o a través de la consola.
2. Introduzca el comando **cisco-business-dashboard recoverpassword**

Después de introducir el comando, se habilita la autenticación de usuario local y se restaura el administrador predeterminado con el nombre de usuario **cisco** y la contraseña **cisco**.

Modificación de los tiempos de espera de sesión

Para modificar los tiempos de espera inactivo y absoluto de las sesiones de usuario, haga lo siguiente:

1. Acceda a **Administración > Usuarios** y seleccione la pestaña **Configuración de usuario**.
2. Modifique los parámetros de **Sesión del usuario** según sea necesario y haga clic en **Guardar**. Pase el cursor por encima de los iconos de ayuda para ver intervalos admisibles para estos parámetros.

Cambio de los valores predeterminados de supervisión

Los perfiles de supervisión le permiten controlar la supervisión de dispositivos que se realiza en la red. Los perfiles de supervisión se pueden aplicar en el nivel de organización o en el de sistema. En el caso de las organizaciones que decidan heredar los perfiles de supervisión del nivel de sistema, el comportamiento se controlará mediante la página **Valores predeterminados de supervisión**.

Para cambiar los **perfiles de supervisión** aplicados en el sistema, haga lo siguiente:

1. Acceda a **Administración > Valores predeterminados de supervisión**.
2. Utilice los menús desplegables para seleccionar el perfil de supervisión adecuado que se aplicará a los dispositivos del tipo correspondiente. Consulte Gestión de perfiles de supervisión para obtener más información sobre la creación de perfiles de supervisión.
3. Haga clic en **Guardar**.

Consulte [Administración de los perfiles de supervisión](#) para obtener más información sobre los tipos de supervisión que se pueden llevar a cabo y cómo configurarlos. Consulte [Administración de las organizaciones, en la página 68](#) para obtener más información sobre el cambio de la configuración de supervisión a nivel de la organización.

Administración de los perfiles de supervisión

Los perfiles de supervisión controlan los datos que se recopilan de los dispositivos y las notificaciones que se generan. Los perfiles se pueden aplicar a diferentes tipos de dispositivos dentro de una organización o en todo el sistema. En un perfil, se admiten dos tipos de monitores: **monitores de notificación** y **monitores de informes**.

Los monitores de notificaciones hacen que se generen notificaciones y alertas, generalmente debido a un cambio en el estado del dispositivo o a un parámetro que cruza un umbral. Las notificaciones tienen distintos niveles de gravedad (informativo, de advertencia y de alerta) y pueden generar mensajes emergentes en la interfaz de usuario y notificaciones por correo electrónico. Las notificaciones activas también están visibles en el **Centro de notificaciones** y se muestran en las vistas de información del dispositivo. Los cambios en las notificaciones también se registran en el **registro de eventos**.



Nota

Si usa notificaciones por correo electrónico, debe asegurarse de que la configuración del correo electrónico sea correcta. Consulte [Administración de la configuración del correo electrónico](#) para obtener más información.

Los supervisores de informes recopilan los datos utilizados para los informes inalámbricos y los gráficos de tráfico en el panel de supervisión.

Se pueden crear varios perfiles de supervisión y se pueden asignar diferentes perfiles a diferentes tipos de dispositivos a nivel de sistema o según la organización. Para obtener más información sobre la asignación de perfiles de supervisión a los dispositivos, consulte [Administración de las organizaciones, en la página 68](#) y [Cambio de los valores predeterminados de supervisión, en la página 75](#).

Agregar un nuevo perfil de supervisión

Para agregar un nuevo perfil de supervisión, haga lo siguiente:

1. Acceda a **Administración > Perfiles de supervisión**.
2. Haga clic en el icono **+** (más) para agregar un perfil nuevo
3. Especifique un nombre para el perfil y una organización a la que asociar el perfil. También puede especificar todas las organizaciones aquí, lo que permite que el perfil se utilice con cualquier organización o como un nivel de sistema predeterminado.
4. También puede proporcionar una descripción del perfil y una lista de direcciones de correo electrónico separadas por comas para recibir notificaciones.
5. Haga clic en **Save** (Guardar)
6. La pantalla se actualiza para mostrar los diferentes monitores de notificaciones e informes. Puede activar y desactivar los monitores individuales utilizando los controles proporcionados.

7. Los monitores de notificaciones tienen ajustes adicionales que pueden modificarse haciendo clic en el icono **Editar** del monitor. La configuración variará entre los monitores, pero incluye los tipos de notificación que se deben generar, la gravedad de la notificación y los umbrales que deben activar la notificación.

Copiar un perfil de supervisión existente

Para copiar un perfil de supervisión existente, haga lo siguiente:

1. Acceda a **Administración > Perfiles de supervisión**.
2. Seleccione la casilla de verificación junto al perfil que desea copiar y haga clic en el icono **Guardar como**.
3. Actualice el nombre del perfil, la descripción, la organización y las direcciones de correo electrónico según sea necesario y, a continuación, haga clic en **Guardar**.
4. Realice los cambios en los monitores de notificaciones e informes según sea necesario. Puede restaurar los valores predeterminados del monitor haciendo clic en el botón **Restablecer valores predeterminados**.

Modificación de un perfil de supervisión

Para modificar un perfil de supervisión existente, haga lo siguiente:

1. Acceda a **Administración > Perfiles de supervisión**.
2. Seleccione la casilla de verificación junto al perfil que desea copiar y haga clic en el icono **Editar**.
3. Actualice la configuración del perfil y las direcciones de correo electrónico según sea necesario y, a continuación, haga clic en **Guardar**.
4. Realice los cambios en los monitores de notificaciones e informes según sea necesario. Puede restaurar los valores predeterminados del monitor haciendo clic en el botón **Restablecer valores predeterminados**.

Eliminación de un perfil de supervisión

Para eliminar un perfil de supervisión existente, haga lo siguiente:

1. Acceda a **Administración > Perfiles de supervisión**.
2. Seleccione la casilla de verificación junto al perfil que desea copiar y haga clic en el icono **Eliminar**.



Nota

Si el perfil se utiliza como perfil de supervisión de nivel de organización, la organización y el tipo de dispositivo correspondientes se actualizarán para heredar la configuración de nivel de sistema. Los perfiles que están en uso como perfiles de supervisión de nivel de sistema no podrán eliminarse. Elimine el perfil de la página **Administración > Valores predeterminados de supervisión** antes de eliminarlo.

Visualización de los intentos de inicio de sesión

Cisco Business Dashboard mantiene un registro de cada intento de inicio y cierre de sesión del sistema, ya sea satisfactorio o no. Para ver este registro, acceda a **Administración > Intentos de inicio de sesión**. En la tabla, se muestra la siguiente información:

Tabla 23: Tabla de intentos de inicio de sesión

Campo	Descripción
Nombre del usuario	El nombre de usuario asociado al evento.
Nombre de visualización	El nombre de visualización del usuario.
IP	La dirección IP del dispositivo desde el que el usuario inició sesión.
Tipo	El tipo de evento. Los valores válidos incluyen LOGIN y LOGOUT.
Estado	Indica si el intento se llevó a cabo correctamente o no.
Marca de tiempo	La fecha y la hora en que tuvo lugar el evento.

Puede utilizar el cuadro de búsqueda situado sobre la tabla para mostrar únicamente las entradas que coincidan con un usuario o dirección IP en particular.

Administración de la configuración de los informes

La página **Configuración de informes** permite establecer la zona horaria para la que se generarán los informes. Las horas de inicio y fin del periodo de los informes aparecerán en la hora local de la zona horaria seleccionada.



CAPÍTULO 12

Sistema

Este capítulo contiene las siguientes secciones:

- [Acerca de Sistema](#), en la página 79
- [Gestión de licencias](#), en la página 80
- [Gestión de certificados](#), en la página 82
- [Administración de la configuración del correo electrónico](#), en la página 84
- [Visualización del uso de la API](#), en la página 85
- [Copias de seguridad y restauración de la configuración de Dashboard](#), en la página 86
- [Administración de la configuración de la plataforma](#), en la página 86
- [Administración de la privacidad](#), en la página 89
- [Administración de la configuración de registro](#), en la página 91
- [Gestión de Probe local](#), en la página 93

Acerca de Sistema

La opción Sistema de Cisco Business Dashboard permite administrar el funcionamiento de la plataforma.

Esta opción se divide en las siguientes páginas:

- **Licencia:** permite administrar las licencias de software de Dashboard.
- **Certificado:** permite administrar los certificados de seguridad de Dashboard.
- **Configuración de correo electrónico:** permite configurar el correo electrónico.
- **Uso de API:** permite supervisar el uso de la API de Cisco Business Dashboard.
- **Copia de seguridad:** permite hacer copias de seguridad de la configuración y otros datos de Dashboard
- **Restaurar:** permite restaurar la configuración y otros datos de Dashboard
- **Configuración de plataforma:** permite administrar la configuración de la red para Dashboard
- **Configuración de privacidad:** permite controlar los datos que se pueden compartir con Cisco.
- **Configuración de registro:** permite cambiar la configuración del registro de Dashboard
- **Probe local:** gestione un Probe alojado en Dashboard

Estas páginas solo están disponibles para los **Administradores**.

Gestión de licencias



Nota Esta página no está incluida en la versión limitada de Cisco Business Dashboard para AWS.

La página **Licencia** permite ver la cantidad y el tipo de licencias necesarias para su red y conectar **Dashboard** al sistema Cisco Smart Licensing. Esta página contiene dos paneles:

- **Estado de las licencias de software Smart:** este panel muestra el estado de registro del cliente Licencia Smart e información sobre la Smart Account en uso.
- **Uso de la licencia Smart:** este panel enumera la cantidad y el tipo de licencias necesarias en función del estado actual de la red. Esta información se actualizará automáticamente a medida que la red cambie y Dashboard actualizará la cantidad de licencias necesarias para Smart Account. El campo Estado muestra si se han obtenido correctamente las licencias necesarias.

Esta página también contiene controles que permiten registrar Dashboard y anular su registro desde su Smart Account.

