GUÍA DEL USUARIO

Cisco Small Business

Guía del usuario de Cisco OnPlus Portal

Cisco y el logotipo de Cisco son marcas comerciales o registradas de Cisco Systems, Inc. y/o sus filiales en Estados Unidos y en otros países. Para ver una lista de marcas comerciales de Cisco, visite esta URL: **www.cisco.com/go/trademarks**. Las marcas comerciales de otros fabricantes a las que se hace referencia en esta documentación son propiedad de sus respectivos propietarios. El uso del término "partner" (o sus equivalentes) no implica una relación de sociedad entre Cisco y cualquier otra empresa. (1110R)

© 2012 Cisco Systems, Inc. Reservados todos los derechos.
Número de documento: 78-20568-01

Contenido

Capítulo 1: Descripción general 13

Acerca de Cisco OnPlus 13

Cisco OnPlus Network Agent 14

Capítulo 2: Introducción a Cisco OnPlus 15

Requisitos de acceso a Cisco OnPlus Portal 15

Registro de cuentas de partner en Cisco OnPlus 17

Primer inicio de sesión en Cisco OnPlus Portal 18

Agregar el primer cliente 19

Requisitos legales del Acuerdo de usuario final 20

Instalación y activación de OnPlus Network Agent en las instalaciones del cliente 21

Comprobación de la activación del cliente con el portal 28

Siguientes pasos 29

Capítulo 3: Conceptos básicos de la interfaz de usuario de Cisco OnPlus Portal 31

Descripción general de la cuenta de partner y Panel del cliente 32

Enlaces Cuenta, Soporte, Documentación y Cierre de sesión 34

Uso de menús flotantes 34

Personalización de las páginas de OnPlus Portal 35

Zona horaria utilizada para la fecha y la hora del portal 35

Avisos emergentes 36

Leyendas e información sobre herramientas 37

Cambio del fondo, tema y logotipo de OnPlus 37

Capítulo 4: Descripción general de la cuenta de partner de OnPlus 39

Página Descripción general y menús de funciones 39

Administración de clientes 41

Cómo agregar un cliente 42

Eliminación de un cliente 43

Suspensión y reanudación de una cuenta de cliente 44
Visualización de la información de contacto y ubicación del cliente 45
Edición del perfil o la dirección de un cliente 45
Actualización de la información de su cuenta de partner de OnPlus 46

Capítulo 5: Visualización de las redes de los clientes 47

Descripción general y funciones del panel 47
Detección de dispositivos 50
Uso de la barra de herramientas del panel 53
Uso de la lista de tareas pendientes 54
Filtro de dispositivos en el panel 54
Uso de la vista Topología de red 55
Funciones de Topología de red 56
Personalización de la configuración del panel 58
Uso de las opciones de la barra de herramientas del panel 61
Expansión o contracción de subárboles 63
Establecimiento de un dispositivo como dispositivo raíz de la red 63
Cómo agregar manualmente dispositivos secundarios 64
Eliminación de dispositivos ausentes o dispositivos agregados manualmente 65
Edición manual de conexiones de dispositivos (reorganización de la relación jerárquica de los dispositivos) 66
Reorganización de dispositivos del mismo nivel en la vista Topología 67
Uso de la vista Lista de dispositivos 68
Funciones de Lista de dispositivos 69
Personalización de la vista Lista de dispositivos 70
Visualización del estado de los clientes 72
Instalación y administración de las aplicaciones de OnPlus 72

Capítulo 6: Trabajar con dispositivos del cliente 75

Acceso a la ventana Información de dispositivo 75
Uso de las funciones de la ventana Información de dispositivo 76

Ajustes 78
Credenciales 80
Acceso de inicio de sesión 80
Habilitar acceso (dispositivos Cisco IOS) 82
Acceso a SNMP 82
Acceso a WMI 83
Controlador de dispositivo 84
Controladores de dispositivo para router IOS genérico y switch IOS genérico 85
Controladores de dispositivos SNMP genéricos 85
Conexión 86
Información 86
Monitores 87
Eventos 87
Firmware 87
Notas 88
Copias de seguridad 88
Solicitud de copia de seguridad de la configuración de un dispositivo 89
Carga de un archivo de configuración del dispositivo 89
Descarga, eliminación y restauración de archivos de configuración del dispositivo 89
Estadísticas de WAN (datos de rendimiento de la red WAN) 90
Soporte 91
Soporte para Instrumental de administración de Windows (WMI) 91
Cómo habilitar el acceso a WMI 92
Cómo agregar monitores de dispositivos WMI 93
Cómo deshabilitar el acceso a WMI y eliminar las credenciales de acceso 94
Edición y realización de acciones en varios dispositivos 95

Capítulo 7: Supervisión y notificaciones 99

Descripción general 99
Tipos de eventos que se pueden supervisar 99
Notificaciones de eventos 100
Proceso de configuración de monitores y notificaciones 101
Ejemplo paso a paso 101

Contacto y regla de entrega predeterminados 104
Cómo agregar y administrar contactos de entrega 104
Cómo agregar un contacto de entrega 105
Edición de un contacto de entrega 106
Eliminación de un contacto de entrega 106
Cómo habilitar o deshabilitar las notificaciones a direcciones de correo electrónico o SMS 106
Uso de las reglas de entrega 107
Directrices importantes para el uso de reglas de entrega 108
Creación de reglas de entrega 109
Visualización de las reglas de entrega 110
Edición de las reglas de entrega 111
Eliminación de reglas de entrega 112
Cómo agregar y administrar monitores de dispositivos 112
Monitores de OnPlus Network Agent predeterminados. 113
Cómo agregar y habilitar monitores de dispositivos 113
Prueba de monitoreo de dispositivos 115
Cómo habilitar y deshabilitar (poner en pausa) un monitor de dispositivos o todos los monitores 115
Eliminación de un monitor de un dispositivo 116
Descripción de los monitores de dispositivos 116
Visualización de eventos 121
Visualización de eventos para todos los clientes 122
Visualización de los eventos de un cliente 123
Visualización del historial de eventos de un dispositivo 124
Tipos de eventos 125

Capítulo 8: Conexión a dispositivos desde el portal 131

Descripción general 131
Directrices, limitaciones y advertencias para conexiones remotas 132
Directrices para todos los tipos de conexión 132
Directrices para conexiones RDP, VNC y de túnel genérico 133

Directrices de conexión web (HTTP/HTTPS) 133
Abrir conexiones RDP, VNC o de túnel genérico (SSH, Telnet) 134
Funcionamiento de las conexiones de túnel en el portal 134
Creación de conexiones RDP, VNC o de túnel genérico (SSH, Telnet) 136
Abrir una conexión web (HTTP/HTTPS) 138
Funcionamiento de las conexiones web remotas 138
Configurar y abrir una conexión web 140
Solución de problemas de configuración de conexiones web (HTTP/HTTPS) 142
Configuración de conexión web recomendada para dispositivos 143
Cerrar manualmente la conexión a un dispositivo remoto 143
Habilitar o deshabilitar las conexiones a dispositivos remotos para un sitio 144

Capítulo 9: Administración y mantenimiento de dispositivos de Cisco 145

Mantenimiento automatizado del dispositivo 145
Configuración de la hora de inicio de las tareas de mantenimiento 146
Copia de seguridad y restauración de la configuración del dispositivo 146
Administración del firmware para dispositivos de Cisco compatibles 147
Carga de firmware de dispositivo al portal 147
Visualización de la información de la versión del firmware cargado 148
Instalación del firmware del dispositivo 149
149

Capítulo 10: Agregar y administrar agentes autorizados 151

Descripción general 151
Invitar agentes 152
Proceso de registro de agentes 152
Aprobar o rechazar solicitudes de agentes pendientes 153
Eliminar un agente 154
Iniciar sesión como agente 154

Qué pueden ver y hacer sus agentes autorizados en el portal 155

Capítulo 11: Acceso de clientes a OnPlus Portal 157

Descripción general 157

Adición de inicios de sesión del cliente 158

Proceso de activación de inicio de sesión del cliente 159

Funciones de OnPlus disponibles para los clientes según el modo de acceso 159

Administración de inicios de sesión del cliente 161

Edición de inicios de sesión del cliente 161

Eliminación de inicios de sesión del cliente 162

Reenvío de invitaciones a inicios de sesión del cliente 162

Capítulo 12: Informes 163

Descripción general 163

Tipos de informes 164

Creación de un informe 165

Visualización de calendarios de informes 168

Previsualización y descarga de informes 168

Eliminación de informes 169

Eliminación de un calendario de informes 170

Capítulo 13: Visualización de la información de soporte de productos Cisco 171

Descripción general 171

Visualización de la información de soporte de productos para todos los clientes 172

Visualización de la información de soporte de productos para un dispositivo determinado 173

Eventos de soporte de productos 174

Incluir información de soporte de productos en los informes 174

Configuración del intervalo de los recordatorios de expiración de soporte de productos 175

Creación de reglas de entrega para notificaciones de soporte de productos 176

Capítulo 14: Mantenimiento de ON100 Network Agent 177

Modificación de la configuración de red después de la activación 177

Restablecimiento de OnPlus Network Agent 178

Restablecimiento de la configuración predeterminada en OnPlus Network Agent 179

Restablecimiento de la configuración predeterminada a través de OnPlus Portal 180

Restablecimiento de la configuración predeterminada con el botón RESET 181

LED de estado de OnPlus Network Agent 181

Desactivación de un sitio para sustituir OnPlus Network Agent (RMA) 183

Transferencia de OnPlus Network Agent a otro cliente 184

Capítulo 15: Integración de la creación de vales de servicio de Autotask 185

Compatibilidad de la versión de Autotask 186

Configuración de los ajustes de Autotask 186

Configuración de los ajustes de Cisco OnPlus Portal 189

Generación de eventos, notificaciones y vales de servicio de prueba 192

Comprobación de la creación de vales de servicio en Autotask 194

Resolución de vales automatizada (solo eventos de monitor de dispositivos) 194

Suspensión de la generación de vales de servicio para todos los clientes 194

Actualización de la información de cuentas global 195

Eliminación de la aplicación Autotask de un cliente 195

Problemas conocidos 196

Capítulo 16: Integración de la creación de vales de servicio de ConnectWise 197

Compatibilidad de la versión de ConnectWise 197

Configuración de los ajustes de ConnectWise 198
Configuración de los ajustes de Cisco OnPlus Portal 199
Generación de eventos, notificaciones y vales de servicio de prueba 202
Comprobación de la creación de vales de servicio en ConnectWise 203
Resolución de vales automatizada (solo eventos de monitor de dispositivos) 204
Suspensión de la generación de vales de servicio para todos los clientes 204
Actualización de la información de cuentas global 205
Eliminación de la aplicación ConnectWise de un cliente 205

Capítulo 17: Habilitar la aplicación Supervisión de paquetes ntop 207

Descripción general 207
Notas, limitaciones y advertencias 209
Agregar la aplicación ntop a Cisco OnPlus Portal 210
Uso de ntop con NetFlow 211
Eliminación de la aplicación Supervisión de paquetes ntop 213

Capítulo 18: Acceso de dispositivos móviles a OnPlus Portal 215

Acceso a OnPlus Portal desde un dispositivo móvil 215
Funciones de OnPlus Portal accesibles a través de la interfaz móvil 216
Funciones no admitidas por la interfaz móvil 217
Activación de un cliente desde un dispositivo móvil 218

Capítulo 19: Comentarios y soporte 219

Comunidad de soporte de Cisco OnPlus 219
Acceso de soporte a registros de OnPlus Network Agent y sitios de los clientes 219
Comprobación del estado de OnPlus Service 220
Envío de comentarios sobre Cisco OnPlus 220

Apéndice A: Recursos adicionales 221

Apéndice B: Compatibilidad con funciones y dispositivos de Cisco 223

Resumen de funciones de los dispositivos 223
Limitaciones específicas del dispositivo para funciones de OnPlus 225
ASA5505 227
UC320 228
ISR890 229
ISR de la serie 1800 de Cisco 230
IAD880 231
Cisco 2800 232
Cisco BE3000 232
Cisco Catalyst 3750 233
UC500 234
SRP500 235
ISR870 235
SA520 236
Router de servicios integrados ISR1900 237
Serie ESW500 238
WAP4410N 239
PVC2300 239
AP521 239
RV042/RV082/RV016 V. 2 240
RV042/RV082/RV016 V. 3 240
IAD2400 240
SG300 o SF300 (versión 1.0 del firmware) 242
SG300 o SF300 (versión 1.1 del firmware) 244
WS-CE520 247
WS-C2960 247
WS-C4948 248
AP541 249
AP801 250

AIR-AP1142 251
Teléfonos IP de las series 6900, 7900, 8900 y 9900 de Cisco 251
Teléfonos IP de la serie SPA300 y SPA500 252
PVC300 252
VC220 253
VC240 253
NSS300 253
Acceso remoto a través de una conexión de túnel genérico 254

1

Descripción general

Le damos la bienvenida a Cisco Small Business OnPlus Service. Para obtener más información acerca de Cisco OnPlus, consulte estas secciones:

- **Acerca de Cisco OnPlus**
- **Cisco OnPlus Network Agent**

Consulte **Introducción a Cisco OnPlus, en la página 15** para obtener información sobre cómo suscribirse y registrar su cuenta de socio de Cisco OnPlus, iniciar sesión en OnPlus Portal, crear cuentas de clientes y activar Cisco OnPlus Network Agent con el portal.

Acerca de Cisco OnPlus

Cisco OnPlus™ Service es una plataforma alojada en la nube de fácil instalación que permite a los socios del canal proporcionar de forma rentable servicios de red administrados a sus clientes mediante la detección y la supervisión de toda la red de la pequeña empresa, además de la creación de informes y la administración remota. Los socios pueden acceder a las redes de sus clientes desde cualquier lugar, en cualquier momento, a través de un portal seguro y utilizando cualquier PC, tableta o dispositivo móvil junto con otras herramientas de Supervisión y administración remotas (RMM) que pueda utilizar e integrándolos con las herramientas de Automatización de servicios profesionales (PSA) existentes.

Cisco OnPlus ofrece las siguientes funcionalidades:

- Supervisión básica de redes y dispositivos, incluido el estado activo/inactivo de los dispositivos compatibles con un sencillo sistema de avisos por medio de correo electrónico o mensajes SMS y registro de eventos.
- Topología de gráficos interactivos y vistas tabulares de la red del cliente, que ofrece un inventario de los dispositivos de la red.
- Acceso remoto desde OnPlus Portal a la administración de los dispositivos de los clientes a través de la Web (HTTP o HTTPS), Protocolo de escritorio remoto (RDP), Computación virtual en red (VNC) o conexiones de túnel genérico.

- Información detallada de los dispositivos (dirección IP, número de serie, versión del firmware, dirección MAC).
- Posibilidad de cargar y administrar firmware para dispositivos Cisco compatibles.
- Copia de seguridad y restauración de la configuración para dispositivos Cisco compatibles.
- Informes personalizados.
- Integración con aplicaciones de automatización de servicios profesionales, como ConnectWise y Autotask, para la generación automática de vales de servicio basados en eventos de red y dispositivos supervisados a través del portal.
- Acceso a la cuenta de varios usuarios (agentes autorizados).
- Acceso móvil desde teléfonos inteligentes o tabletas.
- Información de soporte de productos, contrato de servicio y garantía para dispositivos Cisco.

Cisco OnPlus Network Agent

Cisco OnPlus Network Agent es un dispositivo que se instala en las instalaciones del cliente, uno por sitio. OnPlus Network Agent actúa como un agente local que detecta los dispositivos de la red y envía y recibe datos de Cisco OnPlus Portal.

Para ver una descripción general de los pasos necesarios para instalar y activar el dispositivo OnPlus Network Agent del cliente con el portal, consulte **Introducción a Cisco OnPlus, en la página 15**.

- Para obtener información detallada acerca de la instalación de OnPlus Network Agent en la red del cliente, consulte la *Guía de inicio rápido de Cisco ON100 Network Agent*, disponible en Cisco.com, en www.cisco.com/go/onplus.
- Para leer información importante sobre requisitos previos, directrices y pasos de activación, consulte **Introducción a Cisco OnPlus, en la página 15**.

2

Introducción a Cisco OnPlus

Este capítulo incluye los pasos necesarios para familiarizarse con Cisco OnPlus, desde el registro de la cuenta de partner hasta la creación de la cuenta del cliente y la activación del servicio:

- **Requisitos de acceso a Cisco OnPlus Portal**
- **Registro de cuentas de partner en Cisco OnPlus**
- **Primer inicio de sesión en Cisco OnPlus Portal**
- **Agregar el primer cliente**
- **Requisitos legales del Acuerdo de usuario final**
- **Instalación y activación de OnPlus Network Agent en las instalaciones del cliente**
- **Comprobación de la activación del cliente con el portal**
- **Siguientes pasos**

Requisitos de acceso a Cisco OnPlus Portal

Lea esta sección para conocer información importante sobre los requisitos previos para acceder a OnPlus Portal y los requisitos de compatibilidad con el navegador Web.

Obtener credenciales de inicio de sesión en Cisco.com

Se necesitan credenciales de inicio de sesión en Cisco.com para el registro de Cisco OnPlus Portal. Si aún no tiene credenciales de inicio de sesión en Cisco.com, puede obtenerlas haciendo clic en el enlace **Registro**, en la esquina superior derecha de la página de registro de Cisco.com, y siguiendo las instrucciones que aparecen en la pantalla. Guarde su nombre de usuario y contraseña.

Convertirse en partner registrado de Cisco

Tal y como se establece en los términos y condiciones de OnPlus (sección 1.2), es necesario ser partner registrado de Cisco para obtener acceso a OnPlus Service.

Al registrarse en OnPlus Service, su cuenta se preaprueba.

- Si aún no es partner registrado, vaya a la ficha Partner en www.cisco.com y haga clic en **Hacerse partner**.
- Una vez que sea partner registrado de Cisco, envíenos un mensaje de correo electrónico a accounts-onplus@cisco.com en el que notifique su nuevo estado, e incluya su nombre, el nombre de la empresa y el nombre de usuario de OnPlus Portal.

Para obtener más información, visite la Central de partners de Cisco.com en www.cisco.com/web/partners.

Si no lleva a cabo esta solicitud en un plazo de 45 días, se podría interrumpir su cuenta, lo que incluye, pero sin limitarse a ello, su acceso a OnPlus Portal y cualquier conexión de agentes de OnPlus al servicio.

Cuando se suspende una cuenta de partner:

- Las credenciales de inicio de sesión se deshabilitan para el titular de la cuenta de partner y todos los agentes autorizados.
- Todos los sitios del cliente asociados con la cuenta se desactivan.
- Se muestra un mensaje al intentar iniciar sesión en una cuenta suspendida, junto con información de contacto.

Si la cuenta vuelve a instalarse posteriormente, todos los sitios del cliente deben activarse de nuevo.

Una vez creada la cuenta de partner en OnPlus Portal, puede invitar a otros a convertirse en agentes autorizados. Los agentes autorizados deben obtener credenciales de inicio de sesión en Cisco.com, pero no es necesario que sean partners registrados de Cisco. Para obtener más información sobre los agentes autorizados, consulte **Agregar y administrar agentes autorizados, en la página 151**.

Comprobar la compatibilidad de OnPlus Portal con navegadores web

Se recomienda el uso de las versiones más recientes de los navegadores web Mozilla Firefox e Internet Explorer con OnPlus Portal. Si accede al portal desde un equipo Mac, también puede utilizar el navegador web Safari. **No es aconsejable utilizar Microsoft Internet Explorer 6**.

IMPORTANTE Para que OnPlus Portal funcione correctamente, el navegador web no debe estar configurado para excluir el encabezado de referencia HTTP. Si se excluye, podría haber problemas al guardar o actualizar la configuración en el portal. En los navegadores más actuales esta opción está ajustada correctamente de forma predeterminada.

Se requiere Adobe Flash Player 10.1 o posterior.

La resolución de pantalla mínima recomendada para el equipo en el que se ejecuta el navegador web desde el que se accede al portal es de 1024 x 768.

Registro de cuentas de partner en Cisco OnPlus

Para registrar una cuenta de partner en Cisco OnPlus, siga estos pasos.

PASO 1 Abra un navegador web y escriba la siguiente URL:

www.cisco-onplus.com

PASO 2 Haga clic en el enlace **Registrarse ahora** que se encuentra a la derecha en la página de inicio de sesión.

Aparecerá la página de registro.

Por comodidad, en la página de inicio de sesión se incluyen enlaces a las páginas de registro de cuenta y restablecimiento de contraseña de Cisco.com.

PASO 3 En la página **Registro**, incluya la siguiente información.

- **Información de la cuenta de Cisco.com**. Utilice el ID de usuario y la contraseña de la cuenta de Cisco.com para registrarse en el portal.
- **Información de identidad**. Escriba su información de contacto. Puede editar la información posteriormente, pero deberá rellenar ahora todos los campos.

  En el campo **Dirección de correo electrónico**, escriba la dirección que se utilizará para la confirmación de la cuenta. Recibirá la URL y la información de inicio de sesión de OnPlus Portal en esa dirección de correo electrónico.

  No tiene necesariamente que utilizar la dirección que está asociada con el inicio de sesión en Cisco.com.

  IMPORTANTE La dirección de correo electrónico que incluya aquí se utilizará como destino principal para las notificaciones de OnPlus Portal. Puede cambiarla posteriormente, si lo necesita.

- **Confirmación de seguridad y privacidad**. Introduzca el código de verificación y confirme que ha leído y que acepta la Política de privacidad de Cisco.

PASO 4 Haga clic en **Enviar**.

Aparece la página **Registro completado**.

Recibirá un mensaje de correo electrónico de bienvenida en el que se le informa de que su cuenta ha sido preaprobada. Este mensaje incluye su nombre de usuario de la cuenta de partner y enlaces a información útil para familiarizarse con el servicio.

Para obtener más información, consulte **Convertirse en partner registrado de Cisco, en la página 16**.

IMPORTANTE Asegúrese de que su programa de correo electrónico admite los correos del dominio cisco-onplus.com. Si no recibe el mensaje de correo electrónico de registro según lo esperado, revise la carpeta de correo no deseado de su programa de correo electrónico.

Utilice la URL y el nombre de usuario del mensaje de correo electrónico y la contraseña de Cisco.com para acceder al portal. Consulte la siguiente sección, **Primer inicio de sesión en Cisco OnPlus Portal**.

Primer inicio de sesión en Cisco OnPlus Portal

Una vez aprobado su registro, utilice la información proporcionada en el mensaje de correo electrónico de registro y siga estos pasos para iniciar sesión en el portal por primera vez.

NOTA La sesión se cierra tras 24 minutos de inactividad.

PASO 1 Abra un navegador web y acceda a la URL que se le ha proporcionado en el mensaje de correo electrónico de registro en el portal, por ejemplo:

www.cisco-onplus.com

PASO 2 Inicie sesión.

a. En el campo **Nombre de usuario**, escriba el nombre de usuario de Cisco.com que utilizó al registrarse en OnPlus Portal. El nombre de usuario también se

incluye en el mensaje de correo electrónico de bienvenida de registro en el portal.

b. En el campo **Contraseña**, escriba la contraseña de la cuenta de Cisco.com que utilizó al registrarse en OnPlus Portal. Puede cambiar la contraseña posteriormente.

Aparecen los Términos y condiciones de Cisco OnPlus Portal.

PASO 3 Cuando haya terminado de leer los Términos y condiciones, haga clic en **Aceptar**.

El portal se actualiza y se muestra la página Descripción general. Puesto que aún no ha agregado ningún cliente, la lista de clientes está vacía y muchas de las páginas de funciones del portal no muestran contenido.

Ya está preparado para agregar una cuenta de cliente. Consulte **Agregar el primer cliente, en la página 19**.

Agregar el primer cliente

Para agregar la cuenta de un cliente, siga estos pasos.

PASO 1 En la página Descripción general, haga clic en el botón + **Agregar cliente** en la parte superior derecha de la página, debajo de la barra de navegación.

PASO 2 Para cargar una imagen de logotipo opcional para el cliente, haga clic en **Examinar**.

SUGERENCIA La carga de un logotipo es opcional. Las imágenes deben tener formato JPEG, PNG o GIF. Las imágenes con un tamaño superior a 300 x 300 píxeles se cambiarán de tamaño. Puede agregar o sustituir la imagen en cualquier momento una vez creada la cuenta.

Si la carga se realiza correctamente, se mostrará una marca de verificación y el texto **Imagen válida**. La imagen cargada no se muestra aquí. Una vez creado el cliente, podrá ver el logotipo desde la lista de clientes. Consulte **Visualización de la información de contacto y ubicación del cliente, en la página 45**.

PASO 3 Escriba la información del cliente necesaria en la sección **Perfil** y haga clic en **Siguiente**. Puede agregar o editar el perfil del cliente más tarde.

PASO 4 En la sección **Contacto**, escriba la información de contacto necesaria para ese cliente o desactive la opción **Agregar un contacto** para continuar sin agregar la información de contacto.

Los contactos se utilizan para entregar notificaciones de eventos. Puede agregar o editar los contactos más tarde. Consulte **Cómo agregar y administrar contactos de entrega, en la página 104**.

PASO 5 En la ficha **Resumen**, repase la información que ha introducido y corrija los errores, que aparecerán resaltados.

Utilice los botones **Anterior** y **Siguiente** para desplazarse por las secciones.

PASO 6 Haga clic en **Guardar**.

El portal se actualiza y muestra la página Estado del cliente que acaba de agregar.

La página de estado del cliente muestra su **ID de activación**, ya que el nuevo cliente está en estado de Activación en espera. El **ID de activación** también se muestra en la página **Perfil** del cliente (haga clic en el cliente y seleccione **Perfil** > **Perfil**). Puede copiar y pegar este ID en un editor de texto o en otro programa para utilizarlo más adelante. Este ID se utiliza para activar el dispositivo OnPlus Network Agent del cliente con el portal.

También se agrega una entrada para el nuevo cliente en la página Descripción general. La columna **Estado** indica que el cliente está en estado de **Activación en espera**, puesto que OnPlus Network Agent aún no se ha instalado y activado en las instalaciones del cliente.

Una vez agregado el primer cliente, continúe con **Instalación y activación de OnPlus Network Agent en las instalaciones del cliente, en la página 21**.

Requisitos legales del Acuerdo de usuario final

Para poder instalar un dispositivo OnPlus Network en un sitio del cliente, antes deberá obtener aprobación por escrito para las funcionalidades de supervisión de Cisco. Para ello, el cliente deberá firmar el Anexo A de los Términos y condiciones de Cisco OnPlus. De acuerdo con los Términos y condiciones de Cisco OnPlus Service, Cisco tiene el derecho de revisar sus registros para asegurar que se cumple con este requisito.

El Anexo A de los Términos y condiciones ("Consentimiento y obligaciones del usuario final") se incluye en la versión en PDF de esta guía.

Instalación y activación de OnPlus Network Agent en las instalaciones del cliente

Siga los procedimientos que se incluyen en esta sección para instalar OnPlus Network Agent y activar Network Agent con Cisco OnPlus Portal. Se tratan los siguientes temas:

- **Antes de empezar**
- **Ubicación de OnPlus Agent en la red del cliente**
- **Requisitos de acceso a puertos y protocolos**
- **Instalación de OnPlus Network Agent**
- **Activación de OnPlus Network Agent**

Antes de empezar

OnPlus Network Agent debe estar instalado en las instalaciones del cliente.

El equipo o dispositivo móvil que se utilice para activar OnPlus Network Agent con Cisco OnPlus Portal debe estar conectado a la Red de área local (LAN) o a la Red de área local inalámbrica (WLAN) de las instalaciones del cliente.

NOTA Si hay varias conexiones de red simultánea en el dispositivo que se utiliza para acceder al portal o a OnPlus Network Agent, puede haber problemas de conexión. Por ejemplo, si su equipo tiene una Tarjeta de interfaz de red (NIC) dual con una interfaz cableada y una interfaz inalámbrica, y tiene problemas de conexión con el portal, deshabilite una de las interfaces y vuelva a intentar la conexión.

Solo se instala un dispositivo OnPlus Network Agent por cada cuenta de cliente.

Antes de instalar OnPlus Network Agent, compruebe que tiene lo siguiente:

- Información de activación de Cisco OnPlus Portal para el cliente: El nombre y el **ID de activación** del cliente.

  Para localizar el **ID de activación** del cliente, inicie sesión en el portal; en la página Descripción general, haga clic en la entrada de la lista correspondiente al cliente y, a continuación, seleccione **Perfil** > **Perfil.** El **ID de activación** se encuentra en la sección OnPlus Network Agent de la página de perfil del cliente. Antes de la activación, el ID de activación también se muestra en la página de estado del cliente.

- Una fuente de alimentación para OnPlus Network Agent, ya sea un puerto de LAN con alimentación a través de Ethernet (PoE) o una toma de corriente de 100-240 VCA y 50-60 Hz.
- Una conexión a Internet activa en las instalaciones del cliente.
- Un equipo Windows, Mac o Linux con navegador web.
- Un servidor DHCP en la LAN del cliente.

NOTA Si no hay servidor DHCP en el sitio del cliente, puede hacer una instalación intermedia de OnPlus Network Agent activando al cliente en su red local antes de instalarlo en el sitio del cliente.

Para ello, active el dispositivo OnPlus Agent en la red local y, a continuación, configure la IP estática en Network Agent. Cuando OnPlus Network Agent esté instalado y conectado a la red del cliente, arrancará con la dirección IP estática.

Una vez conectado a la red del cliente, acceda a la vista Panel de ese cliente, pase el ratón sobre el icono Acciones en la barra de herramientas y, a continuación, haga clic en **Restablecimiento de datos** > **Volver a descubrir red** para eliminar toda la información de detección existente y detectar la red y los dispositivos del cliente.