Si Dashboard no puede obtener suficientes licencias para gestionar la red, funcionará en modo de evaluación y se mostrará un mensaje en el encabezado de la interfaz de usuario de Dashboard. Al ejecutarse en modo de evaluación, tiene 90 días para corregir la situación. Si no se corrige el problema en un plazo de 90 días, se limitarán ciertas funciones de Dashboard hasta que se haga obteniendo más licencias o reduciendo el número de dispositivos gestionados.

Registro de Dashboard en su Smart Account

Para registrar Dashboards en su Smart Account, haga lo siguiente:

1. Inicie sesión en su Smart Account en <https://software.cisco.com>. Seleccione el enlace **Licencias de software Smart** situado en la sección License (licencia).
2. Seleccione la página **Inventario** y, si es necesario, cambie la cuenta virtual seleccionada de la predeterminada. Después, haga clic en la pestaña **General**.
3. Cree un nuevo **token de registro de la instancia del producto** haciendo clic en el botón **Nuevo token...** Opcionalmente, añada una descripción y cambie el tiempo de **Expirar tras**. Después, haga clic en **Crear token**.
4. Copie el token que acaba de crear al portapapeles seleccionando **Copiar** del menú desplegable **Acciones** situado a la derecha del token.
5. Acceda a la interfaz de usuario de Cisco Business Dashboard y seleccione **Sistema > Licencia**.
6. Haga clic en el botón **Registrar** y pegue el token en el campo provisto. Haga clic en **Aceptar**.

Dashboard se registrará en Cisco Smart Licensing y solicitará suficientes licencias para la cantidad de dispositivos de red que se estén gestionando. Si no hay suficientes licencias disponibles, se mostrará un mensaje en la interfaz de usuario y dispondrá de 90 días para obtenerlas antes de que se limiten las funciones del sistema.

Eliminación de Dashboard de su Smart Account

Para eliminar Dashboard de su Smart Account y devolver todas las licencias asignadas al grupo, haga lo siguiente:

1. Acceda a la interfaz de usuario de Cisco Business Dashboard y seleccione **Sistema > Licencia**.
2. Seleccione **Anular registro...** de la lista desplegable situada en la parte superior derecha. Haga clic en **Anular registro** de la ventana emergente para confirmar.

Comprobación inmediata de licencias

Cisco Business Dashboard realiza comprobaciones diarias para garantizar que siga habiendo suficientes licencias disponibles para la red y se actualiza inmediatamente si la cantidad de licencias necesarias disminuye. No obstante, si la cantidad de licencias aumenta o si se añaden licencias al grupo o se eliminan de este, puede pasar un día hasta que se actualice Dashboard. Para forzar la actualización de asignaciones de licencias de Dashboard, haga lo siguiente:

1. Acceda a la interfaz de usuario de Cisco Business Dashboard y seleccione **Sistema > Licencia**.
2. Seleccione **Volver a comprobar licencia ahora...** de la lista desplegable en la parte superior derecha. Cisco Business Dashboard consultará Cisco Smart Licensing inmediatamente para garantizar que haya suficientes licencias disponibles para que Dashboard funcione.

Renueve la autorización ahora

La acción Renovar registro ahora hace que Dashboard actualice los certificados usados para autenticar la comunicación con Cisco Smart Licensing. Generalmente solo será necesario por solicitud del servicio de atención al cliente de Cisco cuando se rectifique un corte de comunicaciones prolongado. Para renovar el registro, haga lo siguiente:

1. Acceda a la interfaz de usuario de Cisco Business Dashboard y seleccione **Sistema > Licencia**.
2. Seleccione **Renovar autorización ahora...** de la lista desplegable situada en la parte superior derecha.

Renovar registro ahora

La acción Renovar registro ahora hace que Dashboard actualice los certificados usados para autenticar la comunicación con Cisco Smart Licensing. Generalmente solo será necesario por solicitud del servicio de atención al cliente de Cisco cuando se rectifique un corte de comunicaciones prolongado. Para renovar el registro, haga lo siguiente:

1. Acceda a la interfaz de usuario de Cisco Business Dashboard y seleccione **Sistema > Licencia**.
2. Seleccione **Renovar registro ahora...** de la lista desplegable situada en la parte superior derecha.

Transferencia de Dashboard a otra cuenta

Un nuevo registro de Dashboard permite trasladarlo de una cuenta virtual a otra. Para trasladar un Dashboard de una cuenta a otra, haga lo siguiente:

1. Acceda a la interfaz de usuario de Cisco Business Dashboard y seleccione **Sistema > Licencia**.
2. Seleccione **Volver a registrar...** de la lista desplegable situada en la parte superior derecha.

3. Introduzca el nuevo token de registro en el cuadro provisto. Si Dashboard está registrado en otra cuenta en el momento, asegúrese de que la casilla **Vuelva a registrar la instancia del producto si ya está registrada** esté marcada y haga clic en **Aceptar**.

Gestión de certificados

Durante la instalación, Cisco Business Dashboard creará un certificado autofirmado para proteger la web y otras comunicaciones con el servidor. Puede sustituir este certificado con uno firmado por una entidad de certificación (CA) de confianza. Para ello, deberá generar una solicitud de firma de certificado (CSR) para que la entidad de certificación la firme.

También puede generar un certificado y la clave privada correspondiente de forma totalmente independiente de Dashboard. En ese caso, puede combinar el certificado y la clave privada en un archivo de formato PKCS#12 antes de la carga.

Generación de una solicitud de firma de certificado (CSR)

Para generar una CSR, haga lo siguiente:

1. Acceda a **Sistema > Certificado** y seleccione la pestaña **CSR**.
2. Introduzca valores adecuados en los campos provistos en el formulario mostrado. Estos valores se utilizarán para crear la CSR y estarán incluidos en el certificado firmado que reciba de la entidad de certificación.
3. Haga clic en **Crear** y se descargará automáticamente la CSR en su PC. También puede descargar la CSR más tarde haciendo clic en **Descargar** junto a la etiqueta de la CSR.
4. Si es necesario, puede modificar la CSR volviendo al paso 2.

Carga de un nuevo certificado

Para cargar un nuevo certificado con la GUI de administración, haga lo siguiente:

1. Acceda a **Sistema > Certificado** y seleccione la pestaña **Actualizar certificado**.
2. Seleccione el botón de opción **Cargar certificado**. Puede soltar el archivo que contiene el certificado en la zona de destino o hacer clic en esta para examinar el sistema de archivos. El archivo debe tener formato PEM.

También puede cargar un certificado con la clave privada asociada en formato PKCS#12 seleccionando la opción **Cargar PKCS12**. Debe especificarse la contraseña para desbloquear el archivo en el campo provisto.

3. Haga clic en **Cargar** para cargar el archivo y sustituir el certificado actual.

Para cargar un nuevo certificado con la línea de comandos, haga lo siguiente:

1. Copie el certificado y los archivos de clave privada en el sistema de archivos de Cisco Business Dashboard con SCP o similar. Asegúrese de que el acceso a estos archivos esté restringido solo al personal autorizado, ya que la clave privada es información confidencial.
2. Inicie sesión en el sistema operativo usando la consola o SSH.

3. Aplique el certificado a la aplicación del panel con el comando: **cisco-business-dashboard importcert -t pem -k <private key file> -c <certificate file>**. El certificado y la clave privada se cargarán en la aplicación del panel y sustituirán al certificado actual. Para obtener más información sobre este comando y sus opciones, introduzca **cisco-business-dashboard importcert -h**.



Nota Algunos navegadores pueden generar advertencias para los certificados que ha firmado una entidad de certificación conocida, mientras que otros navegadores aceptan el certificado sin ninguna advertencia. Los clientes de Plug and Play de red también pueden no aceptar el certificado. Esto se debe a que la entidad de certificación ha firmado el certificado con un certificado intermedio que no está incluido en el registro de entidades de confianza del navegador o del cliente PnP. En estas circunstancias, la entidad de certificación proporciona un conjunto de certificados que se deben concatenar con el certificado de servidor antes de cargarlo en Dashboard. El certificado de servidor debe aparecer primero en el conjunto concatenado.

Regeneración del certificado autofirmado

Para volver a generar el certificado autofirmado, siga estos pasos:

1. Acceda a **Sistema > Certificado** y seleccione la pestaña **Actualizar certificado**.
2. Haga clic en **Renovar certificado autofirmado**. Introduzca valores adecuados en los campos provistos en el formulario mostrado. Estos valores se utilizarán para crear el certificado.
3. Haga clic en **Guardar**.

Vista del certificado actual

Para ver el certificado actual, haga lo siguiente:

1. Acceda a **Sistema > Certificado** y seleccione la pestaña **Certificado actual**.
2. El certificado se mostrará en texto sin formato en su navegador.

Descarga del certificado actual

Para descargar una copia del certificado actual, haga lo siguiente:

1. Acceda a **Sistema > Certificado** y seleccione la pestaña **Certificado actual**.
2. Haga clic en **Descargar** en la parte inferior de la página. Su navegador descargará el certificado en formato PEM.

Instale automáticamente un certificado desde Let's Encrypt

A partir de la versión 2.2.1, Cisco Business Dashboard puede obtener y renovar automáticamente un certificado validado por un dominio en **Entidad emisora de certificados de Let's Encrypt** (<https://letsencrypt.org>). Para hacerlo, siga estos pasos:

1. Inicie sesión en el sistema operativo del host usando SSH o a través de la consola.
2. Ejecute el comando **cisco-business-dashboard letsencrypt** y especifique uno o más nombres de host totalmente calificados mediante la opción **-d**. Por ejemplo, **cisco-business-dashboard letsencrypt -d**

dashboard.example.com -d pnpserver.example.com. Todos los nombres enumerados en el comando deben resolverse en la dirección IP del servidor del panel.

3. Siga las indicaciones para emitir un certificado y aplicarlo a la aplicación del panel. El certificado se renovará automáticamente en el panel a medida que se acerca el vencimiento.



Nota El servicio **Let's Encrypt** deberá conectarse al servidor web del panel para verificar la propiedad de los nombres de host. Para permitirlo, el servidor web del panel debe ser accesible desde Internet. Consulte [Administración de la configuración de la plataforma, en la página 86](#) para obtener detalles sobre cómo restringir el acceso a la aplicación del panel a solo direcciones IP autorizadas.