Ubicación de OnPlus Agent en la red del cliente

El éxito y la exactitud del proceso de detección de dispositivos y de la representación de la topología de red puede variar en función de la ubicación de OnPlus Network Agent en la red.

Siga estas directrices para determinar la mejor ubicación de OnPlus Network Agent en la red del cliente:

- Para garantizar una óptima detección de dispositivos y representación de la topología, conecte OnPlus Network Agent al puerto LAN de un router o switch Cisco compatible con OnPlus. Para ver una lista de dispositivos Cisco compatibles con OnPlus, consulte **Resumen de funciones de los dispositivos, en la página 223**.
- Los switches que no son compatibles con CDP (Cisco Discovery Protocol, protocolo de detección de Cisco) podrían generar múltiples mensajes de CDP, dando lugar a una representación de topología imprecisa. Para corregir la topología, reorganice la relación jerárquica de los dispositivos manualmente. Consulte **Cómo agregar manualmente dispositivos secundarios, en la página 64**.

- Los switches que son compatibles con CDP pero que OnPlus Portal no admite consumirán los mensajes CDP de los dispositivos conectados tras ellos. Por consiguiente, esto limita la posibilidad de que OnPlus Agent detecte los dispositivos que se encuentran tras el switch, si esos dispositivos utilizan CDP como único método de detección (por ejemplo, los teléfonos IP de la serie Cisco 7900).
- Se recomienda situar OnPlus Network Agent en el lado de la LAN de todos los dispositivos de la red del cliente. Por ejemplo, si se instala un UC300 en una red Small Business existente tras un dispositivo de seguridad SA500 y OnPlus Agent se sitúa en el lado de la WAN del UC300, el éxito de la detección y la precisión de la topología se verán seriamente limitados. En este caso, sitúe OnPlus Agent en el lado de la LAN del UC300.
- Los routers y switches que OnPlus no admite también pueden detectarse. Sin embargo, pueden limitar seriamente la detección de OnPlus Agent y la exactitud de la topología. Es posible que se requiera la selección manual del controlador y los ajustes de la topología. Para obtener más información, consulte **Cómo agregar manualmente dispositivos secundarios, en la página 64** y **Controlador de dispositivo, en la página 84**.

Requisitos de acceso a puertos y protocolos

OnPlus Network Agent y OnPlus Portal no requieren una configuración especial y se comunicarán con el portal a través del cortafuegos. No obstante, se recomienda que los siguientes puertos estén abiertos para el tráfico de salida (no es necesario abrir ningún puerto de entrada en el cortafuegos).

- Tráfico de salida que debe estar permitido en la red que aloja el dispositivo OnPlus Network Agent:
  - Puerto 53 UDP (DNS)
  - Puerto 80 TCP (HTTP)
  - Puerto 123 UDP (NTP)
  - Puerto 443 TCP (HTTP)
  - Puertos 11300 (TCP) y 11400 (TCP)
  - Puerto 14931 (UDP), supervisión del rendimiento de red WAN a través de OnPlus Network Agent
- Tráfico de salida que debe permitirse para poder utilizar correctamente OnPlus Portal desde un navegador web:
  - Puerto 53 UDP (DNS)

- Puerto 80 TCP (HTTP)
- Puerto 443 TCP (HTTP)
- Puertos 11305 (TCP) y 11700 a través de 11800 (TCP), conexiones de túnel remotas a través del portal
- Puerto 12330 (TCP), comunicación de topología/panel en tiempo real

NOTA El tráfico de salida en estos puertos solo se bloquearía en un entorno de red altamente restrictivo. De forma predeterminada, la mayoría de los routers utilizados por las pequeñas empresas no bloquean el tráfico de salida.

Instalación de OnPlus Network Agent

Para evitar la exposición de los datos del sitio, se recomienda limitar el acceso físico al dispositivo OnPlus Network Agent. Utilice la ranura para candado y un cable de seguridad para proteger el dispositivo y evitar que se mueva sin autorización. Puede obtenerse acceso con privilegios no autorizado mediante la modificación del hardware, lo que invalida la garantía. Puesto que el puerto AUX del dispositivo no es compatible, no debe conectarse nada a él.

Siga las indicaciones de la *Guía de inicio rápido de Cisco ON100 Network Agent* para instalar el hardware de Network Agent, conectarlo a la red del cliente y alimentarlo.

La *Guía de inicio rápido de Cisco ON100 Network Agent* está disponible en Cisco.com, en www.cisco.com/go/onplus.

Activación de OnPlus Network Agent

Cuando los LED STATUS 1 y STATUS 2 de OnPlus Network Agent indiquen que el dispositivo está listo para la activación (STATUS 1 iluminado en verde y STATUS 2 apagado), siga las instrucciones de esta sección para localizar OnPlus Network Agent en la red y abrir la página de activación.

PASO 1 En el equipo conectado a la LAN del cliente, abra un navegador web e inicie sesión en Cisco OnPlus Portal.

PASO 2 Si aún no ha creado una entrada para el cliente, vaya a la página de información general de la cuenta de partner y haga clic en **+ Agregar cliente**. Tras agregar el cliente, se genera un ID de activación.

PASO 3 Acceda a la página **Estado** o **Perfil** del cliente. El estado será Activación en espera.

PASO 4 Haga clic en **Activar ahora**.

PASO 5 En la página **Activar OnPlus Network Agent**, seleccione la dirección MAC correspondiente a la unidad de OnPlus Network Agent que está instalando y, a continuación, haga clic en **Continuar con OnPlus Network Agent**.

Se muestra la página de activación en Cisco OnPlus Network Agent. El ID de activación del cliente se añade automáticamente.

Si no se muestra la dirección MAC de la unidad OnPlus Network Agent del cliente:

- Compruebe que OnPlus Network Agent está encendido y conectado a la red LAN del cliente.
- Si aparece el mensaje "**No ha sido posible determinar la dirección IP de ningún OnPlus Network Agent en su red actual**", lea la información de solución de problemas que aparece en la pantalla y asegúrese de que el entorno de red cumple los requisitos de uso de esta función:
  - OnPlus Network Agent debe estar ubicado en el mismo bloque de dirección IP de WAN pública que el navegador web que utilice para realizar la activación.
  - Compruebe que se está ejecutando el servicio de DHCP en la red local, de modo que OnPlus Network Agent pueda adquirir la dirección IP a través de DHCP. Podrá establecer una dirección IP estática para OnPlus Network Agent más adelante si así lo desea, pero el servicio de DHCP es necesario para el acceso inicial a OnPlus Network Agent.
  - Compruebe que los clientes de DHCP pueden obtener una ruta a Internet.
- Asegúrese de que el cortafuegos de la red del cliente no bloquea el tráfico de salida HTTP o HTTPS en el puerto que OnPlus Network Agent utiliza para comunicarse con el portal.
- Compruebe que no está conectado a la red a través de VPB durante la activación.

Si el método **Activar ahora** que aquí se describe no funciona, consulte **Métodos alternativos para activar OnPlus Network Agent, en la página 27** para conocer otras formas de detectar Network Agent y acceder a la página de activación.

PASO 6 Si es necesario, configure ajustes de red opcionales, como el direccionamiento IP (DHCP o Estático), servidores DNS y servidores NTP. Consulte **Configuración de ajustes de red adicionales en OnPlus Network Agent, en la página 26**.

PASO 7 Haga clic en **Activar**.

PASO 8 Compruebe que la información del cliente coincide con la del cliente cuya instalación está realizando.

PASO 9 Haga clic en **Activación completa**.

El sistema actualizará automáticamente OnPlus Network Agent con la información del perfil del cliente y actualizará el software según corresponda. Se muestran mensajes de estado para que pueda seguir el progreso de configuración del sistema. OnPlus Network Agent podría reiniciarse dos veces durante el proceso, que puede durar hasta 20 minutos, dependiendo de la velocidad de la conexión de banda ancha.

Cuando OnPlus Network Agent está activado y conectado al portal, los dos LED de estado del dispositivo se iluminan en verde fijo.

Continúe con la sección **Comprobación de la activación del cliente con el portal, en la página 28**.

Configuración de ajustes de red adicionales en OnPlus Network Agent

Puede configurar los siguientes ajustes de red opcionales para OnPlus Network Agent:

- **Dirección IP**: seleccione DHCP o Estático.
- **Servidores DNS**: utilice servidores DNS asignados a DHCP o especifique otros servidores DNS.
- **Servidores NTP**: utilice servidores NTP asignados a DHCP o especifique otros servidores NTP.

Para configurar ajustes de red opcionales para OnPlus Network Agent durante la activación, haga clic en **Configurar ajustes de red adicionales** en la página de activación.

Cuando haya terminado de hacer los cambios, haga clic en **Aplicar ajustes de red**.

Después de cambiar la dirección IP de OnPlus Network Agent, se reiniciará el dispositivo. Cuando se haya reiniciado el dispositivo, haga clic en el enlace proporcionado para acceder a OnPlus Network Agent en su nueva dirección IP.

Posteriormente puede cambiar esta configuración si lo necesita. Para modificar esta configuración tras la activación, inicie sesión en Cisco OnPlus Network Agent, haga clic en el enlace **Configuración** en la parte superior de la página y, a continuación, haga clic en **Configurar ajustes adicionales**. El nombre de usuario y la contraseña de OnPlus Network Agent se encuentran en la página del perfil del cliente en el portal.

Métodos alternativos para activar OnPlus Network Agent

Si el enlace **Activar ahora** no funciona, pruebe estos métodos alternativos para detectar OnPlus Network Agent y acceder a la página de activación.

PASO 1 Utilice uno de estos métodos para detectar OnPlus Network Agent.

- Si utiliza un navegador web con compatibilidad integrada con Bonjour (por ejemplo, Safari) o tiene instalado un complemento de navegador Bonjour, utilice el navegador Bonjour para localizar OnPlus Network Agent. El nombre en Bonjour para OnPlus Network Agent es **onplus***<últimos_6_dígitos_de_puerto_LAN_dirección_MAC>*.
- Si utiliza un PC Windows con UPnP habilitado, busque OnPlus Network Agent en el panel de red del explorador de Windows.
- Si tiene acceso al servidor DHCP en la red LAN del cliente, utilícelo para determinar la dirección IP de OnPlus Network Agent. Si necesita hacer referencia a OnPlus Network Agent por su dirección MAC, utilice la dirección MAC del puerto LAN que se encuentra en el panel posterior del dispositivo.

PASO 2 Para abrir la página de activación:

- Si ha utilizado Bonjour o UPnP para localizar OnPlus Network Agent, haga doble clic en su nombre (**onplus***<últimos_6_dígitos_de_puerto_LAN_dirección_MAC>).*
- Si conoce la dirección IP de OnPlus Network Agent, escríbala en la barra de direcciones del navegador web (por ejemplo, 192.168.10.25).

PASO 3 En la página de activación, introduzca el **ID de activación** de Cisco OnPlus Portal.

El ID de activación se muestra en la página **Perfil** del cliente en Cisco OnPlus Portal. Antes de la activación, el ID de activación se muestra en la página **Estado** del cliente en Cisco OnPlus Portal.

Copie y pegue el ID de activación en el campo correspondiente o introdúzcalo manualmente.

Continúe con el paso 6 , consulte **Activación de OnPlus Network Agent, en la página 24**.

Comprobación de la activación del cliente con el portal

Para comprobar que el sitio de un cliente está activo en el portal, siga estos pasos.

PASO 1 Inicie sesión en Cisco OnPlus Portal.

PASO 2 En la página Descripción general, localice el cliente que acaba de instalar y haga clic en la entrada para acceder a la vista Panel.

PASO 3 Seleccione **Estado**. Si el sitio del cliente se ha activado correctamente, se mostrará el estado Activado, En línea.

La primera vez que inicie sesión en el portal tras la activación inicial, no habrá información de detección disponible en el panel del cliente hasta que finalice el proceso de detección del dispositivo. Se muestra el mensaje "No hay información de análisis disponible".

Tras varios minutos, las vistas de topología de red y lista de dispositivos en el panel del cliente se actualizarán para mostrar los dispositivos detectados en la red.

NOTA En función del tamaño de la red, pueden pasar varios minutos hasta que se detectan los dispositivos y se muestran en la topología de red. La detección de dispositivos en redes más complejas y de mayor tamaño puede tardar al menos 15 minutos.

Haga clic en los elementos de la lista **Tarea pendiente** en la vista Panel del cliente para ver una lista de acciones recomendadas. Al hacer clic en un elemento, la página se actualiza y muestra todos los dispositivos que requieren atención para ese elemento.

Por ejemplo, si los dispositivos que están presentes en la red no se muestran según lo esperado, es posible que tenga que proporcionar credenciales de acceso para algunos dispositivos, como puntos de acceso, switches y routers de Cisco, con el fin de permitir la detección de dispositivos adicionales.

Continúe con la sección **Siguientes pasos, en la página 29**.

Siguientes pasos

Cuando el cliente esté activado y pueda ver su red en Topología de red, podrá comenzar a explorar las funciones de OnPlus Portal.

Los capítulos restantes de esta guía proporcionan información detallada acerca del uso de cada una de las funciones de OnPlus Portal.

Capítulo	Descripción
Conceptos básicos de la interfaz de usuario de Cisco OnPlus Portal, en la página 31	Sugerencias para utilizar la interfaz de usuario de OnPlus Portal.
Descripción general de la cuenta de partner de OnPlus, en la página 39	Desplazamiento por las listas y menús del cliente en la página Descripción general y administración de las cuentas de clientes.
Visualización de las redes de los clientes, en la página 47	Uso de las vistas del panel, Topología de red y Lista de dispositivos, para explorar y ver la topología de red y los dispositivos de cada cliente.
Trabajar con dispositivos del cliente, en la página 75	Visualización de información de dispositivos y realización de acciones en dispositivos remotos a través de Cisco OnPlus Portal.
Supervisión y notificaciones, en la página 99	Configuración de monitores de dispositivos, reglas de entrega y contactos de entrega para habilitar notificaciones de eventos supervisados a través del portal.
Conexión a dispositivos desde el portal, en la página 131	Conexión remota a dispositivos a través del portal.
Administración y mantenimiento de dispositivos de Cisco, en la página 145	Actualización de firmware y copia de seguridad y restauración de la configuración para dispositivos Cisco compatibles. También incluye instrucciones para restablecer la configuración predeterminada, reiniciar OnPlus Network Agent, desactivar un cliente y otras operaciones de mantenimiento para Cisco OnPlus Network Agent.
Agregar y administrar agentes autorizados, en la página 151	Invitaciones y administración de cuentas para agentes autorizados en Cisco OnPlus Portal.
Informes, en la página 163	Describe los informes disponibles y cómo generarlos y programarlos.

Capítulo	Descripción
Visualización de la información de soporte de productos Cisco, en la página 171	Visualización de la información de soporte de productos para dispositivos Cisco compatibles a través de OnPlus Portal. Esta información incluye contratos de servicio, garantías de productos, avisos de campo, avisos de final de ciclo de vida de software y hardware y avisos de seguridad de los productos.
Acceso de dispositivos móviles a OnPlus Portal, en la página 215	Acceso y uso de las funciones de OnPlus Portal desde un dispositivo móvil con un navegador web.
Compatibilidad con funciones y dispositivos de Cisco, en la página 223	Incluye los dispositivos Cisco compatibles con OnPlus Portal, junto con las funciones del portal disponibles para cada dispositivo, así como las limitaciones o restricciones aplicables.

3

Conceptos básicos de la interfaz de usuario de Cisco OnPlus Portal

Lea esta sección para ver sugerencias sobre la personalización de las páginas y funciones del portal.

- **Descripción general de la cuenta de partner y Panel del cliente**
- **Enlaces Cuenta, Soporte, Documentación y Cierre de sesión**
- **Uso de menús flotantes**
- **Personalización de las páginas de OnPlus Portal**
- **Zona horaria utilizada para la fecha y la hora del portal**
- **Avisos emergentes**
- **Cambio del fondo, tema y logotipo de OnPlus**

Descripción general de la cuenta de partner y Panel del cliente

OnPlus portal tiene dos áreas principales: Descripción general de la cuenta de partner y Panel del cliente.

Descripción general de la cuenta de partner

La Descripción general de la cuenta de partner incluye todos sus clientes. La página Descripción general se muestra de forma predeterminada la primera vez que inicia sesión en el portal.

Desde la página Descripción general puede agregar nuevos clientes o seleccionar un cliente para acceder a su red o perfil. Utilice los menús para acceder a las funciones de la cuenta de partner, como la entrega de notificaciones, la creación de informes, la administración de agentes autorizados y la carga de firmware. Consulte **Descripción general de la cuenta de partner de OnPlus, en la página 39**.

1	Muestre la página principal Descripción general, que incluye todos los clientes. Haga clic en un cliente de la lista para ver su red y administrar dispositivos. Consulte **Descripción general y funciones del panel, en la página 47**.
2	Cree, edite o elimine reglas y contactos de entrega para las notificaciones de eventos. Consulte **Supervisión y notificaciones, en la página 99**.
3	Cree, programe y visualice informes. Consulte **Informes, en la página 163**.
4	Administre cuentas de agentes autorizados. Consulte **Agregar y administrar agentes autorizados, en la página 151**.
5	Lea información de soporte de productos (consulte **Visualización de la información de soporte de productos Cisco, en la página 171**) y visualice una lista del firmware que ha cargado para dispositivos Cisco compatibles (consulte **Visualización de la información de la versión del firmware cargado, en la página 148**).
6	Un icono de flecha hacia abajo a la derecha de un elemento del menú de nivel superior indica que hay submenús disponibles.

Panel del cliente

Al seleccionar un cliente en la lista de la página Descripción general, se accede a la vista Panel de ese cliente. Desde el panel, puede consultar el estado del cliente y su topología de red, además de interactuar con los dispositivos de su red. Los menús adicionales del panel proporcionan acceso a funciones específicas del cliente, como integración de servicios, perfil del cliente e historial de eventos. Consulte **Visualización de las redes de los clientes, en la página 47**.

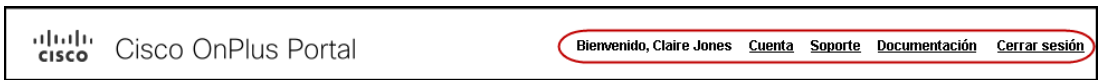
Si el cliente aún está pendiente de activación, accederá a la página de estado del cliente. Si se ha suspendido al cliente, el panel estará vacío.

Para volver a la página Descripción general de la cuenta de partner, haga clic en **Descripción general**.

1	Vuelva a la página principal Descripción general, que incluye todos los clientes.
2	Visualice y acceda al panel de ese cliente. El panel tiene dos vistas principales: ▪ **Topología de red**. Ofrece una vista jerarquía y gráfica de la red de un cliente. Consulte **Uso de la vista Topología de red, en la página 55**. ▪ **Lista de dispositivos**. Esta vista proporciona una lista tabular de los dispositivos de la red del cliente. Consulte **Uso de la vista Lista de dispositivos, en la página 68**. Puede acceder a los dispositivos del cliente y administrarlos desde cualquiera de estas dos vistas. Consulte **Trabajar con dispositivos del cliente, en la página 75**. Puede accederse a la mayoría de las funciones del panel desde cualquiera de estas dos vistas.
3	Muestra información del estado actual del cliente. Consulte **Visualización del estado de los clientes, en la página 72**.
4	Muestre el historial de eventos del dispositivo y el sistema para este cliente. Consulte **Visualización de eventos, en la página 121**.
5	Configure la integración de las aplicaciones de Cisco OnPlus con aplicaciones como ConnectWise y Autotask para este cliente. Consulte **Instalación y administración de las aplicaciones de OnPlus, en la página 72**.
6	Visualice o edite el perfil de la cuenta, la dirección y el período de mantenimiento para este cliente. Desde la página **Perfil**, puede suspender, anular la suspensión y eliminar el cliente. Consulte **Administración de clientes, en la página 41**.

Enlaces Cuenta, Soporte, Documentación y Cierre de sesión

Haga clic en los enlaces de la parte superior de cada página del portal para ver o editar la información de la cuenta de partner, acceder al área de la Comunidad de soporte para productos Small Business de Cisco OnPlus Portal, ver una versión en línea de esta guía y cerrar sesión en el portal.



NOTA Tras 24 minutos de inactividad, se cierra la sesión en el portal y vuelve a aparecer la página de inicio de sesión.

Uso de menús flotantes

Los menús flotantes, con los que se especifican muchos de los ajustes y acciones de OnPlus Portal, son accesibles moviendo el ratón sobre un enlace o icono en la interfaz de usuario.

1	Mueva el ratón sobre un enlace o icono para abrir un menú flotante. Los menús flotantes se cierran automáticamente cuando mueve el ratón fuera del área del menú.

2	Algunos menús flotantes tienen diferentes categorías de opciones. Estas categorías se incluyen en la parte superior del menú flotante. Haga clic en una categoría para ver sus opciones.
3	Los cambios que realice se aplicarán inmediatamente.

Personalización de las páginas de OnPlus Portal

Si puede personalizarse una página del portal, verá el enlace **Personalizar** en la esquina superior derecha de la página. Mueva el ratón sobre el enlace para abrir un menú flotante con opciones de personalización específicas para la página seleccionada en ese momento.

Estos ajustes personalizados se aplican en función del navegador a todos los clientes. Las selecciones se guardan para todas las sesiones del navegador web que esté utilizando. Si utiliza otro dispositivo para acceder al portal o cambia el navegador web, debe restablecer estas opciones.

Los ajustes específicos del cliente se encuentran en la barra de herramientas del panel (consulte **Uso de la barra de herramientas del panel, en la página 53**).

Zona horaria utilizada para la fecha y la hora del portal

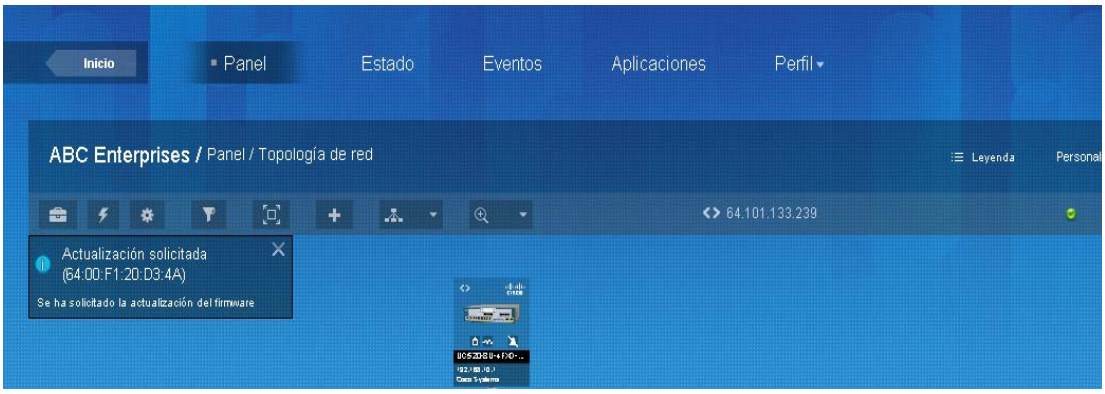
En OnPlus Portal, las fechas y las marcas de tiempo se basan en la zona horaria que se haya especificado en el perfil de la cuenta de partner. La zona horaria actual se muestra en los menús de Personalizar y en otras áreas del portal en las que sea aplicable.

Para cambiar la zona horaria, haga clic en el enlace **Cuenta**, en la parte superior de la página, y seleccione una nueva ubicación en los menús desplegables. Consulte **Actualización de la información de su cuenta de partner de OnPlus, en la página 46**.

Avisos emergentes

Los avisos emergentes aparecen en el área superior izquierda de la vista Topología de red o la vista Lista de dispositivos en el panel para informarle de que hay acciones necesarias y eventos que están ocurriendo en el sitio del cliente que está viendo. Se muestran en el área superior izquierda de la página Panel.

Los avisos emergentes se cierran automáticamente después de 10 segundos.



Para personalizar la configuración de los mensajes emergentes, haga clic en el enlace **Personalizar** del panel y seleccione **Ajustes generales**. Puede seleccionar una de estas opciones:

- Suprimir avisos de actualización de detecciones
- Suprimir avisos de que se necesitan credenciales
- Suprimir todos los avisos emergentes

Leyendas e información sobre herramientas

Haga clic en el icono **Leyenda**, en la parte inferior izquierda de la página Descripción general, para ver las descripciones de los iconos de estado y las acciones que se utilizan en la lista.

La información de leyenda también está disponible en Topología de red.

Para ver información sobre herramientas, pase el ratón sobre los iconos en la vista.

Cambio del fondo, tema y logotipo de OnPlus

Puede cambiar el fondo predeterminado y el tema de la interfaz de usuario del portal. Para ello, haga clic en el enlace **Cuenta** en la parte superior de cualquier página del portal para abrir el perfil de la cuenta de partner.

En la sección **Preferencias globales** del perfil, active o desactive la opción **Usar tema claro**.

- Cuando está activada la opción **Usar tema claro**, se utilizan colores de fondo más claros.
- Haga clic en el enlace **vista previa** a la derecha de la casilla de verificación para ver la apariencia del tema.

Haga clic en Guardar para aplicar los cambios.

En la sección **Preferencias globales**, puede agregar, cambiar o eliminar el **logotipo de la compañía** que aparece en los informes.

- **Explore** para buscar el logotipo que desee cargar y pulse **Guardar** cuando haya localizado el archivo.
- Seleccione **Eliminar** para eliminar la imagen del logotipo y pulse **Aceptar** cuando se muestre la ventana Confirmación.

4

Descripción general de la cuenta de partner de OnPlus

Este capítulo incluye información acerca del uso del área Descripción general de la cuenta de partner del portal para visualizar el estado de los clientes, administrar clientes y acceder a las funciones globales asociadas con su cuenta de partner.

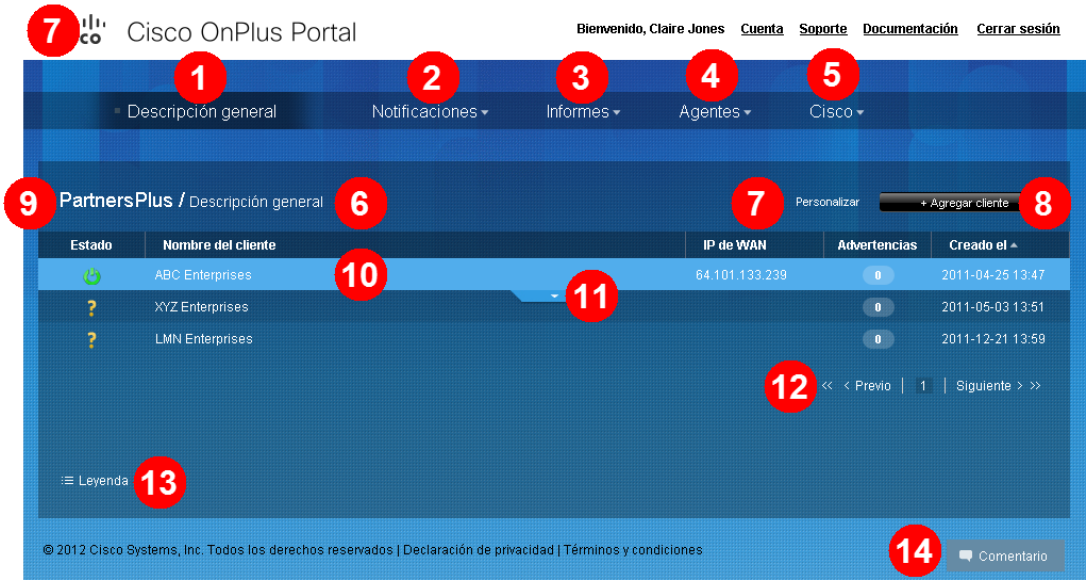
- **Página Descripción general y menús de funciones**
- **Administración de clientes**
- **Actualización de la información de su cuenta de partner de OnPlus**

Página Descripción general y menús de funciones

Al iniciar sesión por primera vez en su cuenta de OnPlus Portal, aparece la página Descripción general. Desde esta página puede:

- Ver una lista de todos sus clientes, que incluye información de estado, recuentos de alertas de 24 horas e información de ubicación para cada cliente.
- Agregar y administrar clientes.
- Hacer clic en cualquier cliente de la lista para abrir su panel. En el panel del cliente, puede ver su topología de red y supervisar o interactuar con dispositivos de forma remota a través del portal.
- Acceder a informes, entrega de notificaciones, administración de agentes autorizados, listas de firmware cargado e información de soporte de productos Cisco.

A continuación, se muestra una página de ejemplo que muestra las funciones disponibles y las áreas de interés de la página Descripción general.



1	Muestra la página principal Descripción general que incluye todos los clientes.
2	Cree, edite o elimine reglas y contactos de entrega para las notificaciones de eventos de OnPlus.
3	Cree, programe y visualice informes.
4	Invite, apruebe, visualice o elimine agentes autorizados. Este menú no se muestra para los agentes autorizados.
5	Vea información de software para dispositivos Cisco compatibles que haya cargado al portal. Vea información de garantía y servicio de soporte de productos para dispositivos Cisco.
6	Lista de clientes. Haga clic en un cliente de la lista para ver los dispositivos de su red e interactuar con ellos.
7	Mueva el ratón sobre el enlace **Personalizar** para agregar o eliminar información.
8	Cree nuevas cuentas de clientes.
9	Resumen de la información de cada cliente.
10	Haga clic en una entrada de la lista para acceder al panel del cliente seleccionado.
11	Haga clic aquí para abrir o cerrar un cuadro que muestra el logotipo, la dirección de correo electrónico y la ubicación (mapa de Google) del cliente seleccionado.

12	Utilice los controles para desplazarse por la lista.
13	Mueva el ratón sobre el icono Leyenda para ver información sobre los iconos de estado que se muestran en la página Descripción general.
14	Proporcione comentarios y solicite mejoras para Cisco OnPlus Portal.

Personalización de la página Descripción general

Puede personalizar la información que se muestra para sus clientes en la página Descripción general.

Para ello, mueva el ratón sobre el enlace **Personalizar** para abrir el menú flotante Personalizar descripción general y seleccione la información que se mostrará en la lista personalizada.

Los cambios se aplican tan pronto como mueve el ratón fuera del menú flotante.

Estos ajustes personalizados se aplican en función del navegador a todos los clientes. Las selecciones se guardan para todas las sesiones del navegador web que esté utilizando. Si utiliza otro dispositivo para acceder al portal o cambia el navegador web, debe restablecer estas opciones.

Puede seleccionar si desea o no mostrar la dirección IP de WAN, la fecha de creación, la fecha de la última actualización y el número de eventos con un nivel de gravedad de Advertencia o superior en las últimas 24 horas. También puede especificar el número de registros que se muestran por página para el sitio.

Administración de clientes

Consulte las siguientes secciones para ver instrucciones de administración de clientes:

- **Cómo agregar un cliente**
- **Eliminación de un cliente**
- **Suspensión y reanudación de una cuenta de cliente**
- **Visualización de la información de contacto y ubicación del cliente**
- **Edición del perfil o la dirección de un cliente**

Cómo agregar un cliente

Cada cliente que agregue representa un cliente único con un único OnPlus Network Agent.

Para agregar la cuenta de un cliente, siga estos pasos.

PASO 1 En la página Descripción general, haga clic en el botón + **Agregar cliente** en la parte superior derecha de la página, debajo de la barra de navegación.

PASO 2 Para cargar una imagen de logotipo opcional para el cliente, haga clic en **Examinar**.

SUGERENCIA La carga de un logotipo es opcional. Las imágenes deben tener formato JPEG, PNG o GIF. Las imágenes con un tamaño superior a 300 x 300 píxeles se cambiarán de tamaño. Puede agregar o sustituir la imagen en cualquier momento una vez creada la cuenta.

Si la carga se realiza correctamente, se mostrará una marca de verificación y el texto **Imagen válida**. La imagen cargada no se muestra aquí. Una vez creado el cliente, podrá ver el logotipo desde la lista de clientes. Consulte **Visualización de la información de contacto y ubicación del cliente, en la página 45**.

PASO 3 Escriba la información del cliente necesaria en la sección **Perfil** y haga clic en **Siguiente**. Puede agregar o editar el perfil del cliente más tarde.

PASO 4 En la sección **Contacto**, escriba la información de contacto necesaria para ese cliente o desactive la opción **Agregar un contacto** para continuar sin agregar la información de contacto.

Puede agregar o editar los contactos más tarde. Consulte **Cómo agregar y administrar contactos de entrega, en la página 104**.

PASO 5 En la ficha **Resumen**, repase la información que ha introducido y corrija los errores, que aparecerán resaltados.

Utilice los botones **Atrás** y **Siguiente** para desplazarse por las secciones.

PASO 6 Haga clic en **Guardar**.

La página Descripción general se actualiza para mostrar una entrada para el nuevo cliente. La columna **Estado** indica que el cliente está en estado de **Activación en espera**, puesto que OnPlus Network Agent aún no se ha instalado y activado en las instalaciones del cliente.

IMPORTANTE La página de estado del cliente muestra su **ID de activación** si el estado es Activación en espera. El **ID de activación** siempre se muestra en la página **Perfil** del cliente. Puede copiar y pegar este ID en un editor de texto o en otro programa para utilizarlo más adelante. Deberá utilizar este ID para activar el dispositivo OnPlus Network Agent del cliente con el portal.

Consulte **Instalación y activación de OnPlus Network Agent en las instalaciones del cliente, en la página 21**.

Eliminación de un cliente

Al eliminar un cliente, toda su información se elimina del portal y no puede recuperarse. Esta acción no se puede deshacer.

Puede restablecerse la configuración predeterminada del dispositivo OnPlus Network Agent del cliente eliminado y volver a activarlo con otro cliente (consulte **Transferencia de OnPlus Network Agent a otro cliente, en la página 184**).

Para eliminar un cliente en OnPlus portal, siga estos pasos.

PASO 1 Antes de eliminar un cliente, es recomendable realizar un restablecimiento de la configuración predeterminada en la unidad OnPlus Network Agent del cliente. De este modo, se eliminan de OnPlus Network Agent todos los datos del cliente, de manera que puede volver a activarse más adelante. Consulte **Restablecimiento de la configuración predeterminada en OnPlus Network Agent, en la página 179**.

NOTA Una vez eliminado un cliente del portal, no podrá acceder de forma remota al dispositivo OnPlus Network Agent del cliente.

PASO 2 En el portal, en la página Descripción general, haga clic en el cliente que desea eliminar.

PASO 3 En el menú Perfil de la parte superior de la página, seleccione **Perfil**.

PASO 4 Haga clic en el botón **Eliminar** en la parte inferior del perfil.

PASO 5 Haga clic en **Aceptar** para confirmar la eliminación.

Suspensión y reanudación de una cuenta de cliente

Cuando se suspende un cliente, también lo hacen todos los servicios del portal. Entre ellos se incluye la detección de dispositivos, la supervisión de dispositivos, las notificaciones a los contactos de destino de los clientes, las actualizaciones de firmware y las copias de seguridad y la restauración de la configuración.

La información del perfil de la cuenta del cliente suspendido se conserva en el portal, de modo que puede reactivarse el cliente posteriormente sin tener que volver a crear la cuenta.

Suspender un cliente

Para suspender un cliente en OnPlus portal, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, haga clic en el cliente que desea suspender.

PASO 2 En el menú Perfil de la parte superior de la página, seleccione **Perfil**.

PASO 3 Haga clic en el botón **Suspender** en la parte inferior del perfil.

La página **Estado** del cliente se actualiza para indicar que la cuenta se ha suspendido. La vista Topología de red y la vista Lista de dispositivos no muestran ningún dispositivo encontrado, puesto que la detección de dispositivos se deshabilita al suspender el cliente.

Reactivación de un cliente suspendido

Para reactivar un cliente suspendido en OnPlus portal, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, haga clic en la cuenta del cliente que desea reactivar.

PASO 2 En el menú Perfil de la parte superior de la página, seleccione **Perfil**.

PASO 3 Haga clic en el botón **Anular la suspensión** en la parte inferior del perfil.

La página **Estado** del cliente se actualiza para indicar que la cuenta se ha reactivado.

Visualización de la información de contacto y ubicación del cliente

Para abrir o cerrar un cuadro con información de contacto del cliente y un mapa de Google con su ubicación, seleccione el cliente y haga clic en el icono de flecha en la pestaña en la parte inferior de la entrada resaltada.

Edición del perfil o la dirección de un cliente

Puede editar el perfil de la cuenta del cliente o su dirección para:

- Cambiar el nombre de la empresa, la información del sector o la zona horaria
- Cambiar la contraseña del cliente
- Agregar o actualizar una imagen de logotipo
- Actualizar la información de la ubicación del cliente

Para editar el perfil del cliente, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, haga clic en el cliente que desee editar.

PASO 2 En el menú Perfil de la parte superior de la página, seleccione **Perfil**.

PASO 3 Edite la información según sea necesario y, a continuación, haga clic en **Guardar**.

Para editar la dirección del cliente, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, haga clic en el cliente que desee editar.

PASO 2 En el menú Perfil de la parte superior de la página, seleccione **Dirección**.

PASO 3 Edite la información según sea necesario y, a continuación, haga clic en **Guardar**.

Actualización de la información de su cuenta de partner de OnPlus

Para actualizar la información de su cuenta de partner de Cisco OnPlus, seleccione **Cuenta** en los enlaces de la esquina superior derecha de la página.

Actualice la información según sea necesario y haga clic en **Guardar**.

Puede actualizar la información de su cuenta en cualquier momento. La dirección de correo electrónico y los números de teléfono de contacto que se introducen aquí pueden utilizarse al crear reglas de notificación para los eventos que se están supervisando. Consulte **Uso de las reglas de entrega, en la página 107**.

La dirección de correo electrónico de su cuenta de partner también puede utilizarse al especificar los destinatarios de los informes programados. Consulte **Informes, en la página 163**.

Cuando está activada la opción **Usar tema claro**, se utilizan colores de fondo más claros. Haga clic en el enlace **vista previa** a la derecha de la casilla de verificación para ver la apariencia del tema.

Puede cambiar fácilmente el **logotipo de la compañía**; para ello, haga clic en **Explorar** para buscar el logotipo que cumpla con los requisitos de carga que aparecen al situar el cursor en el cuadro vacío que se encuentra junto a **Explorar**.

Al registrar su cuenta, se crea una regla de entrega predeterminada para las notificaciones. La regla de entrega predeterminada especifica que los mensajes de correo electrónico de notificación para todos los eventos con el nivel de gravedad Advertencia o superior se enviarán a la dirección de correo electrónico de trabajo de su cuenta de partner. Puede eliminar esta regla o suspender las notificaciones a esta dirección de correo electrónico si es necesario. Consulte **Eliminación de reglas de entrega, en la página 112** y **Cómo habilitar o deshabilitar las notificaciones a direcciones de correo electrónico o SMS, en la página 106**.

5

Visualización de las redes de los clientes

En este capítulo se explica cómo acceder al panel de cada cliente y utilizarlo para ver los detalles de sus redes a través de las páginas Topología de red y Lista de dispositivos. Consulte estos temas:

- **Descripción general y funciones del panel**
- **Detección de dispositivos**
- **Uso de la vista Topología de red**
- **Uso de la vista Lista de dispositivos**
- **Visualización del estado de los clientes**
- **Instalación y administración de las aplicaciones de OnPlus**

Descripción general y funciones del panel

El área Panel en Cisco OnPlus Portal es la interfaz principal de acceso a la red de cada cliente. Allí puede explorar la red del cliente e interactuar con ella mediante la vista jerárquica Topología de red o la vista tabular Lista de dispositivos.

Para acceder al panel de un cliente desde la página Descripción general, haga clic en un cliente de la lista. De forma predeterminada, se muestra la vista Topología de red de la red del cliente.

NOTA Si el sitio del cliente está pendiente de activación, al hacer clic en él aparece su página de estado. Si la cuenta del cliente se encuentra suspendida, el panel muestra un mensaje que indica que no se ha detectado ningún dispositivo.

El siguiente diagrama muestra las funciones y áreas de interés del panel del cliente.

1	Haga clic en **Inicio** para volver a la página principal de lista de clientes.
2	Cuando está resaltado, indica que está viendo la red del cliente seleccionado a través del panel.
3	Muestra el estado actual de este cliente.
4	Muestra el historial de eventos de este cliente.
5	Instale y administre aplicaciones OnPlus para este cliente. Consulte **Instalación y administración de las aplicaciones de OnPlus, en la página 72**
6	Vea o modifique la configuración del perfil del cliente. Desde el perfil del cliente, también puede eliminar o suspender al cliente.
7	Haga clic en el enlace Leyenda para ver información sobre qué representa cada uno de los iconos distintivos, los colores de alarma y los iconos de acciones.
8	Mueva el ratón sobre el enlace **Personalizar** para especificar la configuración que se aplicará al panel para todas las redes del cliente.

9	Exporte una captura de la red del cliente en uno de los siguientes formatos: ▪ Gráfico de red portátil (PNG) ▪ Gráfico vectorial escalable (SVG) ▪ Valores separados por comas (CSV)
10	Nombre del cliente seleccionado.
11	Mueva el ratón sobre los iconos de la barra de herramientas para acceder a herramientas, acciones y ajustes específicos de la vista Topología. **Uso de la barra de herramientas del panel, en la página 53**
12	Dirección IP pública del sitio de este cliente.
13	Mueva el ratón sobre la lista Tarea pendiente para ver las acciones disponibles y el número de dispositivos para los que está disponible cada acción. Consulte **Uso de la lista de tareas pendientes, en la página 54**.
14	Aquí aparecen los avisos de estado y eventos del portal. Consulte **Avisos emergentes, en la página 36**.
15	Área de la vista Red. En la captura anterior se muestra la vista Topología de red. Si se selecciona Lista de dispositivos, se muestra aquí una lista tabular de dispositivos. Consulte **Uso de la vista Topología de red, en la página 55** y **Uso de la vista Lista de dispositivos, en la página 68** para ver información detallada sobre el uso de estas vistas.

Para obtener más información acerca de conceptos y funciones disponibles en las dos vistas del panel, consulte estas secciones:

- **Detección de dispositivos, en la página 50**
- **Solución de problemas habituales de la detección de dispositivos, en la página 51**
- **Activación manual de la detección de dispositivos, en la página 52**
- **Uso de la barra de herramientas del panel**
- **Uso de la lista de tareas pendientes**
- **Filtro de dispositivos en el panel, en la página 54**

Detección de dispositivos

Las vistas del panel se generan automáticamente durante la detección de dispositivos. La detección de dispositivos comienza al activar el cliente y se ejecuta de forma periódica. En función del tamaño de la red, al activar el sitio por primera vez, la detección de la red puede tardar varios minutos.

OnPlus Network Agent utiliza una combinación de mecanismos estándar y propios para la detección de dispositivos, como Bonjour, CDP (Cisco Discovery Protocol, protocolo de detección de Cisco), ARP (Address Resolution Protocol, protocolo de resolución de direcciones), SNMP (Simple Network Management Protocol, protocolo simple de administración de red), tablas CAM (Content Addressable Memory, memoria de contenido direccionable) y UPnP (Universal Plug and Play, Plug and Play universal).

IMPORTANTE Los routers Cisco (en especial los routers IOS) normalmente tienen los protocolos de detección deshabilitados de forma predeterminada. Para obtener los mejores resultados, habilite los protocolos de detección, como CDP o Bonjour, en la interfaz LAN del router.

La detección también se inicia automáticamente cuando se agregan nuevos dispositivos al sitio del cliente. Puede iniciar la detección de forma manual (consulte **Activación manual de la detección de dispositivos, en la página 52**).

NOTA Es posible que tenga que proporcionar credenciales de acceso a dispositivos para habilitar la detección de dispositivos adicionales (por ejemplo, switches gestionados, dispositivos de red Cisco, puntos de acceso inalámbricos y routers). Consulte **Credenciales, en la página 80**.

Solución de problemas habituales de la detección de dispositivos

Problema	Posible causa	Solución
Hay dispositivos en la red pero no se muestran en la vista Topología.	No se han introducido las credenciales de acceso a dispositivos para dispositivos ascendentes, como routers, switches o puntos de acceso.	Desde la vista Topología del cliente, localice el router ascendente, abra la ventana Dispositivo, haga clic en la ficha Credenciales e introduzca las credenciales de inicio de sesión o una contraseña habilitada. Consulte **Credenciales, en la página 80**.
	Los dispositivos se encuentran en otra VLAN o subred distinta a la de OnPlus Network Agent.	Si el router ascendente es un router Cisco compatible con OnPlus Portal y tiene visibilidad en varias VLANS, se puede obtener información de detección adicional en el router ascendente si se proporcionan credenciales de acceso al dispositivo. Desde la vista Topología del cliente, localice el router ascendente, abra la ventana Dispositivo, haga clic en la ficha Credenciales e introduzca las credenciales de inicio de sesión o una contraseña habilitada. Consulte **Credenciales, en la página 80**. Los dispositivos que no son Cisco y los dispositivos Cisco no compatibles con el portal, pueden agregarse de forma manual a la topología (consulte **Cómo agregar manualmente dispositivos secundarios, en la página 64**) o reorganizar su relación jerárquica manualmente (consulte **Edición manual de conexiones de dispositivos (reorganización de la relación jerárquica de los dispositivos), en la página 66**).
El dispositivo es compatible con el portal pero no se muestra o está etiquetado como “Dispositivo desconocido”.	El dispositivo no anuncia ninguno de los protocolos de detección compatibles o estos se han deshabilitado en el dispositivo por razones de seguridad (o de forma predeterminada).	Habilite Bonjour o CDP en el dispositivo. Para algunos dispositivos, es posible que tenga que proporcionar un controlador para habilitar la detección. Desde la vista Topología del cliente, localice el dispositivo afectado, abra la ventana Información de dispositivo, haga clic en la ficha Credenciales, seleccione Controlador y seleccione el dispositivo adecuado. Consulte **Controlador de dispositivo, en la página 84**.

Problema	Posible causa	Solución
Los dispositivos que no sean Cisco o los dispositivos Cisco no compatibles se muestran como “Dispositivo desconocido”. Consulte **Compatibilidad con funciones y dispositivos de Cisco, en la página 223** para ver una lista de dispositivos Cisco compatibles con el portal.	No se ha obtenido suficiente información durante la detección (el dispositivo no anuncia ninguno de los protocolos de detección compatibles o estos se han deshabilitado por razones de seguridad o de forma predeterminada).	Desde la vista Topología del cliente, localice el dispositivo, abra la ventana Dispositivo, haga clic en la ficha Ajustes y edite el nombre, la categoría y la descripción de los dispositivos para identificarlos. Consulte **Ajustes, en la página 78**.

Activación manual de la detección de dispositivos

Puede activar manualmente la detección de dispositivos desde la vista Topología de red o la vista Lista de dispositivos.

- En la vista Topología de red, mueva el ratón sobre el icono de OnPlus Network Agent y seleccione **Información de dispositivo**. Haga clic en la ficha Ajustes, seleccione **Activar detección** en el menú desplegable Acciones y, a continuación, haga clic en **Confirmar**.
- En la vista Lista de dispositivos, haga clic con el botón derecho en el icono de OnPlus Network Agent y seleccione **Ver información del dispositivo**. Haga clic en la ficha Ajustes, seleccione **Activar detección** en el menú desplegable Acciones y, a continuación, haga clic en **Confirmar**.

Uso de la barra de herramientas del panel

La barra de herramientas del panel incluye las siguientes opciones. La barra de herramientas del panel está disponible tanto en la vista Topología de red como en la vista Lista de dispositivos. Para obtener más detalles sobre cómo se utilizan las opciones de la barra de herramientas del panel en la vista Topología de red, consulte **Personalización de la configuración del panel, en la página 58**.

Número	Icono	Descripción
1		**Herramientas**. Mueva el ratón sobre este icono para acceder a las herramientas de Hacer ping en host y Búsqueda de servidor de nombres para comprobar la conectividad de la red y DNS. La opción **Soporte de Cisco** proporciona acceso a las herramientas de soporte de los agentes del Centro de soporte para productos Cisco Small Business.
2		**Restablecimiento de la topología y acciones del sitio**. Mueva el ratón sobre este icono de la barra de herramientas para acceder a las opciones que permiten restablecer la topología y volver a detectar la red. También puede forzar el cierre de una conexión de túnel abierta a un dispositivo remoto, activar manualmente la detección de dispositivos, volver a habilitar las alarmas del dispositivo o desactivar por completo el sitio del cliente.
3		**Ajustes**. Mueva el ratón sobre este icono de la barra de herramientas para acceder a las opciones de ajuste del diseño de la topología y ajustes de pantalla. Puede cambiar el modo de diseño de la topología (automático o manual), establecer la opacidad de la línea de conexión, establecer las opciones de ajuste a la cuadrícula y agregar categorías de dispositivo personalizadas.
4		**Criterios de filtrado**. Especifique los criterios para filtrar los dispositivos que se muestran en la vista Panel. Consulte **Filtro de dispositivos en el panel, en la página 54**.

Número	Icono	Descripción
5		**Modo de pantalla completa**. Solo para Topología de red. Haga clic aquí para acceder al modo de pantalla completa. Presione **ESC** para salir del modo de pantalla completa. En este modo la entrada de texto está deshabilitada.
6		**Agregar nuevo dispositivo**. Agregue manualmente un dispositivo a Topología de red. Consulte **Cómo agregar manualmente dispositivos secundarios, en la página 64**.
7		**Alternar entre las vistas Topología de red y Lista de dispositivos**. Mueva el ratón sobre este icono para seleccionar si desea mostrar la vista Topología de red o la vista tabular Lista de dispositivos. De forma abreviada, puede simplemente hacer clic en el icono para cambiar de vista.
8		**Zoom.** Solo para la vista Topología de red. Seleccione un porcentaje de zoom para la vista Topología o seleccione **Ajustar con zoom**.

Uso de la lista de tareas pendientes

La lista Tarea pendiente de la vista Panel le permite localizar rápidamente dispositivos con condiciones que requieran que se realice una acción, como dispositivos ausentes, dispositivos que necesitan credenciales de acceso y dispositivos con actualizaciones de firmware disponibles.

Haga clic en un elemento de la lista Tarea pendiente para filtrar la vista, de modo que solo se muestren los dispositivos que tengan esa condición.

Cuando haya terminado de realizar las acciones o de ver los detalles del dispositivo, haga clic en **Mostrar todos los dispositivos**.

Filtro de dispositivos en el panel

Para acceder a las opciones de filtro de las vistas Topología de red y Lista de dispositivos, mueva el ratón sobre el icono Filtro , que se encuentra en la barra de herramientas del panel.

Especifique los criterios de filtrado, según se describe en la siguiente tabla, y haga clic en **Aplicar búsqueda** para localizar los dispositivos que cumplan esos criterios.

Haga clic en el enlace **Borrar todos los criterios de búsqueda** para borrar las opciones de búsqueda seleccionadas, cerrar la ventana Buscar y volver a la vista Panel.

Opción de búsqueda	Descripción
Coincidente	**Todos.** Solo se muestran en los resultados los dispositivos que cumplan todos los criterios de búsqueda. **Cualquiera**. En los resultados se muestran los dispositivos que cumplan al menos uno de los criterios de búsqueda.
Criterio de búsqueda	Especifique uno o más de los siguientes criterios: ▪ Texto incluido el nombre y la descripción de los dispositivos. La búsqueda no distingue entre mayúsculas y minúsculas. ▪ Clase de dispositivo. ▪ Categoría del dispositivo. ▪ Icono. Los iconos fotográficos no se incluyen en la búsqueda. Solo se incluyen los iconos de dispositivos que estén actualmente en el inventario del cliente. ▪ Direcciones IP o direcciones MAC que contengan los caracteres especificados. ▪ Número de serie, si se ha obtenido durante la detección. ▪ Dispositivos con números de serie que contengan los caracteres especificados. ▪ Dispositivos con uno o más monitores configurados. ▪ Dispositivos sin monitores configurados.

Uso de la vista Topología de red

Para mostrar la vista Topología de red desde la página principal Descripción general, haga clic en un cliente de la lista. De forma predeterminada, se muestra la vista Topología de red, pero puede cambiar la vista predeterminada del panel (pase el ratón sobre el enlace **Personalizar** y seleccione **Ajustes generales** > **Vista predeterminada**).

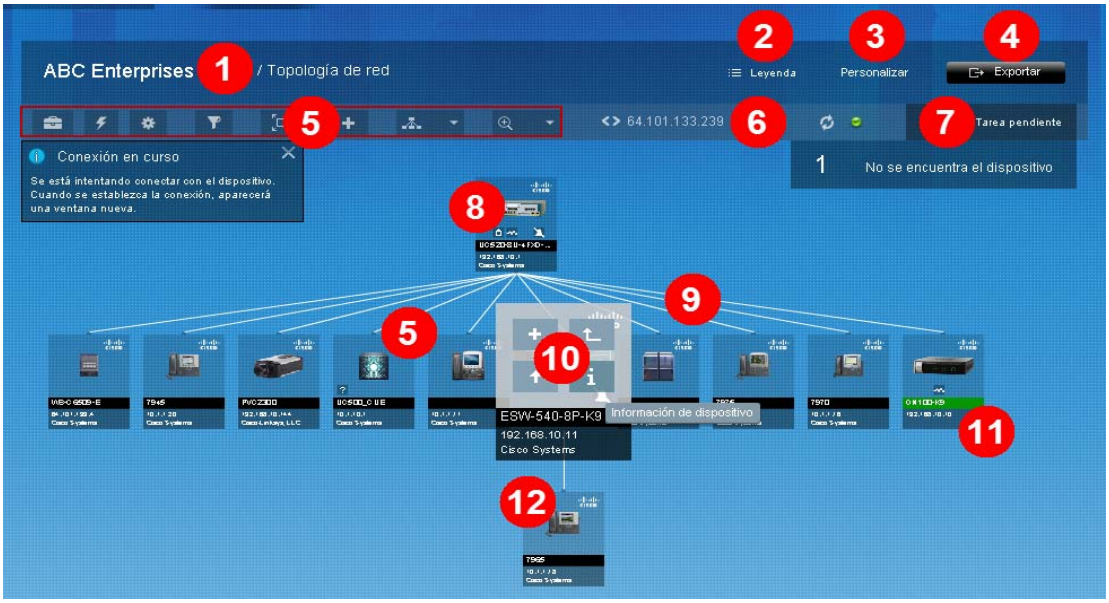
Para obtener más información, consulte estas secciones:

- **Funciones de Topología de red, en la página 56**
- **Personalización de la configuración del panel, en la página 58**
- **Uso de las opciones de la barra de herramientas del panel, en la página 61**

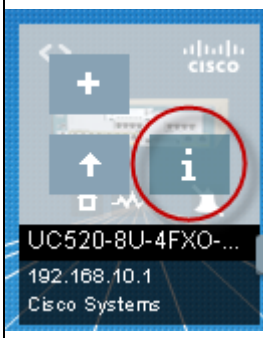
- Expansión o contracción de subárboles, en la página 63
- Establecimiento de un dispositivo como dispositivo raíz de la red, en la página 63
- Cómo agregar manualmente dispositivos secundarios, en la página 64
- Edición manual de conexiones de dispositivos (reorganización de la relación jerárquica de los dispositivos), en la página 66
- Reorganización de dispositivos del mismo nivel en la vista Topología, en la página 67

Funciones de Topología de red

A continuación se muestra un ejemplo de la vista Topología de una red simple. Los números del ejemplo muestran las áreas de interés de la vista Topología.



Número	Descripción
1	Nombre del cliente seleccionado.
2	Haga clic en el enlace Leyenda para ver información sobre qué representan los iconos de acciones, distintivos y colores de alarma.

Número	Descripción
3	Mueva el ratón sobre el enlace **Personalizar** para especificar la configuración del panel que se aplicará a la vista Topología de red para todos los sitios del cliente. Consulte **Personalización de la configuración del panel**.
4	Haga clic para exportar una captura de la vista Topología de red con formato de gráfico .png, archivo de gráfico vectorial escalable (SVG) o archivo de valores separados por comas (.csv) que pueda importar a otras aplicaciones.
5	Barra de herramientas del panel. Consulte **Uso de la barra de herramientas del panel, en la página 53**.
6	Dirección IP de WAN. Dirección IP pública de la red del cliente, si puede determinarse durante la detección del dispositivo.
7	Lista Tarea pendiente del panel. Consulte **Uso de la lista de tareas pendientes, en la página 54**.
8	Dispositivo raíz de la red, indicado por el distintivo . Consulte **Establecimiento de un dispositivo como dispositivo raíz de la red, en la página 63**.
9	Líneas de conexión del dispositivo. Consulte **Edición manual de conexiones de dispositivos (reorganización de la relación jerárquica de los dispositivos), en la página 66**.
10	Para cualquier icono de dispositivo, pase el ratón sobre el icono para acceder a las opciones que permiten agregar dispositivos secundarios, convertir el dispositivo en dispositivo raíz de la red, expandir o contraer subárboles o abrir la ventana Información de dispositivo.  También puede hacer clic con el botón derecho del ratón sobre el icono y seleccionar **Ver información del dispositivo**.
11	OnPlus Network Agent. El resaltado indica que hay una actualización de firmware disponible. El distintivo indica que se han configurado monitores para el dispositivo.
12	Subárbol con dispositivos secundarios. Consulte **Expansión o contracción de subárboles, en la página 63** y **Cómo agregar manualmente dispositivos secundarios, en la página 64**.

Puede ajustar la vista Topología para agregar o modificar dispositivos y cambiar el diseño de la vista:

- Si no se encuentran dispositivos durante la detección, aún puede agregarlos manualmente y editar la configuración para especificar la categoría y la descripción del dispositivo que se mostrarán en la vista Topología. Consulte **Cómo agregar manualmente dispositivos secundarios, en la página 64**.
- Si ha agregado dispositivos manualmente y necesita ajustar las líneas de conexión para mostrar las relaciones correctas, utilice la función **Vincular/Desvincular**. Consulte **Edición manual de conexiones de dispositivos (reorganización de la relación jerárquica de los dispositivos), en la página 66**.
- Si el proceso de detección no identifica correctamente el dispositivo raíz en Topología (generalmente, el router de gateway para Internet), seleccione **Establecer como dispositivo raíz** en el menú Acciones de la ficha Ajustes, en la ventana emergente Detalles de dispositivo. Consulte **Establecimiento de un dispositivo como dispositivo raíz de la red, en la página 63**.
- Consulte **Solución de problemas habituales de la detección de dispositivos, en la página 51** para ver información acerca de cómo tratar los dispositivos desconocidos ( ) y los dispositivos no detectados.

Personalización de la configuración del panel

Para personalizar los ajustes del navegador aplicables al panel del cliente, mueva el ratón sobre el enlace **Personalizar**.

Haga clic en una categoría (por ejemplo, Ajustes de topología) en la parte superior del menú flotante para acceder a su configuración. Esto se explica con detalle en la siguiente tabla.