Administración de la configuración del correo electrónico

La página **Configuración de correo electrónico** permite controlar la forma en que Cisco Business Dashboard enviará los mensajes de correo electrónico. Esta página permite definir los siguientes parámetros:

Tabla 24: Configuración de correo electrónico

Campo	Descripción
Servidor SMTP	El nombre de dominio o la dirección IP del servidor SMTP que se usará.
Puerto SMTP	El puerto TCP que se usará para enviar el correo
Cifrado de correo electrónico	El método de cifrado que se va a utilizar Estas son las opciones: <ul style="list-style-type: none"> • Ninguno • TLS • SSL
Autenticación	Habilite o deshabilite la autenticación de correo electrónico.
Nombre del usuario	Nombre de usuario que se debe especificar si está habilitada la autenticación.
Contraseña	Contraseña que se debe especificar si está habilitada la autenticación.
Dirección de correo electrónico de origen	La dirección de correo electrónico desde la que se envían los mensajes.

Para probar la configuración, haga clic en **Prueba de conectividad**. De este modo, se solicitará una dirección de correo electrónico de destino y se generará un mensaje de correo electrónico de prueba para la dirección especificada.

Visualización del uso de la API

En la página Uso de API, se muestra información sobre las aplicaciones externas que se han integrado con Cisco Business Dashboard. Este informe se divide en las siguientes tres secciones:

- **15-minute Request Monitor** (Monitor de solicitudes de 15 minutos): muestra la tasa media y máxima de solicitudes en los últimos 15 minutos.
- Gráfico **Historial de solicitudes**: muestra un gráfico de la actividad de las solicitudes a lo largo del tiempo. Puede seleccionar periodos de tiempo de las últimas cuatro horas, los últimos siete días o toda la información disponible. Después, puede utilizar los controles deslizantes que hay bajo el gráfico para limitar su enfoque a un periodo de interés determinado.
- Tabla **Información del cliente API**: muestra todos los clientes que han usado la API al menos una vez. En la siguiente tabla, se describe la información proporcionada en la tabla **Información del cliente API**:

Tabla 25: Tabla Información del cliente API

Campo	Descripción
Versión API	La versión empleada por el cliente al acceder a la API.
Id. de cliente	El identificador de una instancia concreta de la aplicación del cliente.
IP del cliente	La dirección IP asociada a este cliente. También muestra la URL de callback en la que Dashboard debe publicar las notificaciones de los eventos cuando la versión de la API es la v1 y se han solicitado notificaciones.
Módulo del cliente	El tipo de aplicación asociada a este cliente.
Versión del cliente	La versión de la aplicación asociada a este cliente.
Nombre del usuario	En el caso de los clientes que usan la API v1, este campo muestra el nombre de usuario presentado por la aplicación al autenticarse en Dashboard. En el caso de los clientes que utilizan la API v2, en este campo aparece el ID de la clave de acceso empleado por el cliente y el nombre de usuario al que está asociada la clave.
Tiempo desde el último acceso	El tiempo transcurrido desde la última actividad de este cliente.
N.º de redes suscritas	El número de redes donde la aplicación ha solicitado notificaciones de eventos. Este número es un enlace que, al hacer clic en él, muestra la tabla Redes suscritas de este cliente. Más adelante, se describe la tabla Redes suscritas.
N.º de dispositivos con licencia suscritos	El número de dispositivos administrados sobre los que se enviarán notificaciones de eventos a este cliente.

Si desea ver información sobre las redes para las que un cliente ha solicitado notificaciones, haga clic en el enlace **N.º de redes suscritas** correspondiente al cliente en la tabla **Información del cliente API**. La tabla **Redes suscritas** se mostrará para el cliente que contenga una lista de las redes para las que el

cliente haya solicitado notificaciones. En la siguiente tabla, se describe la información proporcionada en la tabla **Redes suscritas**:

Tabla 26: Tabla Redes suscritas

Campo	Descripción
Segmentación	El nombre de la red que supervisa el cliente.
N.º de dispositivos con licencia suscritos	El número de dispositivos administrados de esta red sobre los que se enviarán notificaciones de eventos.

Copias de seguridad y restauración de la configuración de Dashboard

Es posible efectuar copias de seguridad de la configuración y otros datos de Cisco Business Dashboard para fines de recuperación ante desastres o para facilitar la migración de Dashboard a un nuevo host. Para proteger los datos sensibles, las copias de seguridad se cifran con una contraseña.

Para realizar una copia de seguridad, haga lo siguiente:

1. Acceda a **Sistema > Copia de seguridad**.
2. Introduzca una contraseña para cifrar la copia de seguridad en los campos **Contraseña** y **Confirmar contraseña**.
3. Haga clic en **Hacer copia de seguridad y descargar**. Se abrirá una ventana emergente que le mostrará el progreso de la copia de seguridad. Los sistemas más grandes pueden necesitar cierto tiempo para llevar a cabo la copia de seguridad, por lo que puede cerrar el medidor de progreso y abrirlo más adelante con el botón **Ver estado**.

Cuando haya finalizado, el archivo de copia de seguridad se descargará en el PC.

Para restaurar una copia de seguridad de configuración en Dashboard, haga lo siguiente:

1. Acceda a **Sistema > Restaurar**.
2. Introduzca la contraseña que usó para cifrar la copia de seguridad en el campo **Contraseña**.
3. Haga clic en **Cargar y restaurar** para continuar. Aparecerá una ventana emergente que le permitirá cargar un archivo de copia de seguridad desde su PC. También puede arrastrar y soltar el archivo de copia de seguridad en el área de destino proporcionada o hacer clic en el área de destino para elegir un archivo del sistema de archivos del PC. Haga clic en **Restaurar** para continuar.

Administración de la configuración de la plataforma

La página **Configuración de la plataforma** permite modificar ajustes clave del sistema sin necesidad de acceder directamente al sistema operativo. Debido a la variación en las plataformas compatibles de Cisco Business Dashboard, no todas las configuraciones estarán disponibles en todas las plataformas.

La configuración de la plataforma se divide en tres grupos: Configuración de red, Servidor web y Variables del sistema, con cada grupo con una pestaña independiente en esta página. Las siguientes secciones describen la configuración disponible en cada pestaña.

Cambio del nombre de host (pestaña Configuración de red)



Nota Esto no se aplica a Cisco Business Dashboard para AWS.

El nombre de host es el nombre usado por el sistema operativo para identificar el sistema y utilizado por Cisco Business Dashboard para identificar Dashboard cuando se generan anuncios de Bonjour. Para cambiar el nombre de host de Dashboard, haga lo siguiente:

1. Acceda a **Sistema > Configuración de la plataforma** y seleccione la pestaña **Configuración de la red**.
2. Especifique un nombre de host para Dashboard en el campo especificado.
3. Haga clic en **Guardar**.

Cambio de la configuración de red (pestaña Configuración de red)



Nota Esto no se aplica a Cisco Business Dashboard para AWS. Para modificar la configuración de red, utilice la consola EC2 de AWS.

Para cambiar la configuración de red de Dashboard, haga lo siguiente:

1. Acceda a **Sistema > Configuración de la plataforma** y seleccione la pestaña **Configuración de la red**.
2. Seleccione el método para la asignación de direcciones IP. Las opciones disponibles son DHCP (opción predeterminada) e IP estática. Si elige la opción IP estática, tendrá que especificar la dirección, la máscara de subred, las gateways predeterminadas y los servidores DNS en los campos apropiados.
3. Haga clic en **Save** (Guardar)

Cambio de la configuración de hora (pestaña Configuración de red)

La opción **Configuración de hora** permite administrar el reloj del sistema de Dashboard. Para ajustar el reloj del sistema, haga lo siguiente:

1. Acceda a **Sistema > Configuración de la plataforma** y seleccione la pestaña **Configuración de la red**.
2. Seleccione la zona horaria adecuada para Dashboard.
3. Seleccione el método para la sincronización temporal. Las opciones disponibles son **NTP (opción predeterminada)** y **Reloj local**. Si elige la opción NTP, podrá modificar los servidores NTP que se deben usar para la sincronización.

Si elige la opción **Reloj local**, podrá ajustar manualmente la fecha y hora mediante los controles disponibles. También puede hacer clic en **reloj** para sincronizar la hora con su PC.

4. Haga clic en **Guardar**.

Modificación de la configuración de puertos (pestaña Servidor web)

La opción **Configuración de puertos** permite controlar los puertos TCP en los que se aloja la interfaz de usuario de Dashboard. Para modificar los puertos de servidor web predeterminados, haga lo siguiente:

1. Acceda a **Sistema > Configuración de la plataforma** y seleccione la pestaña **Servidor web**.
2. Modifique los puertos usados por el servidor web para los protocolos HTTP y HTTPS.
3. Haga clic en **Guardar**.



Nota

Si se configura la máquina virtual para sincronizar el reloj local con la máquina de host, el hipervisor sobrescribirá cualquier cambio en el reloj local realizado a través de la página **Configuración de plataforma**.

Si el hipervisor en uso es VirtualBox y las Guest Additions de VirtualBox están instaladas en la máquina virtual, el servicio NTP (timesyncd) no funcionará.

Restricción del acceso a Dashboard (pestaña Servidor web)

Puede limitar las direcciones IP que pueden acceder a Dashboard mediante la configuración de control de acceso. Puede especificar diferentes rangos de IP para la GUI de Dashboard, la API de Dashboard y para las conexiones de las sondas y los dispositivos administrados.

Para limitar el acceso a Dashboard, haga lo siguiente:

1. Acceda a **Sistema > Configuración de la plataforma** y seleccione la pestaña **Servidor web**.
2. Introduzca un prefijo de red y una máscara en los campos proporcionados. Si se requieren varios prefijos para cualquier sección, haga clic en el icono (+) más para agregar entradas adicionales. Del mismo modo, puede hacer clic en el icono de la papelera para eliminar las entradas existentes.
3. Haga clic en **Guardar**.

Gestión de variables del sistema (pestaña Variables del sistema)

Cisco Business Dashboard utiliza variables del sistema para proporcionar determinados parámetros relacionados con Dashboard al generar plantillas de configuración y otras tareas. Dashboard puede determinar automáticamente algunas variables del sistema, pero hay otras variables que requieren la intervención del usuario. En particular, si se implementa Dashboard en un proxy web o gateway NAT, será necesario que el administrador proporcione información de direccionamiento externo para Dashboard.