Sus selecciones se guardan para el dispositivo que está utilizando para acceder al portal. Si utiliza un dispositivo diferente para acceder al portal, se utilizará la configuración predeterminada y tendrá que rehacer la configuración personalizada. Haga clic en **Restablecer valores predeterminados** para acceder a las opciones de restablecimiento de todos los ajustes del panel o a los ajustes de una categoría específica.

Categoría/ Configuración	Descripción
Ajustes generales. Estos ajustes se aplican tanto a la vista Topología de red como a la vista Lista de dispositivos.	
Vista predeterminada	**Selección auto** determinará la vista en función del número de dispositivos detectados en la red. (Si se detectan entre 1 y 99 dispositivos, se mostrará la vista Topología; si se detectan 100 o más, se mostrará la vista Lista de dispositivos.) **Topología** mostrará todos los dispositivos en la vista Topología independientemente de la cantidad. **Lista de dispositivos** mostrará todos los dispositivos en la vista Lista de dispositivos independientemente de la cantidad.
Suprimir avisos de actualización de detecciones	Cuando esta opción está habilitada, los avisos de actualización de detección no se muestran en el panel.
Suprimir avisos de que se necesitan credenciales	Cuando esta opción está habilitada, los avisos de credenciales del dispositivo necesarias no se muestran en el panel.
Suprimir todos los avisos	Cuando esta opción está habilitada, los avisos emergentes no se muestran en el panel.
Ajustes de topología. Estos ajustes son específicos de la vista Topología de red del panel.	
Aplicar zoom para adaptar al iniciar	Cuando esta opción está habilitada, el porcentaje de zoom de Topología de red se ajusta para adaptarse a la ventana del navegador al iniciar sesión en el portal.
Habilitar animación	Habilite o deshabilite las animaciones en la vista Topología de red.
Mostrar dirección IP	Habilite o deshabilite la muestra de direcciones IP en la vista Topología de red.
Mostrar dirección MAC	Habilite o deshabilite la muestra de direcciones MAC en la vista Topología de red.
Mostrar proveedor NIC	Habilite o deshabilite la muestra del nombre del proveedor de la tarjeta de interfaz de red (NIC) en la vista Topología.

Categoría/ Configuración	Descripción
Invertir uso de botón ALT al arrastrar en el fondo	De forma predeterminada, al hacer clic y arrastrar con ALT + botón IZQUIERDO del ratón sobre el fondo de la vista Topología, se produce un desplazamiento lateral de la vista, mientras que al hacer clic y arrastrar con el botón IZQUIERDO del ratón se seleccionan varios dispositivos. Cuando esta opción está activada, las funciones del botón del ratón se invierten.
Espaciado vertical	Ajuste el espaciado vertical entre dispositivos principales y secundarios en la topología. Esta opción se puede utilizar para mejorar la legibilidad de la vista Topología para redes de gran tamaño.
Ampliar dispositivo al pasar el ratón por él, a niveles de zoom más bajos	Cuando se habilita esta opción, aparece una versión del icono de mayor tamaño al mover el ratón sobre él. De este modo, resulta más fácil ver los iconos y el texto que se muestra en los iconos del dispositivo.
Velocidad del aspecto del menú activable	Especifique el tiempo que tardan en aparecer los botones emergentes del dispositivo al pasar el ratón sobre un icono en la vista Topología. Puede variar entre 50 ms (mínimo) y 1000 ms (máximo).
Ajustes de lista de dispositivos Los ajustes de visibilidad de las columnas son específicos de la vista Lista de dispositivos.	
Visibilidad de columnas	Active o desactive las columnas para mostrarlas u ocultarlas en la vista Lista de dispositivos.
Restablecer valores predeterminados Restaure los ajustes predeterminados por categoría de personalización del panel o todos los ajustes.	
Restablecer ajustes generales	Restablezca todos los Ajustes generales personalizados a los valores predeterminados.
Restablecer ajustes de topología	Restablezca todos los ajustes de la vista Topología personalizados a los valores predeterminados.
Restablecer ajustes de lista de dispositivos	Restablezca todos los ajustes personalizados de la vista Lista de dispositivos a los valores predeterminados.

Categoría/ Configuración	Descripción
Restablecer todo	Restablezca todos los ajustes personalizados del panel a los valores predeterminados.

Uso de las opciones de la barra de herramientas del panel

Para acceder a los ajustes y acciones adicionales que se aplican a la vista Topología de red para clientes determinados, utilice las opciones de la barra de herramientas del panel.

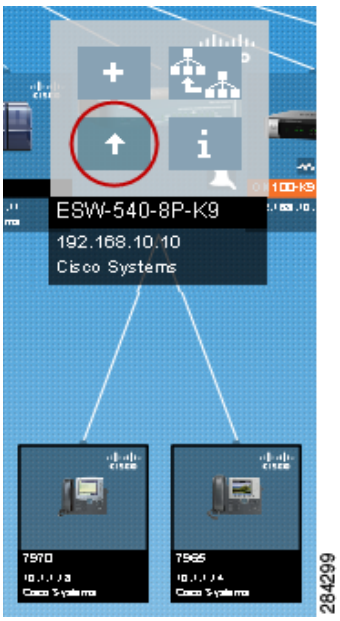
Icono	Categoría	Ajustes y acciones
	Herra-mientas	**Hacer ping en host**. Introduzca una dirección IP o nombre de host, especifique el tamaño del paquete y el número de paquetes, y haga clic en **Ejecutar** para probar la conectividad de la red.
		Búsqueda de servidor de nombres. Introduzca una dirección IP o nombre de host y haga clic en **Ejecutar** para probar la búsqueda de servidor/resolución de nombre de host de DNS.
		Soporte de Cisco. Acceso a las herramientas de solución de problemas del Centro de soporte para productos Cisco Small Business.
	Acciones del sitio	**Restablecimiento de datos** **Restablecer topología**. Restablezca la topología al estado actualmente detectado. Se eliminan todas las modificaciones realizadas en las conexiones del dispositivo para reorganizar la relación jerárquica de los dispositivos. **Volver a descubrir red**. Elimine los ajustes personalizados del dispositivo, los dispositivos agregados manualmente y los monitores de dispositivos y, a continuación, ejecute la detección de dispositivos. Se eliminan todas las modificaciones realizadas en las conexiones del dispositivo para reorganizar la relación jerárquica de los dispositivos.
		Acciones diversas **Activar detección**. Active manualmente la actualización de la detección de dispositivos. **Forzar desconexión**. Cierre la conexión de túnel abierta a un dispositivo remoto, si existe. **Volver a habilitar alarmas**. Vuelva a habilitar las alarmas de todos los dispositivos.
		Desactivar sitio. Elimine este sitio y todos los datos del cliente de OnPlus Network Agent. El dispositivo OnPlus Network Agent no se puede volver a activar de forma remota.

Icono	Categoría	Ajustes y acciones
	Diseño	**Ajustes de topología** **Modo de diseño de árbol**. Seleccione **Automático** para utilizar el diseño de árbol jerárquico automático. La opción Ajustar a cuadrícula no se aplica al modo de diseño Automático. Seleccione **Libre** si desea recolocar los dispositivos en la vista y que se guarden los cambios realizados en el diseño entre sesiones. En el modo de diseño Libre: ▪ No se trazan líneas de conexión. ▪ No hay opciones para editar de forma manual las conexiones para reorganizar la relación jerárquica de los dispositivos, contraer subárboles o convertir el dispositivo en dispositivo raíz. Aún puede agregar dispositivos secundarios a cualquier dispositivo. En cualquier modo, puede: ▪ Arrastrar el ratón sobre varios dispositivos y hacer clic con el botón izquierdo para seleccionarlos y recolocarlos como un grupo. ▪ Utilizar MAYÚS + clic para agregar o eliminar dispositivos de la selección. ▪ Los dispositivos seleccionados aparecen resaltados. Al cambiar del modo Libre al modo Automático, se eliminan todos los cambios realizados en el diseño del modo Libre. **Ajustar a cuadrícula** (solo en el modo de diseño Libre). Habilite o deshabilite Ajustar a cuadrícula en la vista Topología. **Ajustar tamaño de cuadrícula** (solo en el modo de diseño Libre). Seleccione Pequeña, Media o Grande. **Opacidad de conexión**. Establezca la opacidad para las líneas de conexión entre dispositivos principales y secundarios en la vista Topología.
	Categorías de dispositivo	Para agregar una categoría de dispositivo personalizada, haga clic en el icono (+), introduzca un nombre para la categoría y haga clic en **Agregar**. Una vez agregada la categoría, aparecerá en la lista de categorías disponibles al agregar un dispositivo manualmente.
	Criterios de filtrado	Especifique los criterios para filtrar los dispositivos que se muestran en la vista Panel. Consulte **Filtro de dispositivos en el panel, en la página 54**.
	Modo de pantalla completa	Haga clic en este icono para acceder al modo de pantalla completa. Presione ESC para salir del modo de pantalla completa. En este modo la entrada de texto está deshabilitada.

Icono	Categoría	Ajustes y acciones
	Alternar vistas	Haga clic en este icono para utilizar el menú desplegable para alternar entre las vistas Topología de red y Lista de dispositivos.
	Zoom	Seleccione un porcentaje de zoom o seleccione Ajustar con zoom.

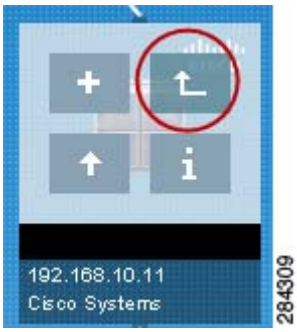
Expansión o contracción de subárboles

Para expandir o contraer subárboles con dispositivos secundarios en la jerarquía de Topología de red, mueva el ratón sobre el icono del dispositivo principal y haga clic en el icono de flecha hacia arriba o hacia abajo para expandir o contraer el subárbol que contiene sus dispositivos secundarios.



Establecimiento de un dispositivo como dispositivo raíz de la red

El dispositivo raíz se utiliza como dispositivo principal de otros dispositivos para los que no puede determinarse una topología precisa. Si el dispositivo raíz de su red no está establecido en el dispositivo al que se conectan con más frecuencia los nuevos dispositivos, localice el dispositivo raíz preferido en Topología de red, haga clic para seleccionar el dispositivo y haga clic en el icono **Establecer como dispositivo raíz**.



Cómo agregar manualmente dispositivos secundarios

Los dispositivos que no se encuentran durante el proceso de detección de OnPlus Portal pueden agregarse al sitio de forma manual desde la vista Topología de red. Normalmente, se trata de dispositivos que no difunden su identidad e información mediante los protocolos de detección utilizados por el portal.

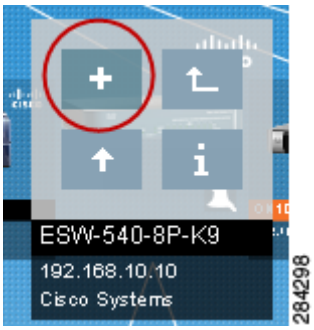
NOTA Si los dispositivos que se encuentran tras un router, switch o punto de acceso no se muestran según lo esperado en las vistas Topología de red y Lista de dispositivos, asegúrese de que ha introducido las credenciales de acceso al dispositivo principal antes de introducirlas manualmente.

Para agregar un dispositivo de forma manual al sitio del cliente, siga estos pasos.

PASO 1 Abra la vista Panel del sitio del cliente y muestre la vista Topología de red.

PASO 2 Desde la vista Topología de red, localice el dispositivo principal del dispositivo que desee agregar.

PASO 3 Mueva el ratón sobre el dispositivo principal y haga clic en el icono del signo (+) para agregar el dispositivo secundario. También puede hacer clic en el icono del signo (+) en la barra de herramientas del panel.



PASO 4 En el diálogo Agregar nuevo dispositivo, seleccione una Categoría y un Tipo de dispositivo para asociar un icono con el dispositivo. Complete el resto de los ajustes del dispositivo. El dispositivo principal es aquel al que se conecta directamente el dispositivo.

PASO 5 Haga clic en **Aceptar**. El nuevo dispositivo aparece en Topología de red, bajo el dispositivo principal.

Eliminación de dispositivos ausentes o dispositivos agregados manualmente

Solo es posible eliminar los dispositivos agregados manualmente que no se hayan detectado mediante el proceso de detección del portal o los dispositivos identificados como ausentes en la red. Las siguientes notas se aplican a la eliminación de dispositivos:

- Una vez detectado un dispositivo, ya no aparece marcado como agregado manualmente y no puede eliminarse de la Topología a menos que esté marcado como “Falta” (no presente en la red).
- Si el dispositivo eliminado vuelve a detectarse posteriormente, se vuelve a agregar al sitio del cliente y aparece en las vistas Topología de red y Lista de dispositivos.
- No puede eliminarse el dispositivo raíz de la red.

Para eliminar un dispositivo, siga estos pasos.

PASO 1 En la vista Topología de red, haga clic en el icono Información de dispositivo de un dispositivo agregado manualmente o un dispositivo identificado como ausente para abrir la ventana Dispositivo.

También puede hacer clic con el botón derecho del ratón sobre el icono y seleccionar **Ver información del dispositivo**.

Un distintivo de signo más identifica los dispositivos agregados manualmente en Topología de red.

Los dispositivos ausentes tienen un distintivo de interrogación .

En la vista Lista de dispositivos, seleccione el dispositivo que se eliminará de la lista y, a continuación, haga clic en el icono que aparece en la barra de herramientas del panel.

PASO 2 En la ventana Dispositivo, haga clic en la ficha **Ajustes**.

PASO 3 En el menú Acciones, seleccione **Eliminar dispositivo**.

PASO 4 Haga clic en **Confirmar**.

Edición manual de conexiones de dispositivos (reorganización de la relación jerárquica de los dispositivos)

Puede editar manualmente las conexiones entre los dispositivos de la vista Topología de red.

Estas son algunas sugerencias para la edición manual de conexiones de dispositivos:

- Tras reorganizar manualmente la relación jerárquica de los dispositivos en la vista Topología de red, las actualizaciones de detección de dispositivos automáticas no se aplican a los dispositivos reorganizados manualmente.
- Para eliminar los enlaces de los dispositivos editados manualmente y volver a habilitar las actualizaciones de detección de dispositivos automáticas, haga clic en el botón **Opciones** de la barra de herramientas del panel y seleccione **Restablecer topología**.
- No puede desconectar completamente un dispositivo detectado de la topología. Los dispositivos agregados manualmente pero que no han sido detectados pueden eliminarse de la topología, si fuera necesario.

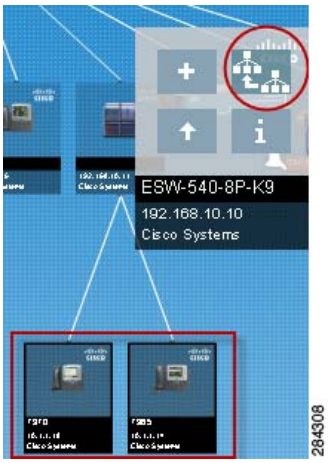
- No puede editar conexiones de dispositivos para reorganizar la relación jerárquica de los dispositivos cuando se está filtrando la vista Topología.

Para editar manualmente conexiones de dispositivos reorganizando su relación jerárquica, siga estos pasos.

PASO 1 En la vista Topología de red, localice y seleccione el dispositivo o dispositivos que quiere volver a vincular. Puede arrastrar el ratón en la vista, utilizar CTRL + botón izquierdo del ratón o MAYÚS + botón izquierdo del ratón para seleccionar varios dispositivos.

Los dispositivos seleccionados aparecen resaltados.

PASO 2 Con los dispositivos resaltados, mueva el ratón sobre el icono en la vista Topología del nuevo dispositivo principal y haga clic en el icono (**Establecer como dispositivo principal de los seleccionados**).



Reorganización de dispositivos del mismo nivel en la vista Topología

En el modo de diseño Automático, puede reorganizar los dispositivos que son secundarios del mismo dispositivo principal en la vista Topología. Es posible que quiera hacerlo para organizar la vista de modo que los dispositivos del mismo tipo estén agrupados.

Para reorganizar los dispositivos que son secundarios del mismo dispositivo principal, seleccione los iconos del dispositivo o dispositivos que desee mover y arrástrelos con el ratón a la derecha o a la izquierda para reorganizarlos.

NOTA Si los dispositivos de la vista Topología están actualmente filtrados, tendrá que deshabilitar el filtro y mostrar todos los dispositivos en la vista antes de reorganizarlos.

Uso de la vista Lista de dispositivos

Para acceder a la vista Lista de dispositivos, haga clic en el icono y seleccione Lista de dispositivos (o simplemente haga clic en el icono para alternar entre las vistas Lista de dispositivos y Topología de red).

En la vista Lista de dispositivos, puede realizar muchas de las tareas que se realizan en la vista Topología de red. Al igual que ocurre en la vista Topología de red, la vista Lista de dispositivos se actualiza automáticamente cuando se detectan nuevos dispositivos.

Para establecer Lista de dispositivos como la vista predeterminada del panel, haga clic en el enlace **Personalizar**, seleccione **Ajustes generales** y seleccione **Lista de dispositivos** como **Vista predeterminada**.

Estas columnas siempre se muestran en la vista Lista de dispositivos:

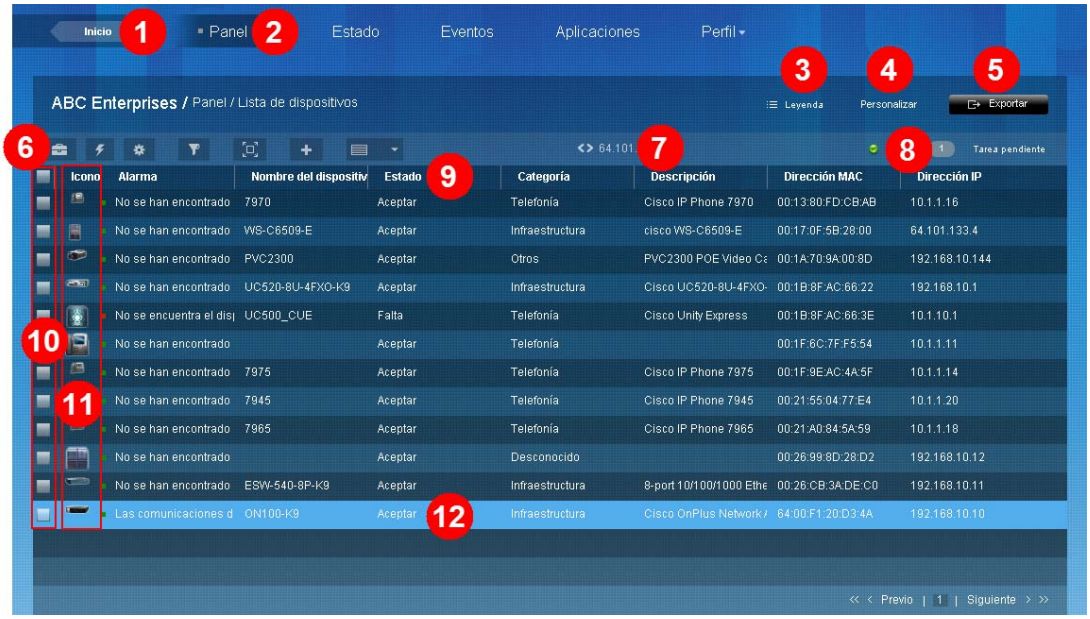
- Casilla de verificación de selección de dispositivo.
- Icono del dispositivo.
- **Alarma**. Esta columna indica las condiciones más recientes que se han encontrado, como credenciales del dispositivo necesarias o actualizaciones de firmware disponibles.
- **Nombre del dispositivo**. Es el nombre del dispositivo que se ha obtenido durante la detección o se ha introducido manualmente.

La vista Lista de dispositivos se trata con más detalle en las siguientes secciones:

- **Funciones de Lista de dispositivos, en la página 69**
- **Uso de la vista Lista de dispositivos, en la página 68**
- **Personalización de la vista Lista de dispositivos, en la página 70**
- **Filtro de dispositivos en el panel, en la página 54**

Funciones de Lista de dispositivos

A continuación, se muestra un ejemplo de la vista Lista de dispositivos que incluye las funciones disponibles y las áreas de interés de la vista.



Los números del ejemplo anterior resaltan las áreas de interés de la vista. Estos se incluyen y describen en la siguiente tabla.

Número	Descripción
1	Haga clic en **Inicio** para volver a la página Descripción general y a la lista principal de clientes.
2	Indica que el panel del cliente está actualmente seleccionado.
3	Mueva el ratón sobre el enlace **Leyenda** para ver el significado de los iconos y los colores de alarma.
4	Mueva el ratón sobre el enlace **Personalizar** para agregar o eliminar columnas en Lista de dispositivos. Consulte **Personalización de la vista Lista de dispositivos, en la página 70**.
5	Exporte Lista de dispositivos a un archivo en formato .csv.
6	Barra de herramientas del panel, que incluye opciones para usar las herramientas, especificar los ajustes de la vista y filtrar dispositivos. Consulte **Uso de la barra de herramientas del panel, en la página 53**.

Número	Descripción
7	Dirección IP de WAN (dirección IP pública del sitio del cliente en cuestión).
8	Lista Tarea pendiente del panel. Consulte **Uso de la lista de tareas pendientes, en la página 54**.
9	Haga clic en los encabezados de las columnas de la vista Panel para organizar las filas en orden ascendente o descendente.
10	Haca clic en la casilla de verificación de un dispositivo para seleccionarlo. Al seleccionar uno o más dispositivos, la barra de herramientas del panel muestra un icono o en el que puede hacer clic para acceder a la ventana Dispositivo (consulte **Uso de las funciones de la ventana Información de dispositivo, en la página 76**). Haga clic en la casilla de verificación de la parte superior de la columna para seleccionar o eliminar la selección de todos los dispositivos. Consulte **Edición y realización de acciones en varios dispositivos, en la página 95**.
11	Iconos del dispositivo. Haga clic con el botón derecho en el icono de un dispositivo para acceder a las opciones que permiten editar y realizar acciones en el dispositivo o abrir una conexión web, RDP o VNC al dispositivo con los parámetros de conexión actuales de ese dispositivo. Consulte **Trabajar con dispositivos del cliente, en la página 75**.
12	El resaltado indica el cliente que está seleccionado en ese momento.

Personalización de la vista Lista de dispositivos

Para personalizar la vista Lista de dispositivos, mueva el ratón sobre el enlace **Personalizar** en el panel y seleccione **Ajustes de lista de dispositivos**.

Haga clic en las casillas de verificación para agregar o eliminar columnas de la vista. Haga clic en **Seleccionar todo** o **No seleccionar ninguno** para cambiar rápidamente la selección de columnas.

Sus selecciones se guardan para el dispositivo que está utilizando para acceder al portal. Si utiliza un dispositivo diferente para acceder al portal, se utilizará la configuración predeterminada y tendrá que rehacer la configuración personalizada. Haga clic en **Restablecer valores predeterminados** para acceder a las opciones de restablecimiento de todos los ajustes del panel o a los ajustes de una categoría específica.

Columna de datos	Descripción
Estado	El estado puede tener uno de estos valores: CORRECTO (el proceso de detección determina que el dispositivo está presente), FALTA (si el dispositivo se ha detectado previamente pero no está presente actualmente) o AGREGADO (dispositivo agregado manualmente).
Categoría	La categoría general del dispositivo (por ejemplo, Infraestructura, Telefonía, etc.).
Clase de dispositivo	La información de la clase de dispositivo obtenida durante la detección (por ejemplo, teléfono, switch, router o desconocido).
Tipo de dispositivo	Número del modelo de dispositivo, obtenido durante la detección.
Información de Windows (WMI)	Información proporcionada por la Interfaz de administración de Windows, si está habilitado el acceso a WMI y el dispositivo es compatible con WMI.
Descripción	Descripción del dispositivo especificada por el usuario.
Se vio por primera vez	La fecha y la hora de la primera detección del dispositivo en la red.
Dirección MAC	Identificador único hexadecimal de 12 caracteres para este dispositivo.
Dirección IP	Dirección IP de la LAN de este dispositivo.
Monitores	Número de monitores habilitados actualmente para este dispositivo.
Plataforma del dispositivo	Información de la plataforma del dispositivo obtenida durante la detección. En el caso de algunos dispositivos, es igual al Tipo de dispositivo o al Nombre del dispositivo.
Estado de copia de seguridad	Fecha de la última copia de seguridad, si procede. Se muestra No compatible si el dispositivo no admite copias de seguridad de la configuración a través del portal.
Ajustes de conexión	Ajustes de la conexión web (HTTP/HTTPA) configurada actualmente para este dispositivo.
Se vio por última vez	Últimos protocolos de detección que proporcionaron información acerca del dispositivo, por ejemplo, CAM, ARP, CDP, DHCP, DDNS, etc.
Número de serie	Número de serie del dispositivo, si se conoce.

Visualización del estado de los clientes

Para ver el estado actual de OnPlus Service, haga lo siguiente:

- Compruebe la columna Estado en la página de información general de la cuenta de partner. Mueva el ratón sobre el icono Estado para ver una descripción.
- Seleccione **Estado** en el panel del cliente. El estado puede ser:
  - **Activación en espera.** Se ha agregado el cliente, pero OnPlus Network Agent no se ha conectado a la red del cliente ni se ha activado con el portal.
  - **Activado, En línea**. Funcionamiento normal.
  - **Cuenta suspendida**. La cuenta del cliente se ha suspendido. Consulte **Suspensión y reanudación de una cuenta de cliente, en la página 44**.
  - **Sin conexión**. OnPlus Network Agent se ha instalado y activado, pero no se está comunicando con el portal.

    Si el agente está conectado a la red del cliente, está encendido y no se está reiniciando o actualizando, pero su estado es Sin conexión, puede significar que la conexión WAN del cliente no está activa. También es posible que la configuración del cortafuegos de la red del cliente esté bloqueando el tráfico de salida en los puertos que el agente utiliza para comunicarse con el portal (consulte **Requisitos de acceso a puertos y protocolos, en la página 23**).

Instalación y administración de las aplicaciones de OnPlus

Para ver las aplicaciones de Cisco OnPlus disponibles e instalarlas para un cliente, seleccione el cliente en la lista de la página Descripción general y, a continuación, seleccione **Aplicaciones**.

Las aplicaciones se agregan para cada cliente por separado. Para comenzar a agregar y configurar una aplicación, localice la aplicación en la lista Todo y haga clic en **Instalar**.

Actualmente, existen los siguientes servicios disponibles:

- **Autotask**. Instale y configure esta aplicación para integrar OnPlus Portal con la creación de vales de servicio de Autotask. Consulte **Integración de la creación de vales de servicio de Autotask, en la página 185**.
- **ConnectWise**. Instale y configure esta aplicación para integrar OnPlus Portal con la creación de vales de servicio de ConnectWise. Consulte **Integración de la creación de vales de servicio de ConnectWise, en la página 197**.
- **Supervisión de paquetes ntop**. Instale la aplicación ntop en Cisco OnPlus Network Agent. Puede utilizarse ntop para la supervisión de paquetes a través de NetFlow o la conmutación de puertos con salida enviada al puerto MON del dispositivo OnPlus Network Agent. Una vez instalada la aplicación, puede iniciar ntop desde OnPlus Portal. Consulte **Habilitar la aplicación Supervisión de paquetes ntop, en la página 207**.

Para utilizar estas aplicaciones, debe hacer lo siguiente:

- Configurar los ajustes de la aplicación para habilitar la integración con OnPlus Portal.
- Configurar los ajustes de las aplicaciones en OnPlus Portal.
- Para Autotask y ConnectWise, también debe configurar reglas y contactos de entrega para que puedan enviarse notificaciones de eventos de OnPlus Portal a las aplicaciones Autotask o ConnectWise para crear vales de servicio.

Las siguientes notas de la aplicación están disponibles en Cisco.com, en www.cisco.com/go/onplus.

- *Integración de la creación de vales de servicio de Autotask con Cisco OnPlus Portal*
- *Integración de la creación de vales de servicio de ConnectWise con Cisco OnPlus Portal*

6

Trabajar con dispositivos del cliente

En este capítulo se explica cómo supervisar y administrar los dispositivos de las redes de los clientes a través de OnPlus Portal. Consulte las siguientes secciones:

- **Acceso a la ventana Información de dispositivo**
- **Uso de las funciones de la ventana Información de dispositivo**
- **Soporte para Instrumental de administración de Windows (WMI)**
- **Edición y realización de acciones en varios dispositivos**

Acceso a la ventana Información de dispositivo

La ventana Información de dispositivo es la interfaz principal para interactuar con los dispositivos que se encuentran en las instalaciones del cliente. Desde esta ventana, puede ver y editar los detalles del dispositivo y los monitores, proporcionar credenciales de acceso a los dispositivos y realizar acciones en ellos.

Para abrir la ventana Información de dispositivo, siga estos pasos.

PASO 1 Abra el panel del cliente en cuestión y localice el dispositivo al que quiera acceder.

PASO 2 Utilice uno de los siguientes métodos para abrir la ventana:

a. Desde la vista Topología de red del panel, mueva el ratón sobre el icono de un dispositivo y, a continuación, haga clic en el icono .

b. Desde la vista Lista de dispositivos, haga clic en la casilla de verificación para seleccionar el dispositivo y, a continuación, haga clic en el icono (Información de dispositivo) en la barra de herramientas del panel.

Uso de las funciones de la ventana Información de dispositivo

El siguiente diagrama ilustra las principales funciones y áreas de interés de la ventana Información de dispositivo.

Si el dispositivo no admite una función en particular, la ficha de esa función no se mostrará.

Ele-mento	Descripción
1	La barra de título de la ventana Información de dispositivo muestra el Nombre del dispositivo.
2	El icono del dispositivo, la dirección IP y la dirección MAC se encuentran en la parte superior de la ventana.
3	**Ajustes**. Realice acciones en el dispositivo seleccionado y visualice o modifique los ajustes para identificar mejor el dispositivo y su categoría.
4	**Credenciales**. Proporcione credenciales de acceso al dispositivo para habilitar las funciones del portal que requieren el acceso al dispositivo, como las actualizaciones de firmware, la exploración del dispositivo durante al detección o la copia de seguridad y la restauración de la configuración.

Elemento	Descripción
5	**Conexión**. Administre la configuración de conexión remota y establezca una conexión remota a un determinado dispositivo a través de OnPlus Portal.
6	**Información**. Visualice información del dispositivo sin formato obtenida para el dispositivo seleccionado durante la detección.
7	**Monitores**. Visualice, agregue y administre monitores de dispositivos para dispositivos seleccionados.
8	**Eventos**. Visualice el historial de eventos para el dispositivo seleccionado.
9	**Copias de seguridad**. Haga copias de seguridad, restaure, descargue o cargue la configuración del dispositivo para dispositivos Cisco compatibles.
10	**Firmware**. Visualice, cargue, descargue o instale firmware para dispositivos Cisco compatibles.
11	**Notas**. Agregue notas para el dispositivo seleccionado.
12	**Soporte** (no se muestra). Para los dispositivos Cisco compatibles, puede ver información de garantía, número de serie, avisos de campo, información de contrato de servicio, avisos de seguridad del producto y anuncios de final de ciclo de vida, final de servicio o final de la venta. La información de contrato de servicio y garantía podría no estar disponible para todos los dispositivos Cisco.
13	**Estadísticas de WAN (datos de rendimiento de la red WAN)** (no se muestra). Visualice los datos de rendimiento de red WAN supervisados a través de OnPlus Network Agent y el dispositivo que proporciona el enlace WAN.
14	**Área de estado** (solo en la ficha Ajustes). Aquí se muestran todas las alarmas que se hayan detectado o las acciones que puedan realizarse en el dispositivo. Pase el ratón sobre el área de estado para ver más información. También puede habilitar y deshabilitar la visualización de alarmas.

Consulte las siguientes secciones para ver información detallada sobre el uso de las opciones de cada una de las fichas de la ventana Información de dispositivo.

- **Ajustes**
- **Credenciales**
- **Conexión**
- **Información**
- **Monitores**
- **Eventos**
- **Firmware**

- Notas
- Copias de seguridad
- Estadísticas de WAN (datos de rendimiento de la red WAN)
- Soporte

Ajustes

Los siguientes menús de acciones y ajustes están disponibles en la pestaña Ajustes:

- Área de **Estado**. Visualice el estado para comprobar si se han detectado alarmas o si hay acciones que puedan realizarse en el dispositivo.

  Si aparecen varios mensajes, pase el ratón sobre el área de estado para verlos. Para habilitar o deshabilitar la visualización de estas alarmas en la ventana Información de dispositivo, haga clic en la X que aparece a la derecha de cada alarma.

- **Nombre del dispositivo**, **Descripción del dispositivo**. Escriba el nombre y la descripción que se mostrarán para el dispositivo. Pueden incluir caracteres alfanuméricos, espacios, guiones (-), guiones bajos (_) y dos puntos (:).

- Habilite la opción **Bloquear**, a la derecha del campo Nombre del dispositivo, para evitar que el nombre se actualice cuando se ejecute la detección del dispositivo.

- **Dirección MAC**, **Dirección IP**. Visualice la dirección MAC y la dirección IP detectadas para el dispositivo. Si el dispositivo se agregó manualmente y no se ha podido detectar la dirección MAC o la dirección IP, puede introducir aquí esos valores de forma manual.

  Una vez detectada la dirección MAC o la dirección IP, estos campos pasan a ser de solo lectura.

- **Icono**. Seleccione un icono diferente que se mostrará para el dispositivo en la vista Panel. Esta opción no es aplicable a OnPlus Network Agent. Cuando se selecciona **Icono específico de dispositivo**, se muestra el icono encontrado durante la detección.

- **Categoría**. Seleccione una categoría para el dispositivo. Las categorías de dispositivo pueden utilizarse para filtrar los dispositivos en las vistas Topología de red o Lista de dispositivos.

Para agregar una categoría de dispositivo personalizada que se muestre en la lista de categorías, pase el ratón sobre el icono en la barra de herramientas del panel y seleccione **Categorías de dispositivo**.

- **Acciones**. Realice acciones en el dispositivo. Haga clic en **Confirmar** para llevar a cabo la acción seleccionada.

  Las acciones disponibles varían en función del dispositivo que se está visualizando. A continuación se muestra una lista de acciones.

Acción	Se aplica a	Descripción
Hacer copia de seguridad de configuración de dispositivo	Dispositivos Cisco que admitan la copia de seguridad y restauración de la configuración a través de OnPlus portal	Se solicita una copia de seguridad de configuración para este dispositivo. Asegúrese de que ha proporcionado credenciales de acceso válidas para el dispositivo. Si la configuración del dispositivo no ha cambiado desde que tuvo lugar la última copia de seguridad, la copia no se realiza y se muestra un aviso. Consulte **Copias de seguridad, en la página 88**.
Conectarse al dispositivo a través de la Web	Cualquier dispositivo	Se abre una conexión web al dispositivo a través de HTTP/HTTPS, utilizando la configuración actual del dispositivo. Esta configuración se encuentra en la ficha Conectar, en la sección Web de la ventana Información de dispositivo. Para ver más información y procedimientos detallados, consulte **capítulo 8, "Conexión a dispositivos desde el portal".**
Desactivar este sitio completo	Solo OnPlus Network Agent	Se eliminan todas las asociaciones y se deshabilita la comunicación entre OnPlus Network Agent y el portal. Esta opción puede utilizarse en caso de pérdida o robo de OnPlus Network Agent, si la unidad es defectuosa o si desea reactivar el dispositivo, ya sea para el cliente actual o para otro cliente.
Eliminar este dispositivo	Dispositivos ausentes o agregados manualmente que no se han detectado	Se elimina de la Topología el dispositivo seleccionado. El dispositivo no puede eliminarse si su eliminación provoca que otros dispositivos de la vista Topología se desconecten del resto de la jerarquía. Esta opción se aplica únicamente a dispositivos ausentes de la red o que se han agregado manualmente y no se han detectado.

Acción	Se aplica a	Descripción
Establecer este dispositivo como raíz	Cualquier dispositivo	Se establece el dispositivo seleccionado como dispositivo raíz para la red del cliente.
Reiniciar dispositivo	Solo OnPlus Network Agent	Se reinicia OnPlus Network Agent.
Activar detección	Solo OnPlus Network Agent	Se inicia manualmente la detección del dispositivo para el sitio.
Actualizar firmware	Solo OnPlus Network Agent	Se actualiza el firmware en este dispositivo. El dispositivo se reinicia después de la actualización. Esta opción solo se muestra si hay una actualización de firmware disponible. OnPlus Network Agent debe estar presente en la red y tener el estado **En línea, Correcto**.

Credenciales

La ficha Credenciales está activa para la mayoría de los dispositivos.

Desde esta ficha pueden administrarse varios tipos de credenciales de acceso. Para obtener más información, consulte estas secciones:

- **Acceso de inicio de sesión, en la página 80**
- **Habilitar acceso (dispositivos Cisco IOS), en la página 82**
- **Acceso a SNMP, en la página 82**
- **Acceso a WMI, en la página 83**
- **Controlador de dispositivo, en la página 84**

Acceso de inicio de sesión

Las credenciales de acceso de inicio de sesión se utilizan para:

- La exploración del dispositivo durante la detección y las actualizaciones de topología.
- El acceso a los dispositivos para realizar funciones de mantenimiento, como la copia de seguridad de la configuración y las actualizaciones de firmware.

Las opciones de acceso de inicio de sesión le permiten:

- **Introducir las credenciales de inicio de sesión para habilitar el acceso al dispositivo**, de modo que puedan detectarse dispositivos de red adicionales (por ejemplo, teléfonos u otros dispositivos que se encuentren tras un switch o router gestionados) y se puedan llevar a cabo determinadas acciones, como actualizaciones de firmware o copias de seguridad de la configuración. También son necesarias las credenciales de acceso al dispositivo para obtener información de garantía y contrato de servicio de Cisco.

  SUGERENCIA Debe hacer clic en **Aceptar** después de introducir las credenciales para que estas se envíen al portal. Debe pasar al menos un ciclo de detección para que se validen las credenciales. Espere unos minutos y, a continuación, consulte la ficha de credenciales para comprobar que son válidas.

- **Habilitar o deshabilitar el acceso de inicio de sesión para un dispositivo**. Si no está marcada (deshabilitada) la opción **Permitir acceso de inicio de sesión**, los campos Nombre de usuario y Contraseña estarán deshabilitados, el proceso de detección de dispositivos no intentará ir más allá del dispositivo (la exploración de la topología está deshabilitada) y las tareas de mantenimiento diario automatizadas no se ejecutarán en el dispositivo.

- **Eliminar las credenciales existentes para un dispositivo**. Para eliminar las credenciales de un dispositivo, marque la opción **Eliminar credenciales existentes** y, a continuación, haga clic en **Aceptar** y cierre la ventana. La próxima vez que acceda a la ficha, los campos de las credenciales estarán vacíos y podrá agregar credenciales nuevas.

Si los campos Nombre de usuario y Contraseña están resaltados en color azul brillante, esto indica que OnPlus Network Agent no ha podido acceder al dispositivo. La lista Tarea pendiente del portal también indicará que se necesitan las credenciales.

Para habilitar el acceso, escriba el nombre de usuario y la contraseña para el dispositivo y haga clic en **Aceptar**. Si las credenciales son válidas, se actualiza la ficha Conectar para indicar que es posible acceder al dispositivo. En las vistas Topología de red y Lista de dispositivos se muestran ahora los dispositivos adicionales detectados.

Si posteriormente se cambia el nombre de usuario y la contraseña y OnPlus Network Agent no puede acceder al dispositivo, se mostrará una **X** y el mensaje **Las credenciales no fueron válidas la última vez que se probaron** en el área de estado. Los campos de las credenciales también estarán resaltados en color azul.

Habilitar acceso (dispositivos Cisco IOS)

En el caso de los dispositivos Cisco IOS, el administrador puede especificar una contraseña diferente que los usuarios deban utilizar para acceder al modo `habilitar` (predeterminado) o a un nivel de privilegio específico.

Debe introducir la contraseña habilitada para poder realizar al copia de seguridad o la restauración de la configuración o para actualizar el firmware en estos dispositivos.

Acceso a SNMP

Desde la ficha Acceso a SNMP (Simple Network Management Protocol, Protocolo simple de administración de red), puede habilitar o deshabilitar el acceso a la administración de SNMPv2 o SNMPv3 introduciendo las credenciales de SNMP. El acceso a la administración de SNMP se utiliza actualmente solo para habilitar las actualizaciones de firmware y la copia de seguridad/restauración de la configuración en dispositivos Cisco SF300/SG300 y para obtener información de detección adicional para switches gestionados genéricos.

IMPORTANTE Antes de establecer el acceso a la administración de SNMP a través del portal, debe configurar y habilitar SNMP en el dispositivo. Consulte la documentación del dispositivo para obtener información acerca de las versiones de SNMP (v. 2 o v. 3) que son compatibles con el dispositivo.

Limitaciones. Las siguientes limitaciones se aplican al acceso a la administración de SNMP a través de OnPlus Portal:

- Una vez habilitado el acceso a la administración a SNMP para un dispositivo a través del portal, este siempre utilizará las credenciales de acceso de SNMP para la autenticación. Si no desea que esto sea así, deberá eliminar las credenciales de acceso a SNMP y deshabilitar el servicio SNMP.
- El acceso a la autenticación SNMP utiliza solo frases de contraseña, no admite claves.
- Siempre se utiliza el ID de motor predeterminado.

Dispositivos Cisco compatibles con OnPlus Portal. Los únicos dispositivos Cisco compatibles con OnPlus Portal que admiten SNMP v. 2 y SNMP v. 3 son los switches de las series SG300 y SF300. Consulte **SG300 o SF300 (versión 1.0 del firmware), en la página 242** y **SG300 o SF300 (versión 1.1 del firmware), en la página 244** para obtener información acerca de los pasos necesarios para configurar el acceso a la administración de SNMP a través del portal en estos dispositivos.

Switches gestionados genéricos o routers gestionados genéricos (dispositivos Cisco no compatibles con OnPlus y dispositivos que no sean Cisco). Estos dispositivos se muestran como Dispositivos desconocidos en la vista Topología (la detección de dispositivos no compatibles no está garantizada). Para identificar estos dispositivos, habilite y configure los ajustes de SNMP en el dispositivo, abra la ventana Información de dispositivo en el portal y haga clic en la ficha **Credenciales** > **Controlador de dispositivo**; seleccione **Switch gestionado genérico, SNMPv2/3** o **Router gestionado genérico, SNMPv2/3** y haga clic en **Aceptar**. Por último, vaya a la ficha **Acceso a SNMP**, introduzca las credenciales de SNMP y haga clic en **Aceptar**. Una vez completado el siguiente ciclo de detección, se mostrará toda la información adicional detectada y el icono del dispositivo mostrará “SNMP”.

Acceso a WMI

Se utilizan credenciales de Acceso a WMI para proporcionar información de detección adicional para equipos Microsoft Windows.

Cuando está habilitado el acceso a WMI para un equipo Windows, se recopila la siguiente información de WMI y se muestra en la ficha de información de la ventana Información de dispositivo.

- Service Pack, versión principal
- Service Pack, versión secundaria
- Tamaño total de la memoria visible, en kilobytes (por ejemplo, un valor de 2061856 equivale aproximadamente a 2 GB)
- Nombre (nombre de Windows para el equipo)
- Descripción (descripción de Windows para el equipo)
- Plataforma (plataforma del sistema operativo Windows, por ejemplo, Microsoft Windows XP Professional)
- Sistema operativo (el mismo que la plataforma), por ejemplo: Microsoft Windows XP Professional
- Número de serie del SO Windows instalado en el equipo

Para obtener información sobre cómo habilitar el acceso a WMI en los equipos del cliente, introducir credenciales y agregar monitores de WMI a los dispositivos, consulte **Soporte para Instrumental de administración de Windows (WMI), en la página 91**.

Controlador de dispositivo

Para los dispositivos Cisco que se hayan detectado automáticamente, se mostrará el mensaje "`Se ha detectado un controlador para este dispositivo y está en uso`".

Algunos dispositivos Cisco no admiten ninguna forma de detección identificable o pueden configurarse de modo que los protocolos de detección estén deshabilitados (por ejemplo, por razones de seguridad). Por consiguiente, estos dispositivos podrían aparecer como Dispositivos desconocidos en la vista Topología de red o la vista Lista de dispositivos, y se muestra el mensaje "`No se puede identificar el controlador adecuado para este dispositivo automáticamente`".

Para obtener información sobre la selección de controladores genéricos para dispositivos Cisco IOS y dispositivos que no son de Cisco, consulte **Controladores de dispositivo para router IOS genérico y switch IOS genérico, en la página 85** y **Controladores de dispositivos SNMP genéricos, en la página 85**.

Para ver información sobre la detección para estos dispositivos, siga estos pasos.

PASO 1 En la ficha Credenciales, haga clic en **Acceso de inicio de sesión** e introduzca las credenciales de inicio de sesión para el dispositivo. Consulte **Acceso de inicio de sesión, en la página 80**.

PASO 2 Si fuera necesario, haga clic en **Habilitar acceso**, en la ficha Acceso, e introduzca la contraseña habilitada para el dispositivo. Consulte **Habilitar acceso (dispositivos Cisco IOS), en la página 82**.

PASO 3 Si está seleccionando uno de los controladores de dispositivo de SNMP, asegúrese de que ha habilitado SNMP en el dispositivo y de que ha introducido las credenciales de acceso a SNMP. Consulte **Acceso a SNMP, en la página 82**.

PASO 4 En la ficha Credenciales, haga clic en **Controlador de dispositivo**.

PASO 5 Seleccione el dispositivo adecuado en la lista desplegable de dispositivos Cisco compatibles.

PASO 6 Haga clic en **Aceptar**.

Controladores de dispositivo para router IOS genérico y switch IOS genérico

Para mejorar la detección de dispositivos Cisco IOS que no son compatibles actualmente con OnPlus Portal, seleccione **Router IOS genérico** o **Switch IOS genérico** como controlador de dispositivo.

Antes de seleccionar el controlador de dispositivo Router IOS genérico o Switch IOS genérico, deberá:

- Habilitar CDP y Vecinos CDP en el dispositivo.
- Proporcione las credenciales de inicio de sesión y habilitación de acceso en OnPlus Portal. Consulte **Acceso de inicio de sesión, en la página 80** y **Habilitar acceso (dispositivos Cisco IOS), en la página 82**.

Los controladores de dispositivos IOS genéricos proporcionan la capacidad de detección y ejecución entre aplicaciones a través del portal. No es posible realizar la copia de seguridad y restauración de la configuración de los dispositivos, ni actualizaciones de firmware a través del portal.

Controladores de dispositivos SNMP genéricos

Para mejorar la detección de dispositivos que no son de Cisco, utilice el controlador de dispositivo SNMP genérico.

Antes de seleccionar el controlador de dispositivo SNMP genérico, deberá:

- Habilitar SNMP en el dispositivo.
- Introducir las credenciales de acceso a SNMP en el portal.

Los controladores SNMP genéricos utilizan una MIB (Management Information Base, base de información de gestión) denominada QBRIDGE para obtener información de la tabla CAM (Content Addressable Memory, memoria de contenido direccionable). Si el dispositivo es compatible con QBRIDGE, la información de la tabla CAM incluirá la información de VLAN, además de la dirección y el puerto MAC. Esto proporciona de manera indirecta información sobre todas las VLAN que se están utilizando, ya que se pueden ver en el switch. También podría detectarse alguna topología adicional si existe compatibilidad con QBRIDGE. Si el dispositivo no es compatible con QBRIDGE, se utilizará la MIB BRIDGE, que no incluye información de VLAN.

El controlador de dispositivo SNMP genérico proporciona la capacidad de detección y ejecución entre aplicaciones a través del portal. No es posible realizar la copia de seguridad y restauración de la configuración de los dispositivos, ni actualizaciones de firmware a través del portal.

Conexión

Desde la ficha Conectar, puede conectarse de forma remota a un dispositivo desde el portal para acceder a su utilidad de administración.

Las opciones que especifique dependen del tipo de conexión remota que se seleccione. Se admiten las conexiones web (HTTP/HTTPS), Protocolo de escritorio remoto (RDP), Computación virtual en red (VNC) y de túnel genérico a un solo puerto TCP.

Para obtener información importante sobre limitaciones y directrices de uso de esta función, sugerencias para la solución de problemas, opciones avanzadas y ajustes de conexión recomendados para dispositivos Cisco, consulte **capítulo 8, “Conexión a dispositivos desde el portal”.**

Información

La ficha Información incluye información de solo lectura acerca de cada dispositivo que se recopila durante la detección del dispositivo. La información varía en función del tipo de dispositivo y puede incluir el SKU (plataforma), la dirección MAC, la versión del firmware, la dirección IP, el protocolo de administración, el puerto de administración, las funcionalidades, el modelo y el número de serie.

Consulte la columna Descripción de cada campo para ver más información sobre lo que representan los datos.

Si está habilitado el acceso a WMI para un equipo Windows, se mostrará información adicional. Consulte **Soporte para Instrumental de administración de Windows (WMI), en la página 91**.

Monitores

En la ficha Monitores, puede agregar, eliminar o poner en pausa los monitores de eventos de un dispositivo. En función del tipo de dispositivo que esté supervisando, habrá diferentes monitores de eventos disponibles.

Para cualquier dispositivo que no sea OnPlus Network Agent o el dispositivo que proporciona el enlace WAN, esta ficha estará vacía la primera vez que acceda a ella, puesto que no se habrán agregado aún monitores de eventos.

NOTA Los monitores de eventos de OnPlus Network Agent (Rendimiento de red, Carga de CPU, IP duplicada, Servidor DHCP, Servicio de DNS y Memoria) están habilitados de forma predeterminada. Los monitores de OnPlus Network Agent no se pueden eliminar, pero pueden deshabilitarse. Puede establecer niveles de gravedad para los monitores y editar su configuración.

Para obtener más información, consulte **Cómo agregar y administrar monitores de dispositivos, en la página 112**.

Eventos

Para los dispositivos que tengan la supervisión habilitada, esta ficha muestra el historial de eventos del dispositivo. Los eventos de la lista tienen un color diferente según su nivel gravedad. El evento seleccionado en ese momento está marcado en azul.

Para ver más información acerca de los tipos de eventos, consulte **Tipos de eventos, en la página 125**.

Para ver instrucciones sobre cómo supervisar eventos y cómo establecer reglas de entrega y los contactos que recibirán las notificaciones de los eventos, consulte **Supervisión y notificaciones, en la página 99**.

Firmware

En la ficha Firmware puede visualizar, instalar, cargar o descargar firmware cargado previamente para dispositivos Cisco. Esta ficha no se muestra en el caso de los dispositivos que no sean Cisco y los dispositivos Cisco que no admiten actualizaciones de firmware a través del portal.

Para obtener más información, consulte **Carga de firmware de dispositivo al portal, en la página 147** y **Instalación del firmware del dispositivo, en la página 149**.

Notas

Utilice la ficha Notas para registrar información textual acerca de un dispositivo remoto en el sitio de un cliente. Agregue, modifique o elimine el texto y haga clic en **Aceptar**.

Copias de seguridad

Se realiza una copia de seguridad de la configuración (si ha cambiado) de los dispositivos que lo admiten una vez cada 24 horas, durante el periodo de mantenimiento del sitio del cliente. Las últimas cinco operaciones de copia de seguridad se muestran en la ficha Copias de seguridad de la ventana Información de dispositivo.

Esta ficha solo se muestra para los dispositivos Cisco que admiten la copia de seguridad y la restauración de la configuración a través de OnPlus Portal.

Para determinados dispositivos Cisco, puede realizar una copia de seguridad, restaurar o cargar la configuración del dispositivo utilizando las opciones de la ficha **Copias de seguridad**.

- Para realizar las operaciones de copia de seguridad y restauración se requieren unas credenciales de acceso válidas. Algunos dispositivos Cisco podrían requerir una contraseña habilitada, además de las credenciales de inicio de sesión. Consulte **Credenciales, en la página 80**.
- Pueden archivarse hasta cinco copias de seguridad de la configuración para cada dispositivo. La columna **Origen** indica si la copia de seguridad se ha generado directamente desde el dispositivo o si se ha cargado al dispositivo.
- También se muestra aquí cualquier comentario opcional que se haya agregado para un archivo de copia de seguridad de la configuración. Seleccione el archivo de copia de seguridad y abra el cuadro de detalles para editar o agregar comentarios.
- Puede restaurar la configuración de un dispositivo anterior desde una de las copias de seguridad guardadas o puede cargar un archivo de configuración y restaurarla.

Para obtener más información, consulte:

- **Solicitud de copia de seguridad de la configuración de un dispositivo**
- **Carga de un archivo de configuración del dispositivo**

- **Descarga, eliminación y restauración de archivos de configuración del dispositivo**

Solicitud de copia de seguridad de la configuración de un dispositivo

Haga clic en **Hacer copia de seguridad ahora** para solicitar una copia de seguridad inmediata de la configuración del dispositivo. Al hacer clic en **Hacer copia de seguridad ahora**, el portal muestra un aviso de solicitud de copia de seguridad. Si el portal detecta que la configuración no ha cambiado, se le notifica que no se ha creado la copia de seguridad.

Carga de un archivo de configuración del dispositivo

Haga clic en **Cargar archivo** para cargar un archivo de configuración del dispositivo en OnPlus Portal. De este modo puede distribuir configuraciones que se sabe que funcionan a dispositivos de destino.

IMPORTANTE Puesto que la forma de interpretar los archivos de configuración varía en función del dispositivo, usted será responsable de que el archivo de configuración que se envía al dispositivo esté completo, así como de su formato, estructura e integridad. Por ejemplo, algunos dispositivos pueden aceptar y aplicar archivos de configuración parciales, mientras que otros dispositivos pueden requerir que se sustituya la configuración completa.

Cisco OnPlus portal no valida ni realiza ninguna comprobación de formato o contenido del archivo cargado.

Descarga, eliminación y restauración de archivos de configuración del dispositivo

Para acceder a las opciones que permiten agregar comentarios, descargar, eliminar y restaurar los archivos de configuración del dispositivo, mueva el ratón sobre el archivo de copia de seguridad deseado y haga clic en la entrada resaltada para abrir el cuadro de detalles.

- En el campo **Comentarios**, agregue o modifique los comentarios de la copia de seguridad seleccionada.
- Haga clic en **Restaurar** para restaurar una configuración volviendo a aplicar un archivo de configuración guardado previamente a un dispositivo y haciendo que esa sea la configuración actual.

  Cuando hace clic en **Restaurar** para seleccionar una copia de seguridad que desee restaurar, un mensaje muestra que se ha solicitado una restauración y se le solicita que confirme la operación. El dispositivo se reinicia tras completarse la operación de restauración.

- Haga clic en **Descargar** para descargar el archivo de copia de seguridad de la configuración del dispositivo en su equipo local.
- Haga clic en **Eliminar** para eliminar el archivo de copia de seguridad guardado en el portal.

Estadísticas de WAN (datos de rendimiento de la red WAN)

La ficha Estadísticas de WAN solo está activa en OnPlus Network Agent. Desde esta ficha puede ver los datos de rendimiento de la red WAN recopilados por el agente. Los datos se muestran en gráficos de oscilación, latencia y pérdida de paquetes.

Las estadísticas disponibles se miden según se describe a continuación.

- **Latencia.** La latencia es el recorrido medio de ida y vuelta entre OnPlus Network Agent y OnPlus Portal medido con 50 paquetes separados por 100 milisegundos. Se ejecuta una secuencia cada 5 minutos. Por lo general, los picos de latencia pueden indicar una congestión de la red entre esos dos puntos en cualquier dirección.
- **Oscilación**. La oscilación por paquete es la desviación de la latencia media medida en los últimos 10 paquetes. La oscilación es el promedio de la oscilación por paquete, que se mide con 40 muestras.
- **Pérdida de paquetes**. La pérdida de paquetes es el porcentaje de paquetes que no han regresado con respecto al número total de paquetes enviados.

Al hacer clic en esta ficha por primera vez, se muestra el siguiente mensaje.

“Los datos no están disponibles actualmente para los gráficos.
Se ha enviado una solicitud para recuperar los datos de ancho de banda del dispositivo. Pueden tardar varios minutos en aparecer. Puede volver más tarde si lo desea.”

Haga clic en **Aceptar** para cerrar la ventana. También puede esperar hasta que se muestre el gráfico.

Tras varios minutos, el gráfico se actualiza y puede verse el gráfico predeterminado, que muestra la Oscilación/Latencia en el tiempo, como se muestra en el siguiente ejemplo. La oscilación aparece en color azul y la latencia en color marrón. Pase el ratón sobre las barras del gráfico para ver los detalles.

Puede ajustar los parámetros del gráfico para el periodo de tiempo, los datos del gráfico (oscilación y latencia o pérdida de paquetes) y el tipo de interpolación (curva, lineal, escalonada).

Soporte

Para dispositivos Cisco, si se proporcionan las credenciales de acceso al dispositivo, y el número de serie y el ID de producto de Cisco se obtienen durante la detección, se mostrará aquí la información del producto Cisco.

Si no se trata de un dispositivo Cisco o si no hay información de soporte disponible para el dispositivo, no se mostrará la ficha Soporte.

Para obtener más información, consulte **Visualización de la información de soporte de productos Cisco, en la página 171**.

Soporte para Instrumental de administración de Windows (WMI)

Cuando se habilita el acceso a WMI para equipos Windows, el portal utiliza la interfaz de Instrumental de administración de Windows para obtener información del dispositivo y configurar los monitores del dispositivo.

IMPORTANTE La información que aquí se proporciona para habilitar el acceso a WMI en equipos Windows no pretende ser completa y podría no cubrir todos los temas relacionados con la habilitación de WMI y la configuración del acceso remoto a WMI.

- Antes de intentar habilitar el acceso a WMI a través de OnPlus Portal, asegúrese de que el acceso remoto a WMI se ha configurado correctamente y funciona en el equipo de su cliente.
- Para obtener más información, consulte la documentación de Microsoft para la versión del sistema operativo que se ejecuta en el equipo Windows o la base de conocimientos de soporte técnico de Microsoft.

Para ver más detalles, consulte estas secciones:

- Cómo habilitar el acceso a WMI, en la página 92
- Cómo agregar monitores de dispositivos WMI, en la página 93
- Cómo deshabilitar el acceso a WMI y eliminar las credenciales de acceso, en la página 94

Cómo habilitar el acceso a WMI

Para habilitar el acceso a WMI en el equipo Windows e introducir las credenciales de acceso a WMI en el portal, realice las siguientes tareas.

PASO 1 En el equipo Windows, siga estos pasos para habilitar el acceso a WMI:

a. Si el equipo ejecuta Windows Vista o Windows 7, deshabilite Control de cuentas de usuario (UAC).

b. Si el equipo ejecuta Windows XP, asegúrese de que Uso compartido simple de archivos está deshabilitado. Para ello, seleccione **Inicio> Panel de control> Opciones de carpeta**. En el diálogo Opciones de carpeta, seleccione la ficha Vista y desplácese a la parte inferior. Compruebe que la opción Uso **compartido simple de archivos** no está marcada. No debería ser necesario reiniciar el equipo después de cambiar esta opción.

c. Habilite los servicios WMI y DCOM en Windows. Para hacerlo, vaya a **Inicio** > **Ejecutar**, escriba **`services.msc`** y presione Intro.

d. Inicie los servicios **Instrumental de administración de Windows** y **DCOM** (Distributed Common Object Model, modelo de objetos componentes distribuido) si aún no se están ejecutando y compruebe que Tipo de inicio está establecido en **Automático**.

e. Habilite las solicitudes remotas de WMI.