Para actualizar la información de la dirección externa de Dashboard, haga lo siguiente:

1. Acceda a **Sistema > Configuración de la plataforma** y seleccione la pestaña **Variables del sistema**.
2. Introduzca la dirección IP y la información del puerto en los parámetros de configuración del sistema externo según sea necesario. Si se deja en blanco, Dashboard utilizará la dirección de la plataforma y la información del puerto para la variable del sistema correspondiente.
3. Haga clic en **Guardar**.

Administración de la privacidad

Algunas de las funciones de Cisco Business Dashboard requieren el uso de servicios en línea alojados por Cisco y conllevan el intercambio de cierta información con este. Estos servicios incluyen:

- **Cisco Active Advisor:** Cisco Business Dashboard puede cargar la información del inventario de la red en el servicio Cisco Active Advisor, <https://www.ciscoactiveadvisor.com>. Esta opción está deshabilitada por defecto.
- **Informes del ciclo de vida:** esta función incluye la generación del **Informe de ciclo de vida**, el **Informe de final de ciclo de vida útil** y el **Informe de mantenimiento** en Cisco Business Dashboard. La función Informes del ciclo de vida está habilitada de forma predeterminada.
- **Actualizaciones de software:** esta característica notifica la disponibilidad de actualizaciones de software para los dispositivos de red y permite aplicarlas automáticamente. La función Actualizaciones de software está habilitada de forma predeterminada.
- **Mejora del producto:** esta función permite a Cisco Business Dashboard enviar información sobre el uso del hardware y el software en la red con el fin de desarrollar más la cartera de productos de Cisco. La función Mejora del producto está habilitada de forma predeterminada.

Todas estas funciones están sujetas a la [política de privacidad de Cisco](#) y usted puede habilitarlas o deshabilitarlas en cualquier momento. La página **Configuración de privacidad** se muestra durante la configuración inicial de Manager y permite deshabilitar cualquiera de las funciones habilitadas de forma predeterminada antes de que se recopilen datos de red. A continuación, puede encontrar más detalles sobre cada una de estas funciones y la información que se debe compartir.

Cisco Active Advisor

Cisco Active Advisor (CAA) es un servicio basado en la nube que proporciona información esencial sobre el ciclo de vida del inventario de red. Al habilitar esta función, Dashboard envía información de inventario de la red a CAA y usted puede ver la información del ciclo de vida útil en el portal de CAA. La información confidencial, como nombres de usuario y contraseñas, no se envía.

Las cargas se pueden realizar automáticamente o a demanda. Para realizar una carga a demanda, siga estos pasos:

1. Acceda a la página **Red** y seleccione una red para verla.
2. Seleccione **Cargar en CAA** en el menú desplegable **Acciones de red**.
3. Si se le solicita, proporcione sus credenciales de cisco.com.
4. De manera opcional, puede seleccionar una etiqueta para que se aplique a la carga.
5. Haga clic en **Cargar**. También puede hacer clic en **Ver los datos del inventario antes del envío** para inspeccionar los datos antes de cargarlos.



Nota Las credenciales de cisco.com facilitadas deben utilizarse para iniciar sesión en el portal de Cisco Active Advisor (<https://www.ciscoactiveadvisor.com>) al menos una vez antes de usarlas para la carga.

Para habilitar las cargas automáticas, siga estos pasos:

1. Acceda a la página **Red**, seleccione una red y haga clic en **Más**. A continuación, seleccione la pestaña **CAA**.
2. Introduzca sus credenciales de cisco.com en los campos proporcionados. De manera opcional, puede seleccionar una etiqueta para que se aplique a la carga.
3. Asegúrese de que la casilla de verificación **Cargar automáticamente los dispositivos descubiertos recientemente** esté marcada.
4. Haga clic en **Guardar**. También puede ver un ejemplo de los datos que se cargarán haciendo clic en el enlace de esta página.

Para deshabilitar las cargas automáticas, siga estos pasos:

1. Acceda a la página **Red**, seleccione una red y haga clic en **Más**. A continuación, seleccione la pestaña **CAA**.
2. Quite la marca de la casilla **Cargar automáticamente los dispositivos descubiertos recientemente**.
3. Haga clic en **Guardar**.

Informes del ciclo de vida

Cisco Business Dashboard proporciona información sobre el estado del ciclo de vida de cada uno de los dispositivos de Cisco de la red. Para ello, Dashboard debe facilitar a Cisco el ID de producto, el número de serie y las versiones de hardware y software de los dispositivos de Cisco. También se puede registrar la dirección IP de Dashboard. No se recopilará ninguna información confidencial o personal de forma intencionada durante este proceso.

Para deshabilitar la generación de informes de ciclo de vida, siga estos pasos:

1. Acceda a **Sistema > Configuración de privacidad**.
2. Quite la marca de las casillas de verificación de los informes que desee deshabilitar.
3. Haga clic en **Guardar**.

Mejora del producto

Al habilitar esta función, Cisco Business Dashboard envía periódicamente información de uso de los productos de hardware y software a Cisco. También se puede registrar la dirección IP de Dashboard. No se recopilará ninguna información confidencial o personal de forma intencionada durante este proceso.

Para ver un ejemplo de la información que se envía, haga lo siguiente:

1. Acceda a **Sistema > Configuración de privacidad**.
2. Haga clic en el enlace **Ver una muestra** que figura junto a la casilla de verificación **Enviar datos de Mejora del producto a Cisco**. Se mostrará un ejemplo de una carga con datos de muestra.

Para deshabilitar la generación de datos de mejora del producto, siga estos pasos:

1. Acceda a **Sistema > Configuración de privacidad**.
2. Quite la marca de la casilla de verificación **Enviar datos de Mejora del producto a Cisco**.
3. Haga clic en **Guardar**.

Actualizaciones de software

El uso de esta función requiere que Cisco Business Dashboard envíe a Cisco el ID del producto y la información sobre la versión del hardware y el software de cada dispositivo. Puede que también se registre su dirección IP local. No se recopilará ninguna información confidencial o personal de forma intencionada durante este proceso.

Para deshabilitar el uso de las actualizaciones automáticas de software, siga estos pasos:

1. Acceda a **Sistema > Configuración de privacidad**.
2. Quite la marca de las casillas de verificación de las comprobaciones de firmware del dispositivo y las comprobaciones de la aplicación de Cisco Business Dashboard.
3. Haga clic en **Guardar**.

Administración de la configuración de registro

La página **Configuración de registro** permite controlar el nivel de detalle de los archivos de registro de los diferentes módulos de software. El nivel de registro predeterminado es **Información**, pero puede reducir el número de mensajes registrados seleccionando **Advertencia** o **Error**, o ver más detalles seleccionando **Depurar**.

Para cambiar los niveles de registro de Dashboard, haga lo siguiente:

1. Acceda a **Sistema > Configuración de registro**.
2. Use los botones de opción para elegir el nivel de registro deseado para cada módulo de software.
3. Haga clic en **Save** (Guardar)

Los archivos de registro de Dashboard se encuentran en el directorio `/var/log/ciscobusiness/dashboard/` del sistema de archivos local. Puede hacer clic en **Descargar archivo de registro** para descargar un archivo con el contenido de este directorio. Puede que lleve varios minutos recopilar todos los datos.

Inicio de sesión en Syslog

A partir de la versión 2.2.1, los registros de aplicación de Cisco Business Dashboard pueden enviarse al servicio Syslog del host y desde allí pueden dirigirse a servidores Syslog externos.

Para habilitar el envío de archivos al servicio syslog del host, haga lo siguiente:

1. Inicie sesión en el sistema operativo del host con SSH o mediante la consola y edite el archivo `/etc/ciscobusiness/dashboard/cisco-business-dashboard-logger.conf`
2. Edite las líneas `xxx.logger` para especificar **archivo**, **syslog** o ambos (separados por una coma). Los siguientes módulos están disponibles: `redis`, `mongo`, `rabbitmq`, `nginx` y `cbd`. Si se especifica el **archivo**, los mensajes de registro se dirigirán a los archivos de registro predeterminados en el directorio `/var/log/ciscobusiness/dashboard/`. Si se especifica **syslog**, los mensajes de registro se dirigirán al servicio syslog en el host.

**Nota**

El módulo `mongo` no es compatible con varios destinos de registro. Si se enumeran varios destinos, la primera entrada tiene prioridad. Además, el módulo `cbd` siempre se registrará en el sistema de archivos independientemente de la presencia o ausencia de la palabra clave **file** en la configuración del registrador.

3. De manera opcional, modifique las líneas `xxx.syslog.facility` para especificar el recurso `syslog` utilizado para cada uno de los módulos. De forma predeterminada, cada módulo se registra en una instalación local `<n>` independiente donde `<n>` oscila entre 1 y 5.
4. Reinicie Cisco Business Dashboard con el comando **cisco-business-dashboard stop** seguido de **cisco-business-dashboard start**.

Cuando la configuración de registro se haya modificado para dirigir los mensajes de registro a **syslog**, el archivo `/etc/rsyslog.conf` debe actualizarse para recibir los registros y dirigir los mensajes de registro del panel al destino deseado. Para obtener información detallada sobre el archivo de configuración, consulte <https://www.rsyslog.com/doc/v8-stable/configuration/index.html>.