   Es posible que tenga que reiniciar el equipo después de cambiar estas opciones para habilitar las solicitudes remotas de WMI.

La siguiente página de soporte de Microsoft ofrece información de ayuda y solución de problemas para equipos miembros de dominios Windows que pueden tener configuradas políticas de grupo que podrían interferir con WMI remoto a través de DCOM:

http://support.microsoft.com/kb/875605

PASO 2 Desde la página Descripción general, haga clic en un cliente para mostrar su panel.

PASO 3 Desde la vista Topología de red o la vista Lista de dispositivos del cliente, localice un equipo Windows con el acceso a WMI habilitado y haga clic en el icono Información de dispositivo (i) para abrir la ventana Información de dispositivo.

PASO 4 En la ventana Información de dispositivo, seleccione la ficha Credenciales y haga clic en **Acceso a WMI**.

PASO 5 Introduzca la siguiente información:

- **Nombre de usuario y Contraseña**: el nombre de usuario y la contraseña de Windows. Puede habilitar cualquier cuenta para que lea información de WMI. Por ejemplo, puede crear una cuenta que solo se utilice para acceder a WMI.
- **Dominio (opcional)**: si el equipo es miembro de un dominio, puede especificarlo. El campo de dominio solo es obligatorio si se trata de una cuenta de dominio. Si introduce un dominio, pero la cuenta no es miembro de un dominio, la información se ignora.

PASO 6 Marque la opción **Permitir acceso a WMI** para habilitar esta función.

PASO 7 Haga clic en **Confirmar**.

Para ver información relacionada, consulte **Cómo agregar monitores de dispositivos WMI, en la página 93** y **Cómo deshabilitar el acceso a WMI y eliminar las credenciales de acceso, en la página 94**.

Cómo agregar monitores de dispositivos WMI

Puede agregar uno o más monitores WMI a un equipo Windows para supervisar la cantidad de espacio libre en disco, el uso de memoria y si un proceso específico se está ejecutando o no en el equipo que se está supervisando.

Puede agregar tantos monitores WMI como necesite.

Las siguientes directrices y notas se aplican a la supervisión de WMI:

- Antes de supervisar eventos a mediante WMI, debe introducir las credenciales de acceso a WMI y asegurarse de que está habilitado el acceso a WMI para el equipo Windows. Para ver instrucciones sobre cómo hacerlo, consulte **Cómo habilitar el acceso a WMI, en la página 92**.
- Solo deben establecerse monitores WMI en dispositivos Windows compatibles con WMI.

- Cuando se superan los umbrales de supervisión de WMI para el espacio en disco y el uso de memoria, se genera un evento de tipo Supervisar: WMI. Cuando el valor que se está supervisando cae por debajo del umbral, se genera un evento de tipo Supervisar: WMI.
- Para un monitor WMI El proceso existe, se genera un evento si alguna vez se detecta que el nombre del proceso no se está ejecutando actualmente en la máquina. Se genera un evento cuando el monitor detecta que el proceso se está ejecutando de nuevo.

Los parámetros que se incluyen a continuación pueden establecerse para estos monitores.

Supervisar	Parámetros
Estado de unidad de disco	▪ Estados de advertencia: Degradado, Pred. de error, Con estrés, Desconocido ▪ Estados críticos: Error, Servicio, No recuperable, Sin contacto, Comunicación perdida
Espacio libre en disco	▪ Etiqueta de volumen (por ejemplo, C:) ▪ Umbral de espacio libre, en %; Advertencia. El valor predeterminado es 10%. ▪ Umbral de espacio libre, en %; Crítico. El valor predeterminado es 5%.
Memoria libre	▪ Umbral de memoria libre, en %; Advertencia. El valor predeterminado es 5%. ▪ Umbral de memoria libre, en %; Crítico. El valor predeterminado es 2%.
El proceso existe	▪ Uno o más nombres de proceso (por ejemplo, winlogon.exe). Utilice comas para separar varios elementos de la lista.

Cómo deshabilitar el acceso a WMI y eliminar las credenciales de acceso

Puede deshabilitar temporalmente el acceso a WMI sin eliminar las credenciales introducidas previamente o puede eliminar por completo las credenciales de WMI existentes.

Si está deshabilitado el acceso a WMI en un dispositivo, los monitores WMI de ese dispositivo no generarán eventos hasta que vuelva a habilitarse el acceso a WMI. Los monitores no están deshabilitados y se reactivan automáticamente cuando vuelve a permitirse el acceso a WMI. Si no desea que se reactive automáticamente la supervisión de WMI tras volver a habilitar el acceso, deshabilite los monitores WMI.

Si se agrega algún monitor WMI a un dispositivo y no se proporcionan las credenciales de WMI en la ficha Credenciales (o se eliminan las credenciales existentes), el icono del dispositivo en Topología de red se resalta inmediatamente. Al acceder al dispositivo para editarlo, la ficha Credenciales se selecciona automáticamente.

Para editar al configuración de acceso a WMI, siga estos pasos.

PASO 1 Abra el panel del cliente y localice el equipo Windows que tenga habilitado el acceso a WMI.

PASO 2 Desde al vista Topología de red o la vista Lista de dispositivos, abra la ventana Información de dispositivo, seleccione la ficha Credenciales y haga clic en **Acceso a WMI.**

PASO 3 Para deshabilitar temporalmente el acceso a WMI pero mantener las credenciales de acceso a WMI existentes, desactive la opción **Permitir acceso a WMI** y, a continuación, haga clic en **Aceptar.**

PASO 4 Para eliminar las credenciales existentes y deshabilitar el acceso a WMI, desactive la opción **Eliminar credenciales existentes** y, a continuación, haga clic en **Aceptar.**

Edición y realización de acciones en varios dispositivos

Puede seleccionar y abrir varios dispositivos para editarlos o realizar determinadas acciones en ellos desde la vista Topología o la vista Panel.

Las siguientes limitaciones se aplican al editar varios dispositivos:

- No puede abrir varias conexiones simultáneas desde el portal a varios dispositivos. Solo puede abrirse una conexión remota (Web, RDP, VNC o de túnel genérico) cada vez.

- Entre las acciones que puede realizar en varios dispositivos seleccionados se incluyen las siguientes (se entiende que la acción es compatible con todos los dispositivos seleccionados):
  - Copia de seguridad de la configuración
  - Reiniciar dispositivo
  - Eliminar dispositivos ausentes o agregados manualmente
  - Reorganización de la relación jerárquica de los dispositivos
- Al editar monitores para varios dispositivos, todos los monitores existentes se eliminan (excepto los monitores de red en OnPlus Network Agent, que no pueden eliminarse) y se sustituyen por nuevos monitores.

  Se le solicitará que confirme la acción de restablecimiento de monitor antes de continuar.

Para seleccionar y editar la configuración o realizar acciones en varios dispositivos, siga estos pasos.

PASO 1 En la página Descripción general, haga clic en la entrada de un cliente cuyos dispositivos desee editar.

PASO 2 Seleccione los dispositivos según se describe a continuación:

- En la vista Topología de red, mantenga presionada la tecla MAYÚS o CTRL y haga clic con el botón izquierdo del ratón en la parte inferior de los iconos de dispositivo para seleccionar los dispositivos que se van a editar. Los dispositivos seleccionados aparecen resaltados.

  También puede hacer clic y arrastrar con el ratón para seleccionar un grupo de dispositivos y utilizar Mayús + clic para agregar dispositivos a la selección o eliminarlos.

  Con los dispositivos seleccionados, mueva el ratón sobre cualquiera de los iconos de dispositivo y, a continuación, haga clic en el icono .
- En la vista Lista de dispositivos, haga clic en las casillas de verificación de los dispositivos que desee seleccionar.

  Con los dispositivos seleccionados, haga clic en el icono en la barra de herramientas del panel.

Como se muestra a continuación, las fichas, los ajustes y las acciones que son válidos para cualquiera de los tipos de dispositivo seleccionados pueden editarse. Los ajustes que estén en ese momento configurados con diferentes valores para los dispositivos seleccionados también se identifican.

PASO 3 Seleccione un ajuste que quiera editar o una acción que desee llevar a cabo.

Si está aplicando una acción, como un reinicio del dispositivo o una copia de seguridad de la configuración, la ventana se actualiza para incluir los dispositivos a los que se aplicará la acción.

PASO 4 Haga clic en **Aceptar** para aplicar los ajustes, en **Confirmar** para realizar la acción seleccionada o en **Cancelar**.

7

Supervisión y notificaciones

En este capítulo se explica cómo utilizar las funciones de supervisión de dispositivos y entrega de notificaciones de eventos de Cisco OnPlus Portal. Se tratan los siguientes temas:

- **Descripción general**
- **Contacto y regla de entrega predeterminados**
- **Cómo agregar y administrar contactos de entrega**
- **Uso de las reglas de entrega**
- **Cómo agregar y administrar monitores de dispositivos**
- **Visualización de eventos**

Descripción general

La función de supervisión y notificaciones de OnPlus Portal le permite recibir notificaciones por correo electrónico o SMS cuando se generan eventos supervisados. Esta sección cubre los siguientes temas:

- **Tipos de eventos que se pueden supervisar**
- **Notificaciones de eventos**
- **Proceso de configuración de monitores y notificaciones**
- **Ejemplo paso a paso**

Tipos de eventos que se pueden supervisar

A través de OnPlus Portal y OnPlus Network Agent puede supervisar lo siguiente:

- **Rendimiento de la red**. Se habilita un conjunto de monitores de red predeterminados en OnPlus Network Agent. Estos monitores generan

eventos cuando se superan los umbrales especificados o se cumplen las condiciones de los siguientes elementos:

- Rendimiento de red WAN (oscilación, latencia, ancho de banda)
- Direcciones IP duplicadas
- Disponibilidad del servicio de DHCP
- servicio de DNS
- Conectividad de OnPlus Agent, carga de CPU y uso de la memoria

- **Acciones en el portal**. Se generan otros eventos al supervisar las actividades del portal, como actualizaciones de firmware, reinicio de dispositivos, copia de seguridad o restauración de la configuración, detección de dispositivos, etc. La mayoría de estas actividades generan eventos con avisos de un determinado nivel de gravedad.
- **Avisos de información de soporte de Cisco**. Los eventos de soporte incluyen avisos de final del ciclo de vida, final de soporte o final de la venta, expiración del contrato de servicio, avisos de seguridad del producto y expiración de la garantía.
- **Dispositivos de los clientes**. Consulte **Descripción de los monitores de dispositivos, en la página 116** para ver información detallada sobre los tipos de eventos que puede supervisar en los dispositivos de los clientes.

Notificaciones de eventos

Para recibir notificaciones de eventos a través de correo electrónico o SMS, debe crear *contactos de entrega* y *reglas de entrega*:

- Los contactos de entrega se utilizan para especificar el destinatario de la notificación y los métodos de entrega que pueden utilizarse (correo electrónico o SMS).
- Las reglas de entrega permiten especificar criterios para el envío de notificaciones de eventos. El contacto y el método de entrega especificado en la regla determinan cómo y a quién se enviará el mensaje.
- Solo puede asociarse un contacto con una regla de entrega.

Al crear una cuenta en el portal, se crean automáticamente un contacto y una regla de entrega predeterminados. Consulte **Contacto y regla de entrega predeterminados, en la página 104**.

Para aprovechar las ventajas de las funciones de supervisión y notificación, configure monitores de dispositivos y reglas de entrega de notificaciones adicionales.

Para obtener más información, consulte estas secciones:

- **Proceso de configuración de monitores y notificaciones, en la página 101**
- **Ejemplo paso a paso, en la página 101**

Proceso de configuración de monitores y notificaciones

Para configurar monitores y notificaciones personalizados, siga estos pasos básicos:

1. Determine las condiciones y los dispositivos o los niveles de gravedad que desee supervisar y a quién debe notificarse cuando los monitores generen eventos.
2. Habilite y configure los monitores adecuados para estos dispositivos. De forma predeterminada, solo están habilitados los monitores de OnPlus Network Agent.
   Consulte **Cómo agregar y administrar monitores de dispositivos, en la página 112**.
3. Cree un contacto de entrega para recibir las notificaciones de eventos. Consulte **Cómo agregar y administrar contactos de entrega, en la página 104**.

   IMPORTANTE Se recomienda crear siempre el contacto de entrega antes que la regla, pues tendrá que asociar el contacto con su información de correo electrónico o SMS al crear la regla.
4. Cree una regla de entrega de notificaciones. Al crear la regla de entrega, utilizará la información de este contacto para el método de entrega. Consulte **Uso de las reglas de entrega, en la página 107**.
5. Realice una prueba del monitor del dispositivo y habilite la opción de generar un evento real basado en el resultado. Consulte **Prueba de monitoreo de dispositivos, en la página 115**.

Ejemplo paso a paso

El siguiente ejemplo ilustra el proceso básico de supervisión y notificaciones.

Escenario

Uno de sus clientes de OnPlus Portal, ABC Enterprises, tiene un servidor que ejecuta importantes aplicaciones empresariales. Le gustaría que su técnico, Marcos Arias, reciba una notificación por medio de SMS en su teléfono móvil cuando el servidor se desactiva o se activa.

PASO 1 En el portal, en la página Descripción general, haga clic en la entrada del cliente correspondiente a ABC Enterprises para ver su panel.

PASO 2 Habilite un monitor de estado activo/inactivo del host en el servidor.

a. Desde la vista Topología de red o la vista Lista de dispositivos, abra la ventana Información de dispositivo para el servidor que desea supervisar.

b. Seleccione la ficha **Monitores**.

c. Haga clic en el icono **+** para ver una lista de los monitores disponibles y seleccione Estado activo/inactivo del host. No hay más ajustes que configurar para este monitor.

   El estado activo/inactivo del host se supervisa mediante una solicitud de eco ICMP IPv4. Se genera un evento con nivel Crítico si no se puede acceder al host. Si el host vuelve a no ser accesible, se generará un evento de tipo Advertencia.

d. Haga clic en **Aceptar**.

e. Haga clic en **Inicio** para volver a la página de información general de la cuenta de partner.

PASO 3 Cree un contacto de entrega para el técnico, Marcos Arias.

a. En la página Descripción general, seleccione **Notificaciones** > **Contactos de envío**.

b. Haga clic en **+ Agregar contacto de entrega**.

c. Introduzca la información de contacto de Marcos y su dirección de correo electrónico SMS. Compruebe que la dirección de correo electrónico SMS está habilitada para recibir las notificaciones.

d. En el campo **Cliente**, seleccione **Ninguno**, ya que Marcos es un contacto global que no está asociado con un cliente específico.

e. En el campo **Idioma preferido**, seleccione en el menú el idioma del contacto. El idioma predeterminado es el inglés.

f. Haga clic en **Guardar**.

PASO 4 Cree una regla de entrega para que Marcos Arias reciba una notificación a través de un mensaje de texto SMS cuando tenga lugar un evento crítico de estado activo/inactivo del host para el cliente ABC Enterprises.

a. En la página Descripción general, seleccione **Notificaciones** > **Reglas de envío**.

b. Haga clic en **+ Agregar regla de entrega**.

c. En el campo del cliente, seleccione **ABC Enterprises**.

d. Haga clic en la casilla de verificación **Especificar evento**.

e. En la menú **Tipo de evento**, seleccione **Supervisar: estado ACTIVO/ INACTIVO del host (ICMP)** para el tipo de evento.

f. En la lista **Contacto**, seleccione Marcos Arias.

g. En la lista **Método de entrega**, seleccione la dirección de correo electrónico SMS de Marcos.

h. Haga clic en **Guardar**.

PASO 5 Haga una prueba del monitor y la regla de entrega.

a. Desde la vista Topología de red o la vista Lista de dispositivos, abra la ventana Dispositivo del servidor que desea supervisar.

b. Seleccione la ficha **Supervisar**.

c. Haga clic en el monitor **Estado activo/inactivo del host**.

d. Haga clic en **Probar monitor**.

e. Marque la opción **Generar un evento** al ejecutar la prueba.

f. Haga clic en **Ejecutar**. Se muestran los resultados de la prueba.

g. Haga clic en **Aceptar** para cerrar la ventana Información de dispositivo.

h. Haga clic en **Inicio** para volver a la página de información general de la cuenta de partner.

a. Seleccione **Notificaciones** > **Reglas de envío**.

b. Seleccione la regla de entrega que creó en el paso 4.

c. Haga clic en el número de **Envío de notificaciones** para la regla seleccionada.

d. Compruebe que se ha incluido la notificación generada al realizar la prueba del monitor de estado activo/inactivo del host.

e. Compruebe que se ha enviado el mensaje de texto SMS al teléfono de Marcos.

Contacto y regla de entrega predeterminados

Al crear una cuenta de partner y completar el registro en el portal, se crea una regla de entrega predeterminada, según la cual se envían las notificaciones para todos los eventos con nivel de gravedad de Advertencia o superior de todos los clientes a la dirección de correo electrónico de contacto de la cuenta de partner que se haya especificado al crearla.

Puede deshabilitar el envío de notificaciones a la dirección de correo electrónico de la cuenta de partner, editar o eliminar la regla de entrega predeterminada y administrar los contactos de entrega. Consulte **Uso de las reglas de entrega, en la página 107** y **Cómo agregar y administrar contactos de entrega, en la página 104**.

Cómo agregar y administrar contactos de entrega

Para habilitar el envío de notificaciones de informes o eventos a través de correo electrónico o SMS (Servicio de mensajes cortos), debe crear contactos de entrega y comprobar que las notificaciones están habilitadas para las direcciones de correo electrónico y SMS especificadas para los contactos de entrega.

IMPORTANTE Se recomienda crear siempre el contacto de entrega antes que la regla, pues tendrá que asociar el contacto con su información de correo electrónico o SMS al crear la regla.

Al agregar un cliente, tiene también la opción de crear un contacto para ese cliente. Este contacto se agrega automáticamente a la lista de contactos de entrega como contacto del cliente.

Cuando se crea un contacto de cliente, el campo **Cliente** indica si se trata de un contacto global o específico del cliente:

- Establezca el campo **Cliente** en **Ninguno** para crear un contacto global. Los contactos globales pueden recibir notificaciones de eventos e informes generados para alguno de los clientes o para todos ellos.
- Seleccione un cliente de la lista en el campo **Cliente** para asociar el contacto con un cliente. Un contacto asociado con un cliente específico solo puede recibir notificaciones de eventos o informes generados para ese cliente.

Para ver instrucciones, consulte estos temas:

- **Cómo agregar un contacto de entrega, en la página 105**
- **Edición de un contacto de entrega, en la página 106**
- **Eliminación de un contacto de entrega, en la página 106**
- **Cómo habilitar o deshabilitar las notificaciones a direcciones de correo electrónico o SMS, en la página 106**

Cómo agregar un contacto de entrega

Para agregar un contacto de entrega de las notificaciones, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, seleccione **Notificaciones** > **Contactos de envío**.

PASO 2 Haga clic en **+ Agregar contacto de entrega**.

PASO 3 Escriba la información necesaria.

Las direcciones de correo electrónico que aquí se proporcionen pueden seleccionarse como métodos de entrega al crear las reglas de entrega de notificaciones.

Las direcciones de correo electrónico SMS y las direcciones de correo electrónico SMS alternativas se usan para enviar mensajes de texto a teléfonos inteligentes y se deben introducir con el formato de dirección que requiera el proveedor de servicios telefónicos, por ejemplo: 9995551212@txt.proveedordeservicios.net.

PASO 4 Si desea asociar este contacto de entrega con un cliente, seleccione un cliente en el menú desplegable **Cliente**. De lo contrario, seleccione **Ninguno** para crear un contacto global.

PASO 5 Seleccione el idioma de este contacto en el menú del campo **Idioma preferido**. El idioma predeterminado es el inglés.

PASO 6 Haga clic en **Guardar**.

Edición de un contacto de entrega

Para editar un contacto de entrega, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, seleccione **Notificaciones** > **Contactos de envío**.

PASO 2 Haga clic en un contacto de la lista para abrir el cuadro de acciones.

PASO 3 Haga clic en **Editar**.

PASO 4 Cuando haya terminado de realizar los cambios, haga clic en **Guardar**.

Eliminación de un contacto de entrega

Si elimina un contacto de entrega asociado con una regla de entrega, la regla también se elimina.

Para eliminar un contacto de entrega, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, seleccione **Notificaciones** > **Contactos de envío**.

PASO 2 Haga clic en un contacto de la lista para acceder al cuadro de acciones.

PASO 3 Haga clic en **Eliminar**.

PASO 4 Haga clic en **Aceptar** para confirmar la eliminación.

Cómo habilitar o deshabilitar las notificaciones a direcciones de correo electrónico o SMS

Los mensajes de notificación enviados a direcciones de correo electrónico y SMS incluyen un enlace que permite al destinatario deshabilitar las notificaciones.

Puede habilitar o deshabilitar las notificaciones a direcciones de correo electrónico o SMS desde Cisco OnPlus Portal. Para ello, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, seleccione **Notificaciones** > **Contactos de envío**.

PASO 2 Haga clic en un contacto de la lista para abrir el cuadro de detalles.

PASO 3 Haga clic en los controles y para habilitar o deshabilitar las direcciones de correo electrónico y SMS que desee. Los cambios se aplican inmediatamente.

Uso de las reglas de entrega

Las reglas de entrega permiten especificar criterios para el envío de notificaciones de eventos.

Se crea una regla de entrega predeterminada durante el registro. Al registrarse en el portal y crear el perfil de la cuenta, se genera una regla de entrega predeterminada, que utiliza su nombre y dirección de correo electrónico de trabajo. La regla predeterminada genera notificaciones para todos los eventos con un nivel de gravedad de Advertencia o superior para todos los clientes. Puede eliminar o editar esta regla predeterminada en cualquier momento.

IMPORTANTE Antes de poder crear reglas de entrega adicionales, deberá establecer los contactos de entrega y asegurarse de que se establecen direcciones de correo electrónico y SMS válidas para el envío de mensajes de texto para los contactos que recibirán las notificaciones.

- Para editar la información de su cuenta de partner, consulte **Actualización de la información de su cuenta de partner de OnPlus, en la página 46**.
- Para crear o editar contactos de entrega, consulte **Cómo agregar y administrar contactos de entrega, en la página 104**.

Para agregar monitores de dispositivos, consulte **Cómo agregar y administrar monitores de dispositivos, en la página 112**.

Los siguientes temas proporcionan información importante acerca de los procedimientos de creación y administración de reglas de entrega:

- **Directrices importantes para el uso de reglas de entrega, en la página 108**
- **Creación de reglas de entrega, en la página 109**

- Visualización de las reglas de entrega, en la página 110
- Edición de las reglas de entrega, en la página 111
- Eliminación de reglas de entrega, en la página 112
- Cómo habilitar o deshabilitar las notificaciones a direcciones de correo electrónico o SMS, en la página 106

Directrices importantes para el uso de reglas de entrega

Siga las directrices que se incluyen en esta sección al crear reglas de entrega de notificaciones.

- **Antes de crear una regla, consulte el historial de eventos para los monitores de eventos y criterios seleccionados con el fin de estimar el volumen de mensajes que se generarán.**

  Seleccione diferentes niveles de gravedad o seleccione un tipo de evento y consulte el volumen y el historial reciente de las notificaciones que se han generado. De este modo, tendrá una idea del funcionamiento del sistema de eventos y podrá determinar qué monitores de eventos le resultarán más útiles.

  El Historial de eventos, en la parte inferior del diálogo Agregar regla de entrega, incluye el número total de eventos generados que coinciden con los criterios seleccionados. Puede utilizarse para estimar la frecuencia con la que la regla de entrega generará las notificaciones. Si cree que una regla podría generar un gran número de notificaciones en poco tiempo, ajuste los criterios de selección antes de hacer clic en **+ Agregar regla de entrega**.

- **Cree reglas de entrega específicas para limitar el volumen de notificaciones que se generan**. Seleccione niveles de gravedad más estrictos o seleccione un tipo de evento específico para limitar el número y reducir el volumen de notificaciones que se generarán. Por ejemplo, si selecciona Todos los clientes y Todos los niveles de gravedad, se generará un gran número de notificaciones.

- **Compruebe la dirección de correo electrónico de contacto del cliente**. Al recopilar información de contacto de sus clientes, asegúrese de que las direcciones de correo electrónico y SMS del cliente que se utilizarán para las notificaciones son de proveedores de servicios válidos, no incluidos en ninguna lista de proveedores prohibidos.

- **Limite el volumen de notificaciones a direcciones de correo electrónico SMS (teléfonos)**. Si el proveedor de gateway SMS limita el número de

mensajes SMS de entrada o salida de un remitente o aplicación, el servicio de gateway de SMS podría no informar al portal de los intentos de entrega fallidos. **Se aplicarán tarifas del proveedor para los mensajes SMS**, por lo que no deberían utilizarse para las reglas de entrega que generen un gran volumen de notificaciones.

Creación de reglas de entrega

Para crear una regla de entrega, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, seleccione **Notificaciones** > **Reglas de envío**.

PASO 2 Haga clic en **+ Agregar regla de entrega**.

PASO 3 Especifique los criterios de la regla de entrega.

a. **Cliente**. Seleccione **Todo** para que se notifiquen los eventos que coincidan con los criterios seleccionados para todos los clientes o seleccione un **Cliente** determinado.

   Si selecciona **Todo**, los contactos asociados con un cliente específico no se incluirán en el menú desplegable Contacto.

   Si selecciona **Cliente**, el menú desplegable **Contacto** incluirá los contactos asociados con ese cliente y todos los contactos que no estén asociados con un cliente en particular. Un contacto estará asociado con un cliente si especifica el cliente al crear el contacto de entrega.

b. **Nivel de gravedad** o **Tipo de evento**.

   Para generar notificaciones basadas en un nivel de gravedad, seleccione **Todo** o seleccione un nivel de gravedad de la lista.

   IMPORTANTE Los niveles de gravedad son acumulativos, es decir, al seleccionar un nivel de gravedad, se incluyen todos los eventos que tengan ese nivel de gravedad o superior. Por ejemplo, si selecciona Error como nivel de gravedad, se enviarán las notificaciones para eventos con los niveles Error, Crítico, Alerta y Emergencia.

   Para enviar notificaciones basadas en un solo tipo de evento, haga clic en la casilla de verificación **Especificar evento** y seleccione un tipo de evento de la lista desplegable. Consulte **Tipos de eventos, en la página 125**.

c. **Contacto**. Seleccione un contacto de entrega de la lista. Si no se muestra ningún contacto, deberá agregar al menos un contacto de entrega antes de continuar. Consulte **Cómo agregar y administrar contactos de entrega, en la página 104**.

d. **Método**. Seleccione un método de entrega de la lista. Debe seleccionar un contacto antes de establecer el método de entrega.

   Los métodos de entrega que se incluyen en la lista son las direcciones de correo electrónico o SMS que se han definido para este contacto. Los métodos de entrega que se han deshabilitado aparecen en la lista, pero al crear la regla, el campo Contacto indicará que la dirección está actualmente deshabilitada.

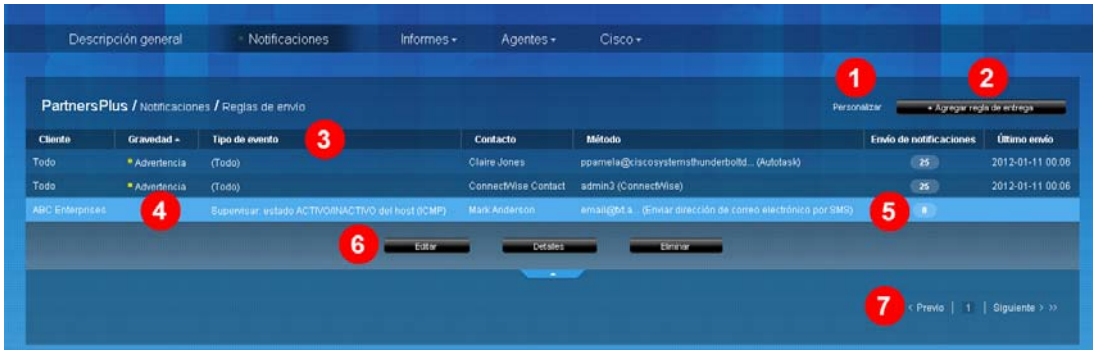
PASO 4 Consulte el **Historial de eventos** para ver cuántos eventos se han generado en las últimas dos semanas con los criterios seleccionados. El historial de eventos se actualiza al seleccionar otros clientes y cambiar el nivel de gravedad o el tipo de evento.

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

PASO 6 Para comprobar que se ha creado la regla, seleccione **Notificaciones** > **Reglas de envío** en el menú de navegación. La nueva regla debería mostrarse en la lista.

Visualización de las reglas de entrega

Para ver una lista de reglas de entrega, acceder a los detalles y las acciones de una regla determinada o ver los detalles de los mensajes de notificación, vaya a la página Descripción general y seleccione **Notificaciones** > **Reglas de envío**.



Número	Descripción
1	Mueva el ratón sobre el enlace Personalizar para especificar el número de reglas que se mostrarán en cada página.
2	Haga clic para agregar una nueva regla de entrega.
3	Haga clic en el encabezado de cualquier columna para ordenar la lista de forma ascendente o descendente.
4	Haga clic en una entrada de la lista para seleccionarla y abrir el cuadro de acciones. Si aparece la palabra DESHABILITADO en el campo Método, significa que se ha deshabilitado la entrega de notificaciones a esa dirección de correo electrónico o SMS.
5	Haga clic en el recuento de notificaciones enviadas para ver los detalles de los mensajes de notificaciones que se han enviado conforme a esa regla.
6	El cuadro de acciones incluye opciones de edición, visualización de detalles y eliminación de la regla.
7	Utilice los controles para desplazarse por la lista si es larga.

Para ver los mensajes de notificación que se han enviado para una regla, haga clic en el número de **Envío de notificaciones**. Haga clic en **Atrás** para volver a la lista de reglas de entrega.

Para ver los detalles de una regla de entrega, haga clic en la regla de la lista para abrir el cuadro de acciones y, a continuación, haga clic en **Detalles**.

Edición de las reglas de entrega

Para editar una regla de entrega, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, seleccione **Notificaciones** > **Reglas de envío**.

PASO 2 Haga clic en la regla de entrega que desee editar.

PASO 3 Haga clic en **Editar** y realice los cambios deseados.

PASO 4 Haga clic en **Guardar**.

Eliminación de reglas de entrega

Para eliminar una regla de entrega, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, seleccione **Notificaciones** > **Reglas de envío**.

PASO 2 Haga clic en la regla de entrega que desee eliminar.

PASO 3 Haga clic en **Eliminar**.

PASO 4 Haga clic en **Aceptar** para confirmar la eliminación.

Cómo agregar y administrar monitores de dispositivos

Cuando se agregan monitores a un dispositivo y se habilitan, se generan eventos en función de los criterios especificados para los monitores. Estos eventos pueden verse en la lista Eventos correspondiente a ese dispositivo.

IMPORTANTE Si desea enviar notificaciones de eventos de monitores de dispositivos a otros destinatarios que no sean los predeterminados, deberá agregar contactos y reglas de entrega adicionales. Consulte las secciones **Contacto y regla de entrega predeterminados, en la página 104** y **Uso de las reglas de entrega, en la página 107**.

Consulte **Ejemplo paso a paso, en la página 101** para ver un sencillo ejemplo y algunos pasos que muestran en qué consiste esta función.

Esta sección cubre los siguientes temas:

- **Monitores de OnPlus Network Agent predeterminados.**
- **Cómo agregar y habilitar monitores de dispositivos**
- **Prueba de monitoreo de dispositivos**
- **Cómo habilitar y deshabilitar (poner en pausa) un monitor de dispositivos o todos los monitores**
- **Eliminación de un monitor de un dispositivo**
- **Descripción de los monitores de dispositivos, en la página 116**

Monitores de OnPlus Network Agent predeterminados.

Al activar el dispositivo OnPlus Network Agent de un cliente, se crea y habilita en el dispositivo un conjunto de monitores de red. A continuación se incluyen los monitores predeterminados:

- rendimiento de red WAN
- Carga de CPU
- Eliminación de direcciones IP duplicadas
- Disponibilidad del servicio de DHCP
- Disponibilidad del servicio de DNS
- Uso de la memoria

El monitor de rendimiento de red WAN también está habilitado en el dispositivo que proporciona la conexión WAN. No puede editar ni eliminar los monitores de dispositivos predeterminados en OnPlus Network Agent, pero sí puede deshabilitarlos. Para obtener más información, consulte **Uso de las reglas de entrega, en la página 107**.

Cómo agregar y habilitar monitores de dispositivos

Para habilitar monitores en un dispositivo, siga estos pasos.

PASO 1 Utilice uno de los métodos siguientes para abrir la ventana Dispositivo del dispositivo al que desee agregar monitores:

- Desde la vista Topología de red, mueva el ratón sobre el icono de un dispositivo y, a continuación, haga clic en el icono (Información de dispositivo).
- En la página Lista de dispositivos, haga clic en la casilla de verificación para seleccionar el dispositivo y haga clic en el icono en la barra de herramientas del panel.

También puede seleccionar varios dispositivos y agregarles el mismo conjunto de monitores. Al agregar monitores a varios dispositivos, todos los monitores previos de los dispositivos seleccionados se eliminarán y se sustituirán por los nuevos.

PASO 2 Seleccione la ficha **Monitores**.

PASO 3 Haga clic en el icono (+) en la esquina superior izquierda de la ventana para mostrar una lista de monitores de dispositivos y seleccionar uno.

PASO 4 Incluya los parámetros necesarios para el tipo de evento seleccionado.

Para algunos tipos de monitores, por ejemplo, Rendimiento del host (ICMP), puede establecer umbrales que se apliquen al generar eventos con nivel Advertencia y Crítico. Consulte **Descripción de los monitores de dispositivos, en la página 116**.

Haga clic en el icono para mostrar información acerca del monitor seleccionado en ese momento.

Consulte **Descripción de los monitores de dispositivos, en la página 116**.

En el ejemplo anterior, el criterio de evento Rendimiento del host (ICPM) especifica lo siguiente:

- Si la latencia es superior a 250 ms, se genera un evento con nivel Advertencia. Si la latencia es superior a 400 ms, se genera un evento con nivel Crítico.
- Si la pérdida de paquetes es superior al 5 %, se genera un evento con nivel Advertencia. Si la pérdida de paquetes es superior al 10 %, se genera un evento con nivel Crítico.
- También se genera un evento si el monitor de rendimiento del host detecta que la latencia o la pérdida de paquetes vuelve a tener niveles aceptables después de un evento con nivel Advertencia o Crítico.

IMPORTANTE Cuando se supervisa un dispositivo, siempre se generan eventos. Pueden verse los eventos en la ficha Eventos de la ventana Información de dispositivo o en el menú Eventos del panel. No se crean ni envían notificaciones para ninguno de los eventos a menos que se hayan creado reglas de entrega con el nivel de gravedad o el tipo de evento adecuado y se hayan habilitado las direcciones de correo electrónico o SMS de los contactos de entrega. Consulte **Uso de las reglas de entrega, en la página 107**.

PASO 5 Repita los pasos anteriores para agregar más monitores a los dispositivos seleccionados.

PASO 6 Haga clic en **Aceptar**.

Al volver a la vista Topología de red, el dispositivo que haya habilitado para la supervisión muestra ahora un distintivo de monitor .

Prueba de monitoreo de dispositivos

Para probar un monitor de dispositivos y generar de forma opcional un evento para el resultado de la prueba, siga estos pasos.

PASO 1 En la ficha Monitores de la ventana Dispositivo, haga clic en el icono Probar monitor para el monitor en cuestión.

PASO 2 Opcionalmente, habilite la opción de generar un evento basado en los resultados de la prueba.

PASO 3 Haga clic en **Ejecutar**. Se muestran los resultados de la prueba.

PASO 4 Haga clic en el icono para ir a la página anterior.

Cómo habilitar y deshabilitar (poner en pausa) un monitor de dispositivos o todos los monitores

Para habilitar o deshabilitar temporalmente un monitor en particular o todos los monitores de un dispositivo, pero mantener su configuración, siga estos pasos.

PASO 1 En la ventana Dispositivo, seleccione la ficha **Monitores**.

PASO 2 Haga clic en un monitor para seleccionarlo y mostrar los ajustes actuales.

PASO 3 Para habilitar o deshabilitar temporalmente un monitor, haga clic en el control **Habilitar/Deshabilitar** asociado con el monitor.

PASO 4 Repita los pasos anteriores para cada monitor del dispositivo que desee habilitar o deshabilitar.

PASO 5 Para habilitar o deshabilitar todos los monitores de un dispositivo, haga clic en **Habilitar todo** o en **Deshabilitar todo**.

PASO 6 Haga clic en **Aceptar**.

Eliminación de un monitor de un dispositivo

Para eliminar un monitor de un dispositivo, siga estos pasos.

PASO 1 En la ventana Dispositivo, seleccione la ficha **Monitores**.

PASO 2 Haga clic en un monitor para seleccionarlo y mostrar los ajustes actuales.

PASO 3 Para eliminar el monitor, haga clic en el icono (-) en la esquina superior izquierda de la ventana.

PASO 4 Haga clic en **Aceptar**.

Descripción de los monitores de dispositivos

Los siguientes monitores de dispositivos pueden configurarse en la ficha Monitores de la ventana Dispositivos.

Monitor de dispositivos	Dispositivos	Descripción
Carga de CPU	Solo OnPlus Network Agent	Supervisa la carga de CPU en OnPlus Network Agent. Se genera un evento con nivel Advertencia si la carga de CPU sobrepasa los umbrales prestablecidos. Está pensado principalmente para uso interno de Cisco.
Servidor DHCP	Dispositivos aplicables	Supervisa el servicio de DHCP para garantizar que esté disponible y esté sirviendo direcciones a los dispositivos en la red. Cuando se agrega este monitor a un dispositivo distinto a OnPlus Network Agent, solo se consideran como servidores DHCP autorizados para la red aquellos dispositivos que tengan un monitor DHCP. Se genera un evento con nivel Crítico si no hay respuesta de ningún servidor DHCP a un paquete de solicitud de DHCP en el tiempo especificado. Se genera un evento de detección de servidores DHCP no autenticados si un servidor DHCP no especificado o que nunca antes se ha visto empieza a responder a solicitudes de DHCP en la red.

Monitor de dispositivos	Dispositivos	Descripción
Servicio de DNS	Dispositivos aplicables	Supervisa el servicio de DNS en este dispositivo para garantizar que esté respondiendo y que sea capaz de resolver consultas relativas al nombre de host de DNS de destino especificado. Se genera un evento con nivel Advertencia o Crítico si la cantidad de memoria libre cae por debajo de los umbrales especificados. Uno de los síntomas de respuesta lenta del servidor DNS es una navegación por Internet torpe.
IP duplicada	Solo OnPlus Network Agent	Supervisa los dispositivos para detectar direcciones IP duplicadas. Se genera un evento de dirección IP duplicada cuando más de un dispositivo reclama la misma dirección en la red.
Rendimiento del host (ICMP)	Cualquier dispositivo aplicable, excepto OnPlus Network Agent	Supervisa la capacidad de acceso al host y el tiempo de respuesta midiendo el rendimiento de latencia y la pérdida de paquetes del host especificado mediante una solicitud de eco ICMP IPv4. Se genera un evento con nivel Advertencia o Crítico si el tiempo de respuesta del host cae por debajo de los umbrales de pérdida de paquetes y latencia especificados. Se genera un evento con nivel Crítico si el host no responde en absoluto.
Estado del host	Cualquier dispositivo aplicable, excepto OnPlus Network Agent	Supervisa la capacidad de acceso al host mediante una solicitud de eco ICMP IPv4. Se genera un evento con nivel Crítico si no se puede acceder al host. Se genera un evento con nivel de Advertencia si más tarde se consigue acceder al host. Utilice este monitor para los hosts que no necesiten mediciones de rendimiento de pérdida y latencia.
Servicio de correo entrante (IMAP)	Cualquier dispositivo aplicable, excepto OnPlus Network Agent	Supervisa la respuesta del servicio de correo IMAP para el puerto especificado en este dispositivo. Se genera un evento con nivel Advertencia o Crítico si el tiempo de respuesta del servicio cae por debajo de los umbrales de latencia especificados. Se genera un evento con nivel Crítico si el host deja de responder por completo a las conexiones IMAP.

Monitor de dispositivos	Dispositivos	Descripción
Servicio de correo entrante (POP3)	Cualquier dispositivo aplicable, excepto OnPlus Network Agent	Supervisa la respuesta del servicio de correo POP3 para el puerto especificado en este dispositivo. Se genera un evento con nivel Advertencia o Crítico si el tiempo de respuesta del servicio cae por debajo de los umbrales de latencia especificados. Se genera un evento con nivel Crítico si el host deja de responder por completo a las conexiones POP3.
Interfaz de gestión de plataforma inteligente (IPMI)	Cualquier dispositivo aplicable, excepto OnPlus Network Agent	Supervisa los sensores IPMI en este dispositivo. Se genera un evento con nivel Advertencia o Crítico si la lectura de alguno de los sensores cae fuera de los umbrales de sensor prestablecidos del dispositivo, dependiendo de qué umbral se cruce. Se genera un evento con nivel Advertencia si el host deja de responder por completo a las conexiones IPMI. Normalmente, IPMI está disponible en los controladores de administración de la placa base (BMC) de servidores como Cisco Unified Computing System (UCS). OnPlus comprueba los sensores IPMI que tienen umbrales definidos, como tensión, temperatura y RPM del ventilador.
Cambio de IP	Cualquier dispositivo aplicable, excepto OnPlus Network Agent	Supervisa la dirección IP de este host para detectar cambios. Se genera un evento con nivel Crítico cuando la dirección IP cambia en este host.
Uso de la memoria	Solo OnPlus Network Agent	Supervisa la carga de CPU en OnPlus Network Agent. Se genera un evento con nivel Advertencia si el uso de la memoria del dispositivo OnPlus Network Agent sobrepasa los umbrales prestablecidos.
Servicio de correo saliente (SMTP)	Cualquier dispositivo aplicable, excepto OnPlus Network Agent	Supervisa la respuesta del servicio de correo SMTP para el puerto especificado en este dispositivo. Se genera un evento con nivel Advertencia o Crítico si el tiempo de respuesta del servicio SMTP cae por debajo de los umbrales de latencia especificados. Se genera un evento con nivel Crítico si el host deja de responder por completo a las conexiones SMTP.

Monitor de dispositivos	Dispositivos	Descripción
Monitor de servidor web seguro	Cualquier dispositivo aplicable, excepto OnPlus Network Agent	Supervisa el servicio web seguro en la URL especificada para asegurarse de que esté respondiendo y de que devuelva la cadena de texto especificada. Se genera un evento con nivel Crítico si no se puede acceder al servicio en la URL especificada, o si la respuesta no contiene la cadena de texto especificada.
Certificado SSL (HTTPS)	Cualquier dispositivo aplicable, excepto OnPlus Network Agent	Supervisa el certificado SSL del servidor web en el host especificado para garantizar su validez y vigencia. Se genera un evento con nivel Advertencia si el certificado caduca en un tiempo inferior al número de días especificado. Se genera un evento con nivel Crítico si no se puede obtener un certificado válido del host, o si el certificado ha caducado.
Servicio de TCP	Cualquier dispositivo aplicable, excepto OnPlus Network Agent	Supervisa el servicio de TCP en el puerto especificado para asegurarse de que responde. Puede especificar una cadena de texto que enviar al puerto TCP y una cadena de texto de devolución esperada. Estas dos cadenas de texto son opcionales e independientes una de la otra. Las cadenas de texto pueden contener las secuencias de escape de salto de línea (\\n), línea nueva (\r) y tabulador (\t). Se genera un evento con nivel Crítico si el puerto TCP de destino no está abierto, o si no se devuelve la cadena de texto esperada opcional.
Servicio de UDP	Cualquier dispositivo aplicable, excepto OnPlus Network Agent	Supervisa el servicio de UDP en el puerto especificado para asegurarse de que responde. Debe especificar una cadena de texto que enviar al puerto UDP y una cadena de texto de devolución esperada. Ambas cadenas de texto son necesarias. Las cadenas de texto pueden contener las secuencias de escape de salto de línea (\\n), línea nueva (\r) y tabulador (\t). Se genera un evento con nivel Crítico cuando no se devuelve la cadena de texto esperada del servicio de UDP.

Monitor de dispositivos	Dispositivos	Descripción
Rendimiento de red WAN	OnPlus Network Agent y el dispositivo raíz de la red del cliente	Supervisa la latencia, la pérdida de paquetes y la oscilación de la red. Supervisar el rendimiento de la red WAN de este sitio mediante la medición de la oscilación, la latencia y la pérdida de paquetes frente a un servicio de retransmisor del portal. Se genera un evento con nivel Advertencia o Crítico si el rendimiento de red WAN cae por debajo de los umbrales especificados. Se genera un evento con nivel Crítico si no hay respuesta desde el servicio de retransmisor del portal. **NOTA** Solo se muestra una instancia de este monitor tanto en OnPlus Network Agent como en el dispositivo que proporciona el enlace WAN para la red del cliente. Si edita los umbrales de supervisión de rendimiento de red WAN en alguno de estos dispositivos, los cambios solo aparecen cuando el monitor se visualiza en el otro dispositivo.
Servicio web	Cualquier dispositivo aplicable, excepto OnPlus Network Agent	Supervisa el servicio web (HTTP) en la URL especificada para asegurarse de que esté respondiendo y de que devuelva la cadena de texto especificada. Se genera un evento con nivel Crítico si no se puede acceder al servicio en la URL especificada, o si la respuesta no contiene la cadena de texto especificada.

Monitor de dispositivos	Dispositivos	Descripción
Interfaz de administración de Windows (WMI)	Host Windows con el servicio WMI habilitado	Supervisa el estado y los umbrales de rendimiento en un host Windows con WMI. El servicio WMI debe estar habilitado en el host de destino y deben proporcionarse credenciales válidas en la ficha Acceso de la ventana Dispositivo del dispositivo en cuestión. Pueden generarse los siguientes eventos, en función del tipo de monitor de WMI: ▪ **Estado de unidad de disco**: se genera un evento de advertencia o crítico si una unidad de disco en el host entra en uno de los estados especificados. Se recomienda usar habitualmente los estados predeterminados proporcionados. ▪ **Espacio libre en disco**: se genera un evento de advertencia o crítico si la cantidad de espacio libre en el disco en el volumen especificado cae por debajo de los umbrales especificados. ▪ **Memoria libre**: se genera un evento de advertencia o crítico si la cantidad de memoria libre cae por debajo de los umbrales especificados. ▪ **Existe el proceso**: se genera un evento crítico si el nombre del proceso especificado no aparece en la lista de tareas que se están en ejecutando en el host Windows.

Visualización de eventos

Pueden generar eventos:

- Los monitores de dispositivos, entre los que se incluyen:
  - Umbrales de ancho de banda y conectividad de red superados
  - Cambios del estado del host
  - Error o retardo de resolución de nombre de host de DNS
  - Cambios de dirección IP
  - Detección de dispositivos

- Acciones del tipo:
  - Inicios de sesión de agentes autorizados
  - Actualizaciones de firmware
  - Operaciones de copia de seguridad y restauración de la configuración
  - Solicitudes de reinicio de dispositivo
  - Creación y envío de informes
  - Eventos de soporte de productos de Cisco
- Eventos específicos de la aplicación
- Servicios que se ejecutan en el portal

Puede ver y filtrar eventos para un solo cliente o para un dispositivo específico.

Para obtener más información, consulte estas secciones:

- **Visualización de eventos para todos los clientes, en la página 122**
- **Visualización de los eventos de un cliente, en la página 123**
- **Visualización del historial de eventos de un dispositivo, en la página 124**
- **Tipos de eventos, en la página 125**

Visualización de eventos para todos los clientes

Para ver los eventos de todos los clientes, siga estos pasos.

PASO 1 En la página de información general de la cuenta de partner, seleccione **Notificaciones** > **Eventos**.

La página Notificaciones/Eventos incluye los eventos de todos los clientes. Para cada evento, se incluye el cliente, la fecha, la gravedad, el tipo, el mensaje y la dirección MAC del dispositivo (si procede). Haga clic en los encabezados de las columnas para ordenar la lista por cliente, fecha, gravedad o tipo.

PASO 2 Si lo desea, seleccione un nivel de gravedad del evento para ver todos los eventos de ese nivel de gravedad o superior para todos los clientes.

PASO 3 Si lo desea, haga clic en un enlace de dirección MAC en la columna Dispositivo para abrir la ventana Información de dispositivo de ese dispositivo.

PASO 4 Haga clic en **Actualizar** para actualizar la lista.

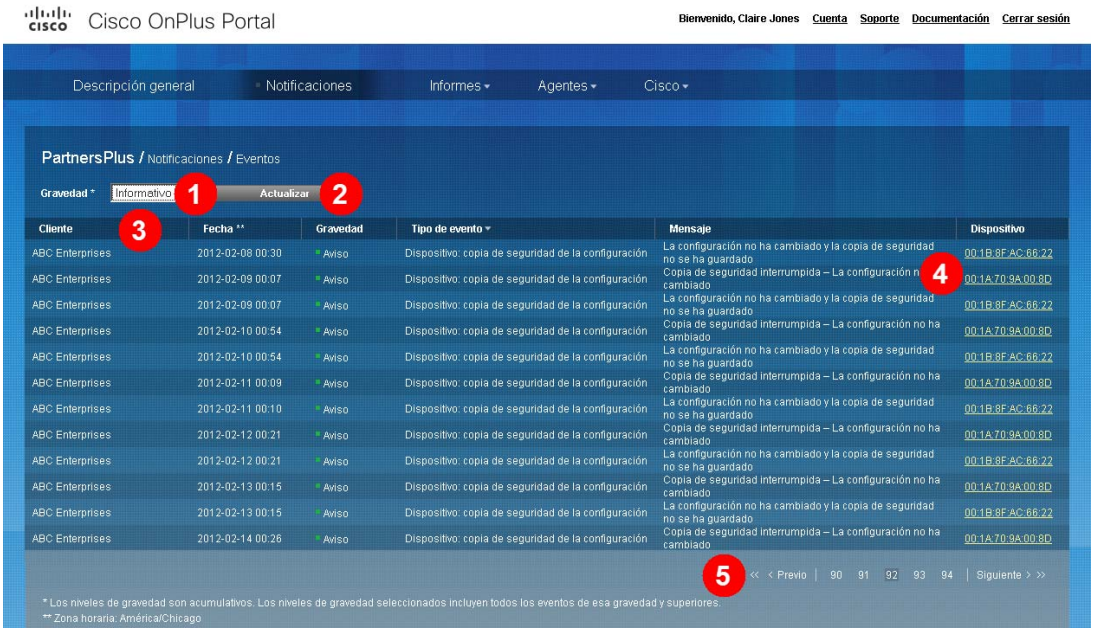
Visualización de los eventos de un cliente

Para ver los eventos de un cliente, siga estos pasos.

PASO 1 En la página Descripción general, haga clic en la entrada del cliente para acceder a su panel.

PASO 2 En el menú de navegación, seleccione **Eventos**.

A continuación puede ver un ejemplo de lista de eventos que muestra las funciones y áreas de interés de la página Eventos del cliente.



Número	Descripción
1	Seleccione una de las opciones de la lista desplegable Gravedad para filtrar la lista de eventos por su gravedad. Los niveles de gravedad son acumulativos. Los niveles de gravedad seleccionados muestran todos los eventos de esa gravedad y superiores.
2	Actualice manualmente la lista Eventos. La lista también se actualiza cuando vuelve a entrar en la página.
3	Haga clic en los encabezados de las columnas para ordenar los eventos por fecha, gravedad o tipo de evento.

Número	Descripción
4	Se muestran mensajes que proporcionan información adicional sobre el evento.
5	Las direcciones MAC de la lista Eventos son enlaces en los que se puede hacer clic. Haga clic en una dirección MAC para ver los detalles del panel del dispositivo con esa dirección.
6	Utilice los controles de la parte inferior de la página para desplazarse por la lista.

Visualización del historial de eventos de un dispositivo

Para ver el historial de eventos de un determinado dispositivo del cliente, siga estos pasos.

PASO 1 En la página Descripción general, haga clic en un cliente de la lista para ver su panel.

PASO 2 Para abrir la ventana Dispositivo de un dispositivo del cliente específico, utilice uno de estos métodos:

- Desde la vista Topología de red, mueva el ratón sobre el icono de un dispositivo y, a continuación, haga clic en el icono . También puede hacer clic con el botón derecho del ratón sobre el icono y seleccionar **Ver información del dispositivo**.
- En la vista Lista de dispositivos, haga clic en la casilla de verificación que se encuentra a la izquierda de la entrada para seleccionarla y mostrar el icono a la derecha de la barra de herramientas. Haga clic en el icono .

  Aparece la ventana Información de dispositivo.

PASO 3 En la ventana Dispositivo, seleccione la ficha **Eventos**. También puede seleccionar filtrar los eventos del dispositivo por gravedad y hacer clic en los encabezados de las columnas para ordenar la lista.

Tipos de eventos

Esta tabla incluye y describe los Tipos de eventos que pueden ocurrir en el portal.

Categoría	Descripción
Aplicación	Aplicación: evento.
Contacto	Mensaje enviado a contacto de destino.
Sitio del cliente	Sitio del cliente: desactivado.
Sitio del cliente	Sitio del cliente: instalación completada.
Dispositivo	Dispositivo: paquete de autoridad de certificación cargado.
Dispositivo	Dispositivo: se ha usado el acceso al soporte de Cisco.
Dispositivo	Dispositivo: copia de seguridad de la configuración
Dispositivo	Dispositivo: copia de seguridad de configuración solicitada.
Dispositivo	Dispositivo: cambio de configuración.
Dispositivo	Dispositivo: restauración de configuración solicitada.
Dispositivo	Dispositivo: configuración restaurada.
Dispositivo	Dispositivo: se ha completado la actualización del firmware.
Dispositivo	Dispositivo: actualización de firmware solicitada.
Dispositivo	Dispositivo: actualización de firmware.
Dispositivo	Dispositivo: nuevo firmware disponible.
Dispositivo	Dispositivo: sin conexión. Un dispositivo supervisado local ya no responde en la red.
Dispositivo	Dispositivo: solicitud de reinicio.
Dispositivo	Dispositivo: estado de conexión de túnel remota (RDP, VNC, TCP). El servidor ha establecido una conexión de túnel remota de puerto RDP, VNC o TCP a un dispositivo o ha cerrado la conexión.
Detección de dispositivos	Descubrimiento: cambio en la detección de dispositivos.
Detección de dispositivos	Descubrimiento: publicación inicial de información de detección de dispositivos.

Categoría	Descripción
Detección de dispositivos	Descubrimiento: nuevo dispositivo. Este evento se genera cuando aparece un nuevo dispositivo en el sitio. Tanto este evento como la detección: la publicación inicial del evento de detección se restablece al ejecutar Restablecer todo. Tras realizar la acción Restablecer todo, la siguiente detección de dispositivos generará un evento Detección: publicación inicial de detección, y cada dispositivo encontrado posteriormente generará un evento Detección: nuevo dispositivo.
Supervisar	Supervisar: conectividad del dispositivo (Ping). Se han superado los umbrales de latencia (ms) y pérdida de paquetes (%) para la supervisión de la conectividad del dispositivo (ICMP).
Supervisar	Supervisar: problemas en hardware de dispositivo.
Supervisar	Supervisar: la dirección IP de dispositivo ha cambiado. La dirección IP de un dispositivo ha cambiado. La comprobación tiene lugar cada vez que se ejecuta la detección de dispositivos. Si este es el dispositivo que proporciona la conexión WAN, también se envía un evento si cambia la dirección IP de WAN.
Supervisar	Supervisar: creación de servidor de DHCP.
Supervisar	Supervisar: resolución de nombre de host de DNS. Se ha detectado recuperación, error o retardo en la resolución de nombre de host de DNS.
Supervisar	Supervisar: estado del host. Eventos de host inactivo (no accesible) o de host activo (recuperación).
Supervisar	Supervisar: tráfico HTTP/servidor web. Eventos asociados con un puerto de servidor web supervisado. Puede especificar el puerto HTTP (el 80 es el predeterminado), el nombre de la página web y el texto para comprobar que el servidor web está activo y funciona correctamente.
Supervisar	Supervisar: tráfico HTTPS/servidor web seguro. Eventos asociados con un monitor de servidor web seguro. Puede especificar el puerto HTTPS (el 443 es el predeterminado), la URL de la página web y el texto que se comprobará para asegurar que el servidor web está activo y funciona correctamente.
Supervisar	Supervisar: servidor de correo entrante IMAP. Eventos asociados con un servidor de correo entrante IMAP seguro.
Supervisar	Supervisar: Interfaz de gestión de plataforma inteligente (IPMI) Eventos asociados con un dispositivo supervisado compatible con IPMI.