Ejecute los siguientes pasos:

1. El archivo `/etc/rsyslog.conf` debe actualizarse para permitir que se reciban mensajes de registro en la interfaz de bucle invertido. Edite el archivo para incluir las siguientes líneas para habilitar esto y restringir que el servidor escuche *solo* en la interfaz de bucle invertido:

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514" address="::1")
input(type="imudp" port="514" address="127.0.0.1")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514" address="::1")
input(type="imtcp" port="514" address="127.0.0.1")
```

2. Cree un nuevo archivo en el directorio `/etc/rsyslog.d/` para contener las directrices de configuración específicas de Cisco Business Dashboard. El nombre del archivo debe tener un formato similar a `40-cisco-business-dashboard-syslog.conf`.
3. Edite el archivo creado en el paso 2 para contener las directrices para enviar la salida del resultado a los destinos deseados. Por ejemplo, suponiendo el uso de las instalaciones predeterminadas en el archivo `cisco-business-dashboard-logger.conf`, la siguiente configuración dirigiría el nivel de advertencia y los mensajes anteriores de la aplicación del panel al servidor `syslog` con el nombre `logger.example.com`:

```
local2.warning @logger.example.com
```

4. Reinicie el daemon de `rsyslog` para aplicar los cambios utilizando el comando **sudo systemctl restart rsyslog.service**

Gestión de Probe local



Nota Esta página no está incluida en Cisco Business Dashboard para AWS.

Cisco Business Dashboard Probe puede instalarse en el mismo host que Cisco Business Dashboard para administrar dispositivos en la red local de Dashboard y la imagen de máquina virtual de Cisco para Dashboard incluye Probe. Si no desea gestionar la red local de Dashboard, puede deshabilitar el Probe ubicado en el mismo lugar llevando a cabo estos pasos:

1. Acceda a **Sistema > Probe local**.
2. Haga clic en el botón conmutador para deshabilitar el Probe local.
3. Haga clic en **Guardar**.

Para eliminar completamente el software Probe de Dashboard, inicie sesión en el sistema operativo y utilice el comando `sudo apt-get --purge autoremove cbd-probe`. Se eliminan el software, la configuración y las dependencias de Probe que no sean necesarias para ninguna otra aplicación.



CAPÍTULO 13

Notificaciones

Este capítulo contiene las siguientes secciones:

- [Acerca de Notificaciones, en la página 95](#)
- [Notificaciones admitidas, en la página 95](#)
- [Visualización y filtrado de notificaciones actuales del dispositivo, en la página 97](#)
- [Visualización y filtrado de notificaciones históricas del dispositivo, en la página 98](#)

Acerca de Notificaciones

Cisco Business Dashboard genera notificaciones cuando se producen distintos eventos en la red. Una notificación puede generar un mensaje de correo electrónico o una alerta emergente que aparece en la esquina inferior derecha del navegador. Todas las notificaciones se registran para revisarlas posteriormente. Las notificaciones también se pueden confirmar cuando ya no sean de interés. En este caso, quedarán ocultas en el **Centro de notificaciones** de forma predeterminada.

Notificaciones admitidas

En la siguiente tabla, se enumeran las notificaciones compatibles con Cisco Business Dashboard:

Tabla 27: Notificaciones admitidas

Evento	Nivel	Descripción	¿Se borra automáticamente?
Notificaciones del dispositivo			
Alcance/Dispositivo detectado	generada por el usuario	Se detecta un nuevo dispositivo en la red.	Sí, 5 minutos después de la detección del dispositivo.
Alcance/Dispositivo inaccesible	Advertencia	Un dispositivo se reconoce mediante un protocolo de detección, pero no se puede acceder a él usando la IP.	Sí, cuando se puede volver a acceder al dispositivo mediante IP.
Alcance/Dispositivo sin conexión	Alertar	Un dispositivo deja de ser detectable en la red.	Sí, cuando el dispositivo se vuelva a detectar.

Evento	Nivel	Descripción	¿Se borra automáticamente?
Se requieren credenciales/SNMP	Advertencia	Probe no puede acceder al dispositivo a causa de un error de autenticación.	Sí, cuando Probe se autentique.
Se requieren credenciales/ID de usuario	Advertencia	Probe no puede acceder al dispositivo a causa de un error de autenticación.	Sí, cuando Probe se autentique.
Servicio del dispositivo/SNMP	Advertencia	SNMP está deshabilitado en el dispositivo.	Sí, cuando se habilite SNMP.
Servicio del dispositivo/Servicio web	Advertencia	El servicio web está deshabilitado en el dispositivo.	Sí, cuando la API del servicio web está habilitada.
Estado	Advertencia/alerta	El nivel de estado del dispositivo cambia a advertencia o alerta.	Sí, cuando el estado del dispositivo vuelva a la normalidad.
Notificaciones de soporte de Cisco			
Firmware	generada por el usuario	Una versión posterior del firmware está disponible en cisco.com.	Sí, cuando el dispositivo se actualice a la última versión.
Fin de vida útil	Advertencia/alerta	Se ha encontrado un aviso de final de ciclo de vida útil del dispositivo o se ha alcanzado un hito de final de ciclo de vida útil.	No
Caducidad del mantenimiento	Advertencia/alerta	El dispositivo está fuera de garantía o no tiene actualmente un contrato de mantenimiento activo.	Sí, si se celebra un nuevo contrato de mantenimiento.
Notificaciones sobre el estado del dispositivo			
CPU	Advertencia/alerta	El uso de la CPU del dispositivo supera los umbrales máximos.	Sí, cuando el uso de la CPU vuelve a un nivel normal.
Tiempo de actividad	Advertencia/alerta	El tiempo de actividad del dispositivo está por debajo de los umbrales mínimos.	Sí, cuando el tiempo de actividad del dispositivo supera los niveles mínimos.
Clientes conectados	Advertencia/alerta	El número de clientes conectados supera los umbrales máximos.	Sí, cuando el número de clientes conectados vuelve a un nivel aceptable.

Visualización y filtrado de notificaciones actuales del dispositivo

Para ver las notificaciones activas de un único dispositivo o de todos ellos, haga lo siguiente:

1. En la ventana **Inicio**, haga clic en el icono **Centro de notificaciones**, situado en la esquina superior derecha de la barra de herramientas global. El distintivo con el número del icono especifica el número total de notificaciones no reconocidas que están pendientes. El color del distintivo indica el nivel de gravedad más alto de los señalados actualmente.

Las notificaciones pendientes aparecen debajo de los iconos del **Centro de notificaciones**. El número del icono de gravedad señala el total de notificaciones de cada una de las siguientes categorías:

- Información (icono de círculo verde)
- Advertencia (icono triangular naranja)
- Alerta (icono triangular invertido rojo)

2. En el **Centro de notificaciones**, puede realizar las siguientes acciones:

- Confirmar una notificación: marque la casilla situada junto a la notificación para confirmarla. Para confirmar todas las notificaciones que se muestran, marque la casilla **CONF TODO**.
- Filtrar las notificaciones que se muestran: en el siguiente paso, se proporcionan instrucciones para esta acción.

3. El cuadro Filtrar limita las notificaciones que aparecen en la tabla. De forma predeterminada, se mostrarán las notificaciones de todos los tipos y todos los niveles de gravedad. Si desea cambiar un filtro existente, haga doble clic en ese filtro para modificar la configuración. Para añadir un nuevo filtro, haga clic en la etiqueta Añadir filtro y seleccione un filtro de la lista desplegable. Tiene a su disposición los siguientes filtros:

Tabla 28: Filtros disponibles

Filtrar	Descripción
Tipo de notificación	El tipo de notificación que se debe mostrar. Por ejemplo, para mostrar notificaciones de dispositivos que no tengan conexión, elija Dispositivo sin conexión en la lista desplegable.
Gravedad	El nivel de gravedad de las notificaciones que se deben mostrar. Estos son algunos ejemplos: <ul style="list-style-type: none"> • Información • Advertencia • Alertar Puede incluir mayores niveles de gravedad marcando la casilla Mayor .
Include Ack (Incluir confirmaciones)	Permite incluir las notificaciones que se han confirmado.

Filtrar	Descripción
Red	Muestra las notificaciones de las redes especificadas. Comience a escribir en el filtro y las redes coincidentes aparecerán en una lista desplegable. Haga clic para seleccionar la red que desee. Puede incluir varias redes en el filtro.
Dispositivo	Muestra las notificaciones de los dispositivos especificados. Comience a escribir en el filtro y los dispositivos coincidentes aparecerán en una lista desplegable. Haga clic para seleccionar el dispositivo que desee. Puede incluir varios dispositivos en el filtro.



Nota Las notificaciones para cada dispositivo se pueden ver en los paneles **Información básica** e **Información detallada** del dispositivo.

Para controlar cómo recibe las notificaciones, cambie la configuración de estas en el nivel de organización o sistema. Para obtener más información, consulte [Administración de las organizaciones](#) o [Cambio de los valores predeterminados de supervisión, en la página 75](#).

Visualización y filtrado de notificaciones históricas del dispositivo

La aparición o el cambio de estado de las notificaciones se registra como un evento en Dashboard y puede verse a través del registro de eventos. Se puede ver un subconjunto del registro de eventos a través de los paneles **Información básica** o **Detalles del dispositivo** de dispositivos individuales. El panel **Información básica** solo muestra los eventos de las últimas 24 horas, mientras que el panel **Detalles del dispositivo** muestra todos los datos históricos del dispositivo disponible. Los eventos del panel **Detalles del dispositivo** pueden filtrarse para ayudar a separar aquellos eventos que resulten de interés. Consulte [Acerca del registro de eventos](#) para obtener más información sobre cómo ver y filtrar el historial de eventos.



CAPÍTULO 14

Resolución de problemas

Este capítulo contiene las siguientes secciones:

- [Captura de la información de diagnóstico de red, en la página 99](#)
- [Administración de la configuración del registro de Probe, en la página 100](#)

Captura de la información de diagnóstico de red

La función **Mostrar información técnica de la red** permite capturar fácilmente información de diagnóstico sobre la red en un formulario que se puede analizar posteriormente o enviar a un ingeniero de soporte. Se puede generar información con la función **Mostrar información técnica** desde la interfaz de usuario de Manager o directamente desde la de Probe en caso de que esté solucionando algún problema con la conexión entre Dashboard y Probe. Para capturar información con la función **Mostrar información técnica de la red**, siga estos pasos:

1. Acceda a **Red** y seleccione la red de la que desea recopilar información de diagnóstico. Seleccione la pestaña **Acciones** y haga clic en **Mostrar información técnica**.
También puede iniciar sesión en la interfaz de usuario de Probe y acceder a **Resolución de problemas > Mostrar información técnica de la red**.
2. Use las casillas para controlar si se deben excluir o no las contraseñas y los certificados de las configuraciones de dispositivos y dónde se debe enviar la información de diagnóstico. Están disponibles las siguientes opciones:
 - Adjuntar la información de diagnóstico a un caso de soporte de Cisco existente. Para esto, escriba el número de caso en el campo correspondiente.
 - Enviar la información de diagnóstico por correo electrónico. Escriba una lista de direcciones de correo electrónico separadas por comas en el campo especificado.
 - Descargar la información de diagnóstico en su PC.

Si va a generar la información de **Mostrar información técnica de la red** desde Probe, no dispone de las opciones para enviarla por correo electrónico o adjuntarla a un caso de soporte. Debe descargar la información de diagnóstico en su PC.

3. Haga clic en **Recopilar datos de diagnóstico**.

La información de diagnóstico se proporciona en un archivo zip y contiene una página web básica para facilitar la exploración de los datos recopilados. Para acceder a los datos, haga lo siguiente:

1. Descomprima el archivo de información de diagnóstico en la ubicación que desee de su PC.
2. Use un navegador web para abrir el archivo index.html ubicado en el directorio que ha creado.

Administración de la configuración del registro de Probe

La pestaña **Configuración de registro** de Dashboard puede administrarse desde la interfaz de usuario de Manager o directamente desde la de Probe en caso de que esté solucionando algún problema con la conexión entre Dashboard y Probe. La configuración del registro determina qué información debe almacenar Probe en sus archivos de registro. Esta información reviste interés principalmente para ayudar a los ingenieros que diagnostican problemas con Cisco Business Dashboard.

Para cambiar la configuración del registro de una red determinada, acceda a **Red** y seleccione la red de la que desea cambiar la configuración. Haga clic en **Más** para mostrar el panel **Network Detail** (Detalles de la red) y, a continuación, seleccione la pestaña **Configuración de registro**. También puede iniciar sesión en la interfaz de usuario de Probe y acceder a **Administración > Configuración de registro**.

La configuración disponible incluye los siguientes parámetros:

Tabla 29: Configuración de registro

Campo	Descripción
Nivel de registro	<p>El nivel de detalle que se debe registrar. Están disponibles las siguientes opciones:</p> <ul style="list-style-type: none"> • Error: solo mensajes de error. • Advertencia: errores y advertencias. • Información (valor predeterminado): mensajes informativos y de nivel superior. • Depurar: todos los mensajes, incluidos los de depuración de poca importancia.

Campo	Descripción
Módulo de registro	<p>Módulo para el que se deben registrar los mensajes. Están disponibles las siguientes opciones:</p> <ul style="list-style-type: none">• Todos (predeterminado): todos los módulos• Agente con notificación de instalación: comunicación entre Probe y Dashboard• Detección: eventos de detección de dispositivos y detección de topología• Sentido ascendente: comunicación entre Dashboard y Probe• Servicios: traducción de mensajes entre el sentido ascendente y el descendente• Sentido descendente: comunicación de bajo nivel entre Probe y los dispositivos• Sistema: proceso del sistema central que no cubra cualquier otro módulo <p>Puede seleccionar varios módulos según sea necesario.</p>

Los archivos de registro de Probe se incluyen en el contenido de **Mostrar información técnica de la red**. Para obtener más información sobre la opción **Mostrar información técnica de la red**, consulte la sección [Captura de la información de diagnóstico de red](#), en la página 99.



CAPÍTULO 15

Preguntas frecuentes

En este capítulo, se responden las preguntas frecuentes sobre las funciones de Cisco Business Dashboard y los problemas que se pueden producir. Los temas se organizan en las siguientes categorías:

- [Preguntas frecuentes generales, en la página 103](#)
- [Preguntas frecuentes sobre detección, en la página 103](#)
- [Preguntas frecuentes sobre configuración, en la página 104](#)
- [Preguntas frecuentes sobre consideraciones de seguridad, en la página 104](#)
- [Preguntas frecuentes sobre el acceso remoto, en la página 107](#)
- [Preguntas frecuentes sobre la actualización del software, en la página 108](#)

Preguntas frecuentes generales

- Q. ¿Qué idiomas son compatibles con Cisco Business Dashboard?
- A. Cisco Business Dashboard se ha traducido a los siguientes idiomas:
- Chino
 - Inglés
 - Francés
 - Alemán
 - Japonés
 - Español

Preguntas frecuentes sobre detección

- Q. ¿Qué protocolos usa Cisco Business Dashboard para administrar mis dispositivos?
- A. Cisco Business Dashboard usa diversos protocolos para detectar y administrar las redes. Los protocolos exactos que se usarán para un dispositivo concreto varían según los tipos de dispositivos.

Entre los protocolos utilizados, podemos destacar los siguientes:

- Detección de servicios DNS y DNS multidifusión (también conocidos como *Bonjour*, consulte los *RFC 6762* y *6763*)

- Protocolo de detección de Cisco (CDP)
- Protocolo de detección de capa de enlace (consulte la *especificación IEEE 802.1AB*)
- Protocolo simple de administración de red (SNMP)
- RESTCONF (consulte <https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/>)
- API de servicios web propias

Q. ¿Cómo detecta Cisco Business Dashboard las redes?

A. Cisco Business Dashboard Probe elabora una lista inicial de dispositivos de la red a partir de los anuncios de CDP, LLDP y mDNS. A continuación, Probe se conecta a cada dispositivo usando un protocolo compatible y recopila información adicional, como las tablas de adyacencia CDP y LLDP, las tablas de direcciones MAC y las listas de dispositivos asociados. Esta información se usa para identificar dispositivos adicionales de la red. El proceso se repite hasta que se hayan detectado todos los dispositivos.

Q. ¿Realiza Cisco Business Dashboard exploraciones de red?

A. Cisco Business Dashboard no explora activamente la red. Probe usará el protocolo ARP para explorar la subred IP a la que está directamente asociado pero no tratará de explorar otros rangos de direcciones. Probe también probará todo dispositivo detectado en busca de un servidor web y un servidor SNMP en los puertos estándar.

Preguntas frecuentes sobre configuración

Q. ¿Qué sucede cuando se detecta un nuevo dispositivo? ¿Cambiará su configuración?

A. Se agregarán nuevos dispositivos al grupo de dispositivos predeterminado. Si se han asignado perfiles de configuración al grupo de dispositivos predeterminado, esa configuración se aplicará a los dispositivos recién detectados.

Q. ¿Qué sucede cuando muevo un dispositivo de un grupo de dispositivos a otro?

A. Se eliminará cualquier configuración de VLAN o WLAN asociada con perfiles que se apliquen actualmente al grupo de dispositivos original y que no se apliquen también al nuevo grupo de dispositivos. Por otra parte, se agregarán al dispositivo las configuraciones VLAN o WLAN asociadas con perfiles que se apliquen al nuevo grupo y que no se apliquen al grupo original. Los ajustes de configuración de sistema se sobrescribirán con los perfiles aplicados al nuevo grupo. Si no se han definido perfiles de configuración de sistema para el nuevo grupo, la configuración de sistema del dispositivo no cambiará.

Preguntas frecuentes sobre consideraciones de seguridad

Q. ¿Qué rangos de puertos y protocolos requiere Cisco Business Dashboard?

A. En la siguiente tabla, se muestran los protocolos y los puertos que usa Cisco Business Dashboard:

Tabla 30: Cisco Business Dashboard - Protocolos y puertos

Puerto	Dirección	Protocolo	Uso
TCP 22	Tácticas	SSH	Acceso de línea de comandos a Dashboard. SSH está deshabilitado de forma predeterminada en la imagen de máquina virtual de Cisco.
TCP 80	Tácticas	HTTP	Acceso web a Dashboard. Redirige a un servidor web seguro (puerto 443).
TCP 443	Tácticas	HTTPS TCP multiplexado	Acceso web seguro a Dashboard. Comunicación entre Probe y Dashboard.
TCP 50000-51000	Tácticas	HTTPS	Acceso remoto a los dispositivos.
UDP 53	Saliente	DNS	Resolución de nombres de dominio.
UDP 123	Saliente	NTP	Sincronización de tiempo.
TCP 443	Saliente	HTTPS	Acceso a los servicios web de Cisco para obtener información como actualizaciones de software, estado de soporte y avisos de fin de vida útil. Acceso a los servicios de actualización del sistema operativo y de las aplicaciones.
UDP 5353	Saliente	mDNS	Anuncios de servicio DNS multidifusión a la red local donde se anuncia Dashboard.

- Q.** ¿Qué rangos de puertos y protocolos requiere Cisco Business Dashboard Probe?
- A.** En la siguiente tabla, se muestran los protocolos y los puertos que usa Cisco Business Dashboard Probe :

Tabla 31: Cisco Business Dashboard - Protocolos y puertos

Puerto	Dirección	Protocolo	Uso
TCP 22	Tácticas	SSH	Acceso de línea de comandos a Probe. SSH está deshabilitado de forma predeterminada en la imagen de máquina virtual de Cisco.
TCP 80	Tácticas	HTTP	Acceso web a Probe. Redirige a un servidor web seguro (puerto 443).
TCP 443	Tácticas	HTTPS	Acceso web seguro a Probe.

Puerto	Dirección	Protocolo	Uso
UDP 5353	Tácticas	mDNS	Anuncios de servicio DNS multidifusión desde la red local. Usado para la detección de dispositivos
UDP 53	Saliente	DNS	Resolución de nombres de dominio.
UDP 123	Saliente	NTP	Sincronización de tiempo
TCP 80	Saliente	HTTP	Administración de dispositivos sin la seguridad de servicios web habilitada.
UDP 161	Saliente	SNMP	Administración de dispositivos de red.
TCP 443	Saliente	HTTPS TCP multiplexado	Administración de dispositivos con la seguridad de servicios web habilitada Acceso a los servicios web de Cisco para obtener información como actualizaciones de software, estado de soporte y avisos de fin de vida útil. Acceso a los servicios de actualización del sistema operativo y de las aplicaciones. Comunicación entre Probe y Dashboard.
UDP 5353	Saliente	mDNS	Anuncios de servicio DNS multidifusión a la red local donde se anuncia Probe.

- Q.** ¿Cuánta seguridad hay en la comunicación entre Cisco Business Dashboard y Probe?
- A.** Todas las comunicaciones entre Dashboard y Probe se cifran con una sesión TLS 1.2 autenticada con certificados de servidor y cliente. La sesión se inicia desde Probe hasta Dashboard. Cuando se establece por primera vez la asociación entre Dashboard y Probe, el usuario debe iniciar sesión en Dashboard a través de Probe.
- Q.** ¿Tiene Cisco Business Dashboard acceso de "puerta trasera" a mis dispositivos?
- A.** No. Cuando Cisco Business Dashboard detecta un dispositivo compatible, intenta acceder al dispositivo usando las credenciales predeterminadas de fábrica de dicho dispositivo con el nombre de usuario y la

contraseña "cisco" o la comunidad SNMP "public". Si la configuración del dispositivo no es la predeterminada, el usuario deberá especificar las credenciales correctas en Cisco Business Dashboard.

- Q. ¿Están seguras las credenciales que se almacenan en Cisco Business Dashboard?
- A. Las credenciales para acceder a Cisco Business Dashboard se codifican mediante hash de forma irreversible mediante el algoritmo SHA512. Las credenciales para dispositivos y otros servicios, como **Cisco Active Advisor**, se cifran de forma reversible mediante el algoritmo AES-128.
- Q. ¿Cómo recupero una contraseña perdida para la interfaz de usuario web?
- A. Si ha perdido la contraseña para todas las cuentas de administración de la interfaz de usuario web, la puede recuperar iniciando sesión en la consola de Probe y ejecutando la herramienta **cbdprobe recoverpassword** o iniciando sesión en la consola de Dashboard y ejecutando la herramienta **cisco-business-dashboard recoverpassword**. Esta herramienta restablece la contraseña de la cuenta de Cisco al valor predeterminado, que es cisco. En caso de que la cuenta de Cisco se haya eliminado, se volverá a crear la cuenta con la contraseña predeterminada. A continuación, puede ver un ejemplo de los comandos que se deben proporcionar con objeto de recuperar la contraseña usando esta herramienta.

```
cisco@cisco-business-dashboard:~$ cisco-business-dashboard recoverpassword ¿Está seguro?
(s/n) s Se recuperó la cuenta Cisco con la contraseña predeterminada recoverpassword
de Cisco Business Dashboard con éxito cisco@cisco-buisness-dashboard:~$
```



Nota Al emplear Cisco Business Dashboard para AWS, la contraseña se definirá como el ID de instancia de AWS.

- Q. ¿Cuál es el nombre de usuario y contraseña predeterminados para el cargador de arranque de la máquina virtual?
- A. Las credenciales predeterminadas de la máquina virtual son nombre de usuario: **root** y contraseña: **cisco**. Estos se pueden cambiar ejecutando la herramienta `config_vm` y respondiendo sí cuando se le pregunte si quiere cambiar la contraseña del cargador de arranque.

Preguntas frecuentes sobre el acceso remoto

- Q. Si me conecto a la interfaz de administración de un dispositivo desde Cisco Business Dashboard, ¿la sesión es segura?
- A. Cisco Business Dashboard tuneliza la sesión de acceso remoto entre el dispositivo y el usuario. El protocolo que se use entre Probe y el dispositivo dependerá de la configuración del dispositivo de extremo; en cualquier caso, Cisco Business Dashboard siempre establecerá la sesión usando un protocolo seguro si hay uno habilitado (por ejemplo, HTTPS tendrá preferencia sobre HTTP). Si el usuario está conectado al dispositivo a través de Dashboard, la sesión pasará por un túnel cifrado en su recorrido entre Dashboard y Probe, con independencia de los protocolos habilitados en el dispositivo. La conexión entre el navegador web del usuario y Dashboard siempre será del tipo HTTPS.
- Q. ¿Por qué se cierra inmediatamente mi sesión de acceso remoto en un dispositivo cuando abro una sesión de acceso remoto en otro dispositivo?
- A. Cuando se accede a un dispositivo a través de Cisco Business Dashboard, el navegador considera cada conexión como si fuera con el mismo servidor web (Dashboard) y, por lo tanto, presentará las cookies de cada dispositivo a los demás dispositivos. Si varios dispositivos usan el mismo nombre de cookie, es posible que la cookie de un dispositivo se sobrescriba con la de otro. Esto suele pasar con las cookies de sesión y el resultado es que la cookie solo es válida para el dispositivo visitado más recientemente. Los

demás dispositivos que usan el mismo nombre de cookie considerarán que la cookie no es válida y cerrarán la sesión.

- Q.** ¿Por qué falla la sesión de acceso remoto con un error como el siguiente? **Error de acceso: La entidad solicitada es demasiado grande El campo del encabezado HTTP es superior al tamaño admitido.**
- A.** Tras efectuar numerosas sesiones de acceso remoto con distintos dispositivos, el navegador tendrá un gran número de cookies almacenadas para el dominio de Dashboard. Para solucionar este problema, use los controles del navegador para borrar las cookies del dominio y, después, vuelva a cargar la página.

Preguntas frecuentes sobre la actualización del software

- Q.** ¿Cómo mantengo actualizado el sistema operativo de Dashboard?
- A.** Dashboard usa como sistema operativo la distribución Linux Ubuntu. Los paquetes y el núcleo se pueden actualizar usando los procesos estándares de Ubuntu. Por ejemplo, para realizar una actualización manual, inicie sesión en la consola con el usuario cisco e introduzca los comandos `sudo apt-get update` y `sudo apt-get upgrade`. El sistema no debe actualizarse a una nueva versión de Ubuntu y se recomienda no instalar otros paquetes aparte de los que suministra Cisco en la imagen de la máquina virtual o los instalados como parte de una instalación mínima de Ubuntu.
- Q.** ¿Cómo actualizo Java en Dashboard?
- A.** Cisco Business Dashboard utiliza los paquetes OpenJDK de los repositorios de Ubuntu. OpenJDK se actualizará automáticamente como parte de la actualización del sistema operativo central.
- Q.** ¿Cómo mantengo actualizado el sistema operativo de Probe?
- A.** Cisco Business Dashboard usa como sistema operativo la distribución Linux Ubuntu. Los paquetes y el núcleo se pueden actualizar usando los procesos estándares de Ubuntu. Por ejemplo, para realizar una actualización manual, inicie sesión en la consola con el usuario cisco e introduzca los comandos `sudo apt-get update` y `sudo apt-get upgrade`. El sistema no debe actualizarse a una nueva versión de Ubuntu y se recomienda no instalar otros paquetes aparte de los que suministra Cisco en la imagen de la máquina virtual o los instalados como parte de una instalación mínima de Ubuntu.
- Q.** ¿Cómo mantengo actualizado el sistema operativo de Probe al utilizar Raspberry Pi?
- A.** Los paquetes y kernel de Raspbian pueden actualizarse mediante los procesos estándar utilizados para las distribuciones de Linux basadas en Debian. Por ejemplo, para realizar una actualización manual, inicie sesión en la consola con el usuario cisco e introduzca los comandos `sudo apt-get update` y `sudo apt-get upgrade`. El sistema no debería actualizarse a una nueva versión principal de Raspbian. Se recomienda que no se instalen paquetes adicionales más allá de los instalados como parte de la versión "Lite" de la distribución de Raspbian y los añadidos por el instalador de Probe.



CAPÍTULO 16

Apéndice A: Administración de plantillas de configuración

Este apéndice está formado por las siguientes secciones:

- [Descripción general, en la página 109](#)
- [Sintaxis de configuración, en la página 109](#)
- [Creación de plantillas de configuración, en la página 112](#)

Descripción general

Las plantillas de configuración se pueden utilizar cuando hay varios dispositivos que tienen requisitos de configuración muy similares, pero hay una pequeña cantidad de parámetros que deben ser diferentes para cada dispositivo. Por ejemplo, una red puede utilizar una configuración idéntica para todos los conmutadores, pero cada conmutador tiene un nombre de host y una dirección IP de administración únicos. Las plantillas de configuración permiten tener un solo archivo de configuración que contiene toda la configuración común, con marcadores de posición para los elementos de la configuración que deben ser únicos.

Hay dos partes en una plantilla de configuración: la configuración propiamente dicha y los metadatos que controlan cómo se presentan los marcadores de posición en la interfaz de usuario cuando se crea un registro de dispositivos. Las siguientes secciones describen estas tareas en detalle.

Sintaxis de configuración

La parte de configuración de una plantilla de configuración es un documento de texto muy similar a la configuración de un dispositivo normal. De hecho, cuando se crea una plantilla de configuración, la estrategia recomendada es partir de una copia de seguridad de la configuración tomada de un dispositivo de muestra que ya esté configurado con las características y los ajustes que la plantilla debe habilitar. Una plantilla de configuración difiere de la configuración de un dispositivo en que los parámetros específicos del dispositivo, como el nombre de host, se sustituyen por marcadores de posición. Cuando se crea un nuevo registro de dispositivo, se le presenta un formulario que le permite especificar los valores correctos para cada uno de los marcadores de posición de la plantilla de configuración. Estos valores se combinan con la plantilla de configuración para generar la configuración real que se enviará al dispositivo.



Nota Los valores de los marcadores de posición se combinan con la plantilla de configuración en el momento en que la configuración se envía al dispositivo. Esto significa que la configuración final del dispositivo puede ser diferente de la que se muestra en la vista previa si cualquier variable del sistema cambia antes de que el dispositivo se conecte al administrador.

Las configuraciones se crean como plantillas de Mustache <https://mustache.github.io/>. Mustache permite el uso de diversos marcadores de posición, conocidos como etiquetas en la documentación de Mustache, entre ellos:

- Variables simples, en las que el marcador de posición se sustituye por el valor especificado en el registro del dispositivo. Una variable simple tiene el formato `{{name}}`.
- Secciones, en las que el marcador de posición engloba un bloque de configuración, que incluye de manera opcional otros marcadores de posición. El contenido de la sección puede excluirse de la configuración final, incluirse una vez o repetirse varias veces. El comportamiento de este tipo de marcador de posición viene definido por los metadatos de la plantilla y los valores que el usuario proporciona al crear un registro de dispositivo. Una sección tiene el formato `{{#name}}...{{/name}}`, en el que la primera etiqueta marca el inicio del bloque y la segunda marca el final.
- Comentarios que se pueden utilizar para documentar la plantilla de configuración. Un comentario tiene el formato `{{! Comentario}}`.

A continuación, se muestra un ejemplo de una plantilla simple:

```
!
hostname {{hostname}}
!
{{! Insert a list of VLANs}}
{{#vlans}}
interface vlan {{vlan-id}}
  name {{vlan-name}}
!
{{/vlans}}
```

En este ejemplo, hay varios marcadores de posición diferentes:

- `{{hostname}}` es una variable simple. Se reemplazará por el valor establecido para el nombre de host en el registro del dispositivo.
- Hay un comentario que se coloca justo después de la configuración del nombre de host. El comentario no se incluirá en la configuración enviada al dispositivo.
- `{{#vlans}}...{{/vlans}}` es una sección que se utiliza en este ejemplo para mantener una lista de VLAN individuales. Para cada VLAN definida en el registro del dispositivo, se creará una copia del contenido de este contenedor en la configuración del dispositivo.
- `{{vlan-id}}` y `{{vlan-name}}` son variables simples, pero se incluyen en la lista `{{#vlans}}`. Cuando se crea el registro del dispositivo, puede especificar varios valores para `{{vlan-id}}` y `{{vlan-name}}` que se usarán para generar la configuración necesaria para crear cada una de esas VLAN.

Para obtener más detalles sobre la sintaxis de Mustache, consulte la página de Mustache en <https://mustache.github.io/mustache.5.html>.

Metadatos de la plantilla

Cada plantilla de configuración contiene metadatos que describen cómo se debe presentar cada marcador de posición al usuario cuando se crean los registros de dispositivos. Estos metadatos se generan al crear plantillas con el editor de plantillas. Cuando crea o edita una plantilla de configuración, el editor de plantillas se muestra con la configuración en la izquierda y un formulario a la derecha que le permite establecer los metadatos para cada marcador de posición.

Cada marcador de posición de la configuración se muestra a la derecha, junto con los siguientes controles:

- Una casilla de verificación **obligatoria**. Este control determina si el usuario debe proporcionar un valor para este marcador de posición o no.
- Una lista desplegable de **tipos**. Esta le permite seleccionar el tipo de marcador de posición, que controla cómo se muestra dicho marcador de posición al usuario.
- Un **título**. Este puede utilizarse para proporcionar un nombre más intuitivo para el parámetro en la GUI. Si no se especifica un título para un marcador de posición, se muestra el propio marcador de posición.
- Un icono de **edición**. Algunos tipos tienen más configuraciones disponibles para controlar la presentación. Por ejemplo, un marcador de posición de cadena puede delimitarse aún más para que sea una dirección IP o URI y el formulario de entrada mostrará un error si el texto introducido tiene el formato correcto. Algunos tipos también pueden configurarse en función de la información del sistema, en lugar de la entrada del usuario. Consulte Variables del sistema y dinámicas a continuación para obtener más detalles.
- Controles de **subida/bajada**. Estas flechas le permiten cambiar el orden en el que se muestran los marcadores de posición al usuario. Los marcadores de posición se pueden agrupar en función de lo que sea más lógico para el usuario, en lugar de hacerlo con el orden en que aparecen en la configuración.

El editor de plantillas también proporciona una función de vista previa que se puede utilizar para proporcionar un ejemplo de cómo se mostrará el formulario de marcadores de posición al usuario al crear y editar registros de dispositivos.

Tipos de marcadores de posición

Se dispone de los siguientes tipos de marcadores de posición:

- Cadena: los marcadores de posición de este tipo se mostrarán en la GUI como un simple cuadro de entrada de texto.
- Número entero: los números enteros se muestran como un cuadro de entrada de texto con controles para aumentar o disminuir el valor del número que se muestra. Solo se pueden introducir números en este campo.
- Booleano: un marcador de posición booleano se muestra en la GUI como una casilla de verificación. Si se marca la casilla de verificación, el marcador de posición se establece en el valor de cadena "true". Si no se marca la casilla de verificación, el valor es "false". Una sección también puede designarse como booleana, en cuyo caso la configuración contenida en la sección solo se incluirá cuando se marque la casilla de verificación de la sección.
- Contenedor: el contenedor se puede utilizar para agrupar otros marcadores de posición en el formulario.
- Lista: una lista es un contenedor o una sección de configuración que se puede repetir varias veces en un archivo de configuración generado. Cuando se generan elementos de formulario para los marcadores de posición dentro de una lista, se añaden controles adicionales para agregar o eliminar los elementos de la lista.

Además de los tipos simples enumerados anteriormente, las variables de cadena se pueden delimitar aún más haciendo clic en el icono **Editar**. Estas son algunas de las opciones disponibles:

- Especificar un valor predeterminado para el marcador de posición.
- Establecer la longitud mínima o máxima de los marcadores de posición de cadena.
- Especificar una lista predefinida de opciones que se pueden seleccionar (usando la opción Enum).
- Limitar el formato de una cadena para que sea una de nombre de host, URI, dirección IPv4 o dirección IPv6. Una cadena también puede designarse como un área de texto si es probable que haya una cantidad importante de contenido que introducir.

Variables del sistema y dinámicas

Es posible que los marcadores de posición no solo tomen sus valores de la entrada del usuario, sino que también pueden tomarlos de los parámetros definidos en el sistema. Las variables del sistema son parámetros que se han definido para el propio Manager, como la dirección IP del Manager. Al establecer que un marcador de posición tome su valor de una variable del sistema, el Manager insertará dicho valor en la configuración sin intervención del usuario. Algunas de las implementaciones más complejas pueden precisar una entrada de usuario para que las variables del sistema funcionen correctamente. Consulte [Administración de la configuración de la plataforma, en la página 86](#) para obtener más información.

Las variables dinámicas son similares a las variables del sistema, pero los valores se generan dinámicamente según la información, como el usuario que ha iniciado sesión o el grupo de dispositivos al que pertenece el dispositivo. Las variables dinámicas y del sistema se utilizan para permitir que las plantillas sean más portátiles entre dispositivos y sistemas.

Creación de plantillas de configuración

La estrategia recomendada para crear plantillas de configuración es comenzar con la configuración de un dispositivo de red del tipo adecuado con la configuración deseada, realizar una copia de seguridad de la configuración del dispositivo y cargarla al Manager para utilizarla como punto de partida. Como alternativa, puede crear una copia de una plantilla existente mediante la función Guardar como. De cualquier manera, a partir de una configuración existente, se puede reducir el tiempo que se tarda en crear una plantilla y, además, reducir la cantidad de revisiones necesarias para lograr el resultado deseado. Al crear una nueva plantilla, deberá especificar una organización a la que pertenecerá la plantilla y los ID de producto (PID) con los que se puede utilizar la plantilla. Los ID de productos pueden contener * y ? como caracteres comodín.

Una vez que haya creado la configuración inicial, puede actualizarla mediante el siguiente proceso:

1. Navegue hasta **Plug and Play de red > Configuraciones** y, luego, abra la configuración inicial en el editor de plantillas seleccionando la configuración y haciendo clic en el icono **Editar**.
2. El editor de plantillas se muestra con el archivo de configuración inicial que se muestra a la izquierda en una ventana del editor de texto. El editor de texto admite muchas funciones de edición comunes, como buscar, reemplazar y varias secuencias de manipulación de teclas de cursor. Consulte la lista en la siguiente [Tabla 32: Comandos comunes del editor](#).

Modifique la configuración insertando marcadores de posición, como se describe en [Sintaxis de configuración](#). Cada vez que se inserta un nuevo marcador de posición, se agrega la entrada correspondiente al formulario de la derecha.

3. Modifique los metadatos asociados con cada marcador de posición utilizando el formulario de la derecha para asegurarse de que el marcador de posición se presente al usuario de la manera más adecuada. Consulte [Metadatos de la plantilla](#) más arriba para obtener más información sobre cómo especificar metadatos. Puede utilizar la función de vista previa para ver cómo se presentará el formulario al usuario cuando se crea un registro de dispositivo.
4. Repita los pasos 2 y 3 hasta que haya creado marcadores de posición para todos los parámetros de configuración que deben variar entre los dispositivos.
5. Una vez que la plantilla se haya completado como desea, haga clic en **Guardar**.



Nota

Cada vez que se guarda una plantilla, se crea una nueva versión de la misma. Las versiones anteriores de las plantillas se conservan en el Manager a menos que las elimine de forma explícita. Cuando se asigna una plantilla a un dispositivo, se asigna una versión específica de la plantilla, que es la última versión de manera predeterminada. A medida que se crean nuevas versiones, los dispositivos existentes seguirán usando la versión que se asignó cuando se crearon. No se puede eliminar una versión de plantilla que esté asignada actualmente a un dispositivo.

Tabla 32: Comandos comunes del editor

Función	Descripción	Atajos de teclado	
		PC	Mac
Seleccionar todo	Seleccionar todo el contenido del editor	Ctrl-A	Cmd-A
Eliminar línea	Elimina la parte de la línea que se encuentra después del cursor. Si esa parte consta solo de espacio en blanco, la nueva línea al final de la línea también se elimina.		Ctrl-K
Eliminar línea	Elimina la línea completa debajo del cursor, incluida la nueva línea al final	Ctrl-D	Cmd-D
Deshacer	Deshacer el último cambio	Ctrl-Z	Cmd-Z
Rehacer	Rehacer el último cambio deshecho	Ctrl-Y	Mayús-Cmd-Z Cmd-Y
Ir al comienzo del documento	Mover el cursor al inicio del documento	Ctrl-Inicio	Cmd-Arriba Cmd-Inicio
Ir al final del documento	Mover el cursor al final del documento	Ctrl-Fin	Cmd-Fin Cmd-Abajo
Ir al inicio de línea	Mover el cursor al inicio de la línea	Alt-Izquierda	Ctrl-A
Ir al final de línea	Mover el cursor al final de la línea	Alt-Derecha	Ctrl-E

Función	Descripción	Atajos de teclado	
		PC	Mac
Aplicar más sangría	Aplicar sangría a la línea o la selección actual	Ctrl-]	Cmd-]
Aplicar menos sangría	Reducir la sangría de la línea o la selección actual	Ctrl-[Cmd-[
Buscar		Ctrl-F	Cmd-F
Buscar siguiente		Ctrl-G	Cmd-G
Buscar anterior		Mayús-Ctrl-G	Mayús-Cmd-G
Reemplazar		Mayús-Ctrl-F	Cmd-Alt-F
Reemplazar todos		Mayús-Ctrl-R	Mayús-Cmd-Alt-F