Categoría	Descripción
Supervisar	Supervisar: duplicación de dirección IP. Cuando se detecta una IP duplicada en la red, se genera un evento Supervisar: dirección IP duplicada. Al resolver un problema de IP duplicada, se genera un segundo evento Supervisar: dirección IP duplicada para indicar la recuperación.
Supervisar	Supervisar: Ancho de banda de la red (latencia, pérdida de paquetes, oscilación). Umbrales de latencia, pérdida de paquetes y oscilación de red superados o evento de recuperación asociado con estos umbrales.
Supervisar	Supervisar: carga de CPU de OnPlus. El monitor de carga de CPU de OnPlus Network Agent genera estos eventos cuando se superan los umbrales de uso de CPU o vuelven a niveles normales posteriormente. Está pensado principalmente para uso interno de Cisco.
Supervisar	Supervisar: uso de la memoria de OnPlus Network Agent. Supervisa el uso de la memoria en OnPlus Network Agent. Este monitor siempre está habilitado. Está pensado principalmente para uso interno de Cisco.
Supervisar	Supervisar: servidor de correo entrante POP3. Eventos asociados con un servidor de correo entrante POP3 seguro.
Supervisar	Supervisar: detección de servidores DHCP no autenticados.
Supervisar	Supervisar: servidor de correo saliente SMTP. Eventos asociados con un monitor de puerto de servidor de correo saliente SMTP.
Supervisar	Supervisar: certificado SSL.
Supervisar	Supervisar: tráfico TCP. Estos eventos están asociados con un servicio de TCP supervisado en el puerto especificado.
Supervisar	Supervisar: tráfico UDP. Estos eventos están asociados con un servicio de UDP supervisado en el puerto especificado.
Supervisar	Supervisar: información de administración de Windows (WMI)

Categoría	Descripción
OnPlus	OnPlus: estado de la conexión. Este monitor de estado de la conexión de OnPlus Network Agent informa del estado de OnPlus Network Agent. Los eventos de Site Comms activo/inactivo se generan con un nivel de gravedad de Aviso para acciones normales de funcionamiento activo/inactivo, como un reinicio solicitado por el usuario de OnPlus Agent o una actualización automática de firmware en OnPlus Network Agent en el período de mantenimiento diario. Si se produce un fallo inesperado en la conexión, los eventos de Site Comms activo/inactivo correspondientes se generan con un nivel de gravedad de Advertencia.
OnPlus	OnPlus: error E/S. Un error E/S ocurrido durante el inicio de sesión puede indicar que el sistema de archivos de OnPlus Network Agent está lleno o corrupto.
OnPlus	OnPlus: conexión de portal a OnPlus Network Agent.
OnPlus	OnPlus: el proceso ha terminado de forma inesperada. Un proceso ha terminado de forma inesperada en el dispositivo OnPlus.
OnPlus	OnPlus: estado de la conexión de túnel remoto. Túnel remoto establecido por el servidor a OnPlus Network Agent.
OnPlus	OnPlus: es posible que se bloquee el puerto TCP 11300 (multidifusión). La conectividad del sitio puede ser limitada. Este evento se genera si CPE puede generar la detección hacia el portal, pero el latido no está conectado en ese momento. Esto normalmente significa que el sitio tiene políticas de salida restrictivas que impiden el tráfico de salida en el puerto 11300. Consulte **Requisitos de acceso a puertos y protocolos, en la página 23**.
Producto	Producto: alerta de Cisco Security (PSIRT)
Producto	Producto: alerta de contrato de servicios de Cisco
Producto	Producto: avisos de final de la venta, del ciclo de vida y de soporte.
Producto	Producto: aviso de final de la venta, del ciclo de vida y de soporte
Producto	Producto: alerta de final de garantía
Producto	Producto: alerta de final de garantía.
Producto	Producto: alerta de seguridad (PSIRT).
Informe	Informes: creación completada.

Categoría	Descripción
Informe	Informes: creación solicitada.
Informe	Informes: informe enviado. Los eventos de envío de informes solo se generan para informes periódicos programados con al menos un correo electrónico de contacto especificado para el destinatario. Si no se especifica un destinatario, se genera un evento de informe finalizado en su lugar.

8

Conexión a dispositivos desde el portal

En este capítulo se explica cómo establecer conexiones remotas a dispositivos del sitio del cliente desde Cisco OnPlus Portal. Se tratan los siguientes temas:

- **Descripción general**
- **Directrices, limitaciones y advertencias para conexiones remotas**
- **Abrir conexiones RDP, VNC o de túnel genérico (SSH, Telnet)**
- **Abrir una conexión web (HTTP/HTTPS)**
- **Cerrar manualmente la conexión a un dispositivo remoto**
- **Habilitar o deshabilitar las conexiones a dispositivos remotos para un sitio**

Descripción general

Utilice la función Conectar con dispositivo para establecer una conexión remota a un dispositivo de las instalaciones del cliente mediante uno de los siguientes tipos de conexión: web (HTTP), web segura (HTTPS), protocolo de escritorio remoto (RDP), cliente de red virtual (VNC) o túnel genérico (por ejemplo, una conexión de puerto Telnet o SHH).

Utilice esta función para administrar de forma remota los dispositivos de sus clientes. La función Conectar con dispositivo le permite:

- Conectar de forma segura con dispositivos remotos que se encuentran en las instalaciones del cliente sin tener que configurar el reenvío de puertos del gateway para acceder a los dispositivos que se encuentran tras el cortafuegos del cliente.
- Iniciar la utilidad de configuración de un dispositivo desde una ubicación remota
- Realice tareas secundarias en el equipo de las instalaciones del cliente, como comprobar el estado del dispositivo o realizar ajustes en su configuración.

El soporte para conexiones remotas a dispositivos de terceros y dispositivos de Cisco que son totalmente compatibles con OnPlus es limitado. Cisco no puede probar y confirmar la funcionalidad de todas las posibles combinaciones de dispositivos de Cisco, protocolos y dispositivos de otros fabricantes.

Directrices, limitaciones y advertencias para conexiones remotas

Lea esta sección para conocer directrices, advertencias y limitaciones importantes relacionadas con las conexiones remotas establecidas a través de OnPlus Portal.

- **Directrices para todos los tipos de conexión, en la página 132**
- **Directrices para conexiones RDP, VNC y de túnel genérico, en la página 133**
- **Directrices de conexión web (HTTP/HTTPS), en la página 133**

Directrices para todos los tipos de conexión

Las siguientes directrices, limitaciones y advertencias se aplican a todas las conexiones remotas establecidas a través de OnPlus Portal:

- OnPlus Network Agent debe estar activo y funcionando normalmente en el sitio.
- Solo puede haber una conexión de túnel de un tipo determinado (web, RDP, VNC o túnel genérico) abierta *por sitio de cliente*. Las nuevas conexiones sustituyen a las anteriores.
- Si la conexión está inactiva durante 20 minutos, se cierra automáticamente.
- Deben estar habilitadas las conexiones remotas en el sitio. Para obtener más información, consulte **Habilitar o deshabilitar las conexiones a dispositivos remotos para un sitio, en la página 144**.
- Para garantizar el correcto funcionamiento del túnel, el equipo y la red que se utilizan para acceder al portal deben permitir las conexiones TCP salientes en los puertos 11305 y 11700 a través de 11800. El tráfico TCP de salida de estos puertos no suele bloquearse, por lo que solo sería un problema en un entorno de red restrictivo.

Directrices para conexiones RDP, VNC y de túnel genérico

Las siguientes directrices, limitaciones y advertencias se aplican a las conexiones RDP, VNC y de túnel genérico establecidas a través de OnPlus Portal:

- Las conexiones de túnel realizadas desde OnPlus Portal están pensadas para las tareas dirigidas por el usuario, como los cambios de configuración remotos o las actividades de depuración. No son adecuadas para operaciones de datos de gran volumen o servicios permanentes, como las copias de seguridad automatizadas.
- La conexión termina tras 10 minutos de inactividad (es decir, si no se ha realizado ningún intento de conexión a través del túnel). Las conexiones de túnel se cierran tras 20 minutos de inactividad.
- Una conexión de túnel a un dispositivo que transmita contenido a través de una segunda conexión utilizando un puerto diferente no funcionará. Si existe alguna posibilidad de desactivar la transmisión a través de la segunda conexión, deberá hacerlo cuando intente realizar una conexión remota.

  La cámara de vídeo IP Cisco PVC2300, que depende de un servicio que utiliza el protocolo de asignación de puertos NAT (NAT-PMP) para transmitir contenido a otra conexión a través de un puerto diferente, es un buen ejemplo de este tipo de dispositivo.

Directrices de conexión web (HTTP/HTTPS)

Las siguientes directrices, limitaciones y advertencias se aplican a las conexiones web remotas (HTTP/HTTPS) establecidas a través de OnPlus Portal:

- No todos los dispositivos admiten la ficha Conectar. Consulte el **apéndice B, “Compatibilidad con funciones y dispositivos de Cisco”.** para saber qué dispositivos de Cisco admiten esta función.
- Se está realizando un esfuerzo razonable para admitir conexiones web a dispositivos de otros fabricantes, pero no se puede garantizar que funcionen correctamente.
- El navegador web debe permitir cookies y ventanas emergentes de OnPlus Portal para poder conectarse de forma remota a un dispositivo a través de HTTP/HTTPS.
- Las conexiones remotas a dispositivos que utilizan correctamente URL relativas en su contenido deberían funcionar.

Sin embargo, los errores en los navegadores web y los servidores, y el contenido incorrecto procedente de los dispositivos pueden ser causa de que algunas funciones y dispositivos no funcionen correctamente (por ejemplo, el dispositivo podría redireccionar a una dirección de LAN local no enrutable). Este tipo de fallos en la conexión remota indica que existen problemas en el propio dispositivo.

Una sencilla manera de averiguar si el fallo se debe a un problema en el dispositivo es utilizar un dispositivo gateway para el reenvío de puertos a través del cortafuegos al dispositivo con un equipo externo. Si esto no funciona, probablemente es el dispositivo el que está causando el problema.

- Diferentes navegadores web o versiones diferentes del mismo navegador web pueden mostrar un comportamiento diferente con el mismo dispositivo.
- Si se está conectando a un dispositivo que transmite contenido a través de una segunda conexión utilizando un puerto diferente, este tipo de conexión remota no funcionará. Si existe alguna posibilidad de desactivar la transmisión a través de la segunda conexión, deberá hacerlo cuando intente realizar una conexión remota.

  La cámara IP Cisco PVC2300 es un ejemplo de este tipo de dispositivo. Al conectarse a Internet Explorer, no utiliza JPEG en movimiento para enviar contenido. En su lugar, utiliza una segunda transmisión con asignación de puertos UPnP. En el caso de la cámara Cisco PVC2300, este problema se resuelve utilizando otro navegador en lugar de Internet Explorer.

Abrir conexiones RDP, VNC o de túnel genérico (SSH, Telnet)

Los temas de esta sección proporcionan información sobre el establecimiento de conexiones de túnel con dispositivos remotos a través del portal:

- **Funcionamiento de las conexiones de túnel en el portal, en la página 134**
- **Creación de conexiones RDP, VNC o de túnel genérico (SSH, Telnet), en la página 136**

Funcionamiento de las conexiones de túnel en el portal

El diagrama que se muestra a continuación ofrece una descripción general de la implementación en el portal de las conexiones RDP, VNC y de túnel genérico.

Como se muestra en el diagrama, una conexión de túnel remota establecida a través de OnPlus Portal incluye tres segmentos:

- El segmento entre el equipo remoto y OnPlus Portal.

  Para conexiones web, este segmento se asegura, ya que se requiere HTTPS para conectarse al portal. En el caso de las conexiones RDP, VNC y de túnel genérico, no se proporciona seguridad adicional.

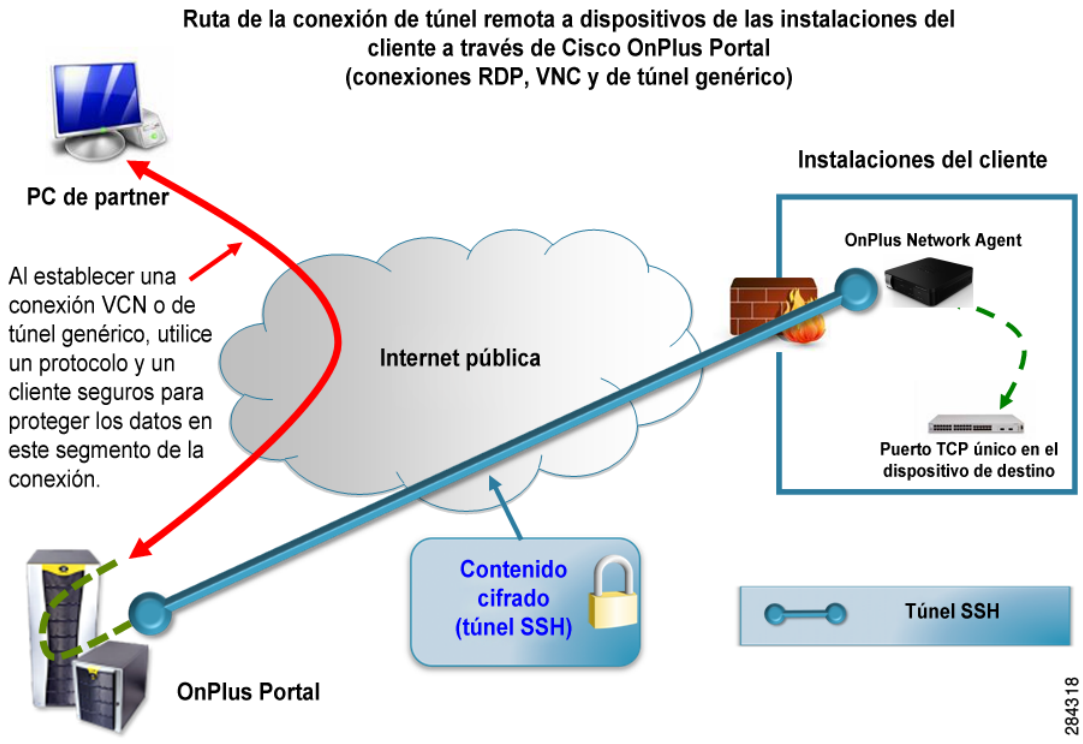
- El segmento entre OnPlus portal y OnPlus Network Agent.

  Este segmento de la conexión se asegura utilizando un túnel SSL.

- El segmento entre OnPlus Network Agent y el dispositivo de destino.

  Este segmento de la conexión se encuentra completamente detrás de cualquier cortafuegos existente en el sitio del cliente. Las conexiones HTTPS están cifradas, pero no así las conexiones HTTP.

NOTA El siguiente diagrama se aplica solo a conexiones RDP, VNC o de túnel genérico. Para las conexiones proxy web, se aplica una conexión HTTPS segura entre el equipo del partner y OnPlus Portal.



Las siguientes notas se aplican a la implementación de conexiones de OnPlus Portal:

- El equipo del partner tiene un único puerto al que conectarse mientras dura la conexión. Una vez establecida la conexión, el túnel se vincula exclusivamente con la dirección IP de origen del equipo del partner. El puerto utilizado en esta conexión se asigna de forma dinámica y no debe marcarse.
- Si el protocolo utilizado para la conexión admite varias conexiones de clientes simultáneamente a un solo puerto TCP en el dispositivo de destino (por ejemplo, Telnet y SSH), se admitirán varias conexiones a través del mismo túnel.
- La conexión de túnel genérico debería admitir cualquier protocolo TCP de un solo puerto.
- Si el dispositivo de destino admite Wake on LAN (WOL), se envían paquetes WOL durante los primeros 10 segundos de la creación inicial del túnel.

  Para obtener más información, consulte la documentación del hardware y el sistema operativo del dispositivo de destino. Debe ser usted quien configure WOL para los dispositivos y resuelva los problemas de WOL que pudieran surgir.

Creación de conexiones RDP, VNC o de túnel genérico (SSH, Telnet)

Para crear una conexión RDP, VNC o de túnel genérico (por ejemplo, para el acceso remoto SSH o Telnet a un dispositivo), siga estos pasos.

PASO 1 Asegúrese de que el dispositivo al que se está conectando está configurado para permitir la conexión:

- Para todas las conexiones de túnel de asignación directa (RDP, VNC o de túnel genérico), el cortafuegos del dispositivo de destino debe estar configurado para permitir el acceso al dispositivo.
- Para conexiones VNC, el servidor VNC del dispositivo de destino y el cliente VNC del equipo que accede al dispositivo deben estar configurados correctamente. Se recomienda el uso de un servidor y un cliente VNC seguros.
- Para conexiones RDP, debe estar habilitado Escritorio remoto compartido en el dispositivo de destino. Para obtener más información, consulte la documentación de Microsoft para RDP.

- Para conexiones de túnel genérico, puede realizarse una conexión a un solo puerto TCP. Debe haber un servicio activo en el puerto en el dispositivo de destino y los cortafuegos deberán permitir las conexiones.

PASO 2 Inicie la conexión mediante uno de estos métodos:

- Para intentar la conexión con la configuración predeterminada, haga clic con el botón derecho en el icono del dispositivo en la vista Topología y seleccione **Conectarse al dispositivo a través de RDP** o **Conectarse al dispositivo a través de VNC**.
- Para configurar los ajustes de conexión, abra la ventana Información de dispositivo desde la vista Topología de red o la vista Lista de dispositivos, seleccione la ficha Conectar, seleccione un tipo de conexión (RDP, VNC o túnel genérico) y configure los ajustes. Haga clic en **Conectar con dispositivo** para realizar la conexión utilizando los ajustes que ha configurado.

  Para conexiones RDP, VNC y de túnel genérico, solo tiene que especificar el número de puerto correcto para el protocolo deseado en el dispositivo de destino.

Si el túnel se crea correctamente, aparece la ventana Conexión, que incluye un enlace a la conexión.

Si está creando una conexión RDP, se le solicitará que guarde o abra el archivo de perfil de conexión .rdp que se utilizará con su aplicación RDP instalada. Del mismo modo, si está creando una conexión VNC en un PC Windows, se le solicitará que guarde o abra el archivo de perfil de conexión .vnc.

Para SSH, Telnet u otros túneles genéricos, puede cortar y pegar la dirección. O bien, puede hacer clic en el icono **Copiar al portapapeles** para copiar la dirección al portapapeles y pegarla en la aplicación de un cliente (por ejemplo, un cliente Telnet o SSH).

El túnel está vinculado exclusivamente a la dirección IP de origen del primer dispositivo que intenta conectarse al túnel.

PASO 3 Haga clic en **Aceptar** para cerrar la ventana Conexión disponible.

Cuando se establece la conexión, aparece el distintivo de conexión remota en el icono del dispositivo, en la vista Topología de red. La ventana Información de dispositivo también indica que el dispositivo está conectado a través de un túnel.

El icono del dispositivo muestra un distintivo de conexión para indicar que el dispositivo está conectado a través de un túnel.

El área de estado de la ventana Información de dispositivo también se actualiza y muestra el mensaje "Conexión de túnel establecida con este dispositivo".

De forma abreviada, puede hacer clic con el botón derecho del ratón en el icono de un dispositivo que admita conexiones remotas desde la vista Topología o la vista Panel del cliente y seleccionar **Conectarse al dispositivo a través de la Web, Conectarse al dispositivo a través de RDP o Conectarse al dispositivo a través de VNC**. Al establecer una conexión de túnel utilizando este método, se utilizan los ajustes configurados en ese momento.

Abrir una conexión web (HTTP/HTTPS)

En las siguientes secciones podrá obtener información sobre cómo abrir una conexión web (HTTP/HTTPS) a un dispositivo remoto a través de OnPlus Portal:

- **Funcionamiento de las conexiones web remotas**
- **Configurar y abrir una conexión web, en la página 140**
- **Solución de problemas de configuración de conexiones web (HTTP/HTTPS), en la página 142**
- **Configuración de conexión web recomendada para dispositivos, en la página 143**

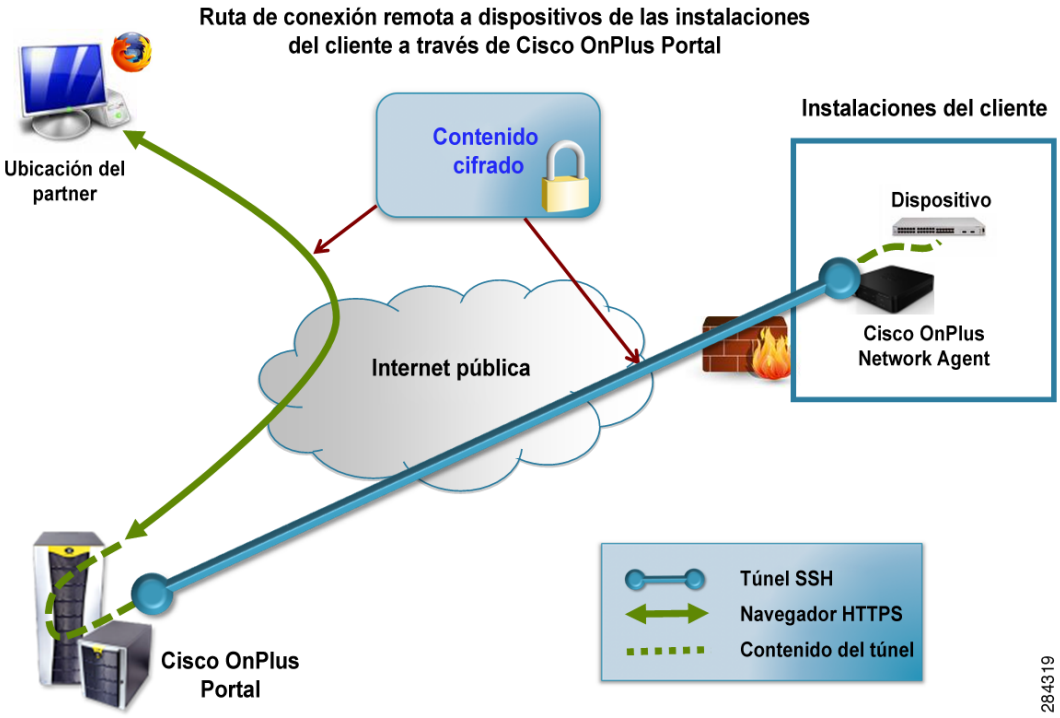
Funcionamiento de las conexiones web remotas

Al realizar una conexión a los dispositivos de las instalaciones del cliente a través de la Web, todo el tráfico público de Internet que pasa a través de OnPlus Portal se cifra, incluso el contenido web no cifrado.

El diagrama que a parece a continuación muestra lo siguiente:

- El tráfico de entrada y salida del navegador web que utiliza para acceder a OnPlus Portal está cifrado y se transmite a través de una conexión HTTPS.
- El tráfico de entrada y salida de OnPlus Portal y OnPlus Network Agent en las instalaciones del cliente está cifrado y se transmite a través de un túnel SSH.
- La última etapa de la conexión al equipo de las instalaciones del cliente en la ubicación remota se lleva a cabo extendiendo el túnel desde OnPlus Network Agent hasta el puerto del dispositivo en las instalaciones del cliente.

  Los ajustes configurados en la ficha Conectar para un dispositivo del portal determinan si la conexión local entre OnPlus Network Agent y el dispositivo está cifrada o no.



Configurar y abrir una conexión web

Para configurar los ajustes de conexión y abrir una conexión a un dispositivo remoto en las instalaciones del cliente desde OnPlus Portal, siga estos pasos.

PASO 1 En la página Descripción general del portal, haga clic en un cliente de la lista y muestre su Topología de red.

PASO 2 Mueva el ratón sobre el icono en la vista Topología del dispositivo al que quiera conectarse y haga clic en el icono de Información de dispositivo.

También puede hacer clic en el icono con el botón derecho del ratón y seleccionar **Ver información del dispositivo**.

PASO 3 En la ventana Información de dispositivo, haga clic en la ficha **Conectar**.

PASO 4 Haga clic en **Web**.

PASO 5 Edite los ajustes de la conexión web según se describe en la siguiente tabla.

Ajuste	Descripción
Puerto Web del dispositivo	Introduzca el número de puerto necesario para las conexiones a este dispositivo. El puerto de administración predeterminado es el 80, que debería ser válido para un gran número de dispositivos. Puede editar este ajuste según sea necesario. Consulte la documentación del dispositivo para saber si se necesita otro puerto o una conexión HTTPS.
Conexión HTTPS segura	Active la opción **Conexión HTTP segura** si el dispositivo requiere una conexión HTTPS (SSL). Si se activa esta opción, el puerto de administración se establece en el 443, que es el predeterminado para las conexiones HTTPS (SSL). Puede editar el número de puerto si fuera necesario. Este ajuste debe utilizarse solo para dispositivos que requieran una conexión HTTPS/SSL segura.
Reparar encabezados	Solo debe habilitar la opción Reparar encabezados en los siguientes casos: ▪ La conexión al dispositivo falla; y ▪ Aparecen direcciones IP privadas (por ejemplo, 192.168.x.x) en el campo de URL del navegador web que se está utilizando para conectarse al dispositivo. Cuando se habilita **Reparar encabezados**, las referencias a direcciones IP privadas se eliminan de los encabezados y se hacen relativas.

Ajuste	Descripción
Reparar URL	Solo debe habilitar la opción Reparar URL en los siguientes casos: ▪ La conexión al dispositivo falla; y ▪ Se ven tiempos de espera de conexión; o ▪ Se carga la página del dispositivo remoto pero los enlaces a otro contenido desde la página no funcionan. Cuando se habilita **Reparar URL**, el direccionamiento absoluto de URL de contenido se sustituye por el direccionamiento relativo.
Deshabilitar comportamiento del proxy	Solo debe habilitar la opción **Deshabilitar comportamiento del proxy** en los siguientes casos: ▪ La conexión al dispositivo falla; o ▪ La página del dispositivo remoto se carga, pero otro contenido de la página, como los applets de Java, no funciona. Cuando está habilitada la opción Deshabilitar comportamiento del proxy, ciertas funciones de proxy web del túnel están deshabilitadas y se establece en su lugar un túnel genérico al Puerto Web del dispositivo. Las opciones Reparar encabezados y Reparar URL se desactivan. El portal recuerda esta configuración, pero no la configuración del túnel genérico.

Para obtener información sobre la configuración recomendada para dispositivos específicos y sugerencias para la solución de problemas, consulte los siguientes temas:

- **Solución de problemas de configuración de conexiones web (HTTP/HTTPS), en la página 142**
- **Configuración de conexión web recomendada para dispositivos**

PASO 6 Haga clic en **Conectar con dispositivo**.

Cuando la conexión está preparada, aparece la ventana Conexión disponible.

PASO 7 En la ventana emergente Conexión disponible, seleccione **Haga clic aquí para conectarse** para abrir la conexión al dispositivo en una nueva ventana del explorador.

Haga clic en **Aceptar** para cerrar la ventana.

PASO 8 Inicie sesión en el dispositivo y vea o actualice los ajustes de configuración como lo haría normalmente.

Aparece un distintivo de conexión remota en el icono del dispositivo en la Topología de red del dispositivo conectado actualmente.

PASO 9 Cuando haya terminado con la conexión, vuelva a abrir la ventana Información de dispositivo, seleccione la ficha Conectar y haga clic en **Desconectar de dispositivo**. Haga clic en **Desconectar** cuando se le solicite para confirmar la acción.

Tras 20 minutos de inactividad, la conexión se cierra automáticamente.

De forma abreviada, puede hacer clic con el botón derecho del ratón en el icono de un dispositivo que admita conexiones remotas desde la vista Topología o la vista Panel del cliente y seleccionar **Conectarse al dispositivo a través de la Web**. Al establecer una conexión utilizando este método, se utilizan los ajustes configurados en ese momento.

Solución de problemas de configuración de conexiones web (HTTP/HTTPS)

Cuando intente establecer una conexión remota a un dispositivo a través del portal, pruebe la conexión a dispositivos nuevos editando la configuración de conexión en el siguiente orden:

- En primer lugar, intente la conexión con la configuración predeterminada: puerto web del dispositivo establecido en el 80 y el resto de opciones desactivadas.
- Intente utilizar una conexión HTTPS (SSL) con el puerto predeterminado; algunos dispositivos requieren una conexión HTTPS.
- Si la aplicación de administración requiere un puerto específico, pruebe editando el número de puerto.

- Si ve referencias a direcciones IP privadas en URL, intente marcar la opción Reparar encabezados con el Puerto Web del dispositivo establecido en el 80.
- Si se agotan los tiempos de espera de conexión o no funcionan los enlaces de las páginas de contenido, pruebe a habilitar la opción Reparar URL.
- Para algunos dispositivos, es posible que tenga que habilitar tanto Reparar encabezados como Reparar URL.
- Pruebe las opciones anteriores con otro navegador web.
- Es posible que surjan problemas al intentar establecer una conexión web a switches de la serie ESW500 (por ejemplo, un error de tiempo de espera de conexión o una página en blanco). Intente la conexión a través de HTTPS en el puerto 443 utilizando Internet Explorer 7 o Safari. Firefox no funciona con switches de la serie ESW500. Safari no funciona con puntos de acceso WAP4410N.

Configuración de conexión web recomendada para dispositivos

Si el dispositivo al que se está conectando tiene un conjunto de ajustes de conexión que se sabe que funcionan con OnPlus Portal, estos valores predeterminados recomendados aparecen definidos automáticamente en la ficha Conectar de ese dispositivo.

Si los ajustes de conexión que ha configurado son diferentes de los ajustes recomendados, se muestra un mensaje y se le ofrece la opción de **Restaurar ajustes adecuados**.

Cerrar manualmente la conexión a un dispositivo remoto

Para cerrar manualmente una conexión de túnel abierta a un dispositivo remoto en el sitio de un cliente, siga estos pasos.

PASO 1 En la página Descripción general del portal, haga clic en el cliente para abrir su panel.

PASO 2 En la barra de herramientas del panel, haga clic en el icono de acciones del sitio , haga clic en **Acciones diversas** y, a continuación, haga clic en **Forzar desconexión**.

Habilitar o deshabilitar las conexiones a dispositivos remotos para un sitio

Las conexiones remotas a dispositivos del sitio del cliente a través de OnPlus Portal están habilitadas de forma predeterminada. Si un cliente no quiere permitir conexiones remotas a dispositivos en su sitio, puede deshabilitar esta función iniciando sesión en el dispositivo OnPlus Network Agent del cliente.

NOTA Una vez deshabilitadas las conexiones remotas, deberá conectarse directamente a la LAN de las instalaciones del cliente para habilitar las conexiones remotas.

Para habilitar o deshabilitar las conexiones remotas desde el portal a los dispositivos del sitio de un cliente, siga estos pasos.

PASO 1 Desde un PC conectado directamente a la LAN en las instalaciones del cliente, abra un navegador web y conéctese a OnPlus Network Agent.

Puede hacerlo introduciendo la dirección IP de OnPlus Network Agent en la barra de URL o a través de Bonjour.

PASO 2 En la página de inicio de sesión de OnPlus Network Agent, introduzca estas credenciales.

Nombre de usuario: **admin**
Contraseña: *<contraseña_cliente>*

SUGERENCIA La contraseña que debe utilizar es la Contraseña del cliente, que se muestra en la sección **Información de activación** de la página Perfil del cliente en el portal (en la página Descripción general, haga clic en el cliente y, a continuación, seleccione **Perfil** > **Perfil**).

PASO 3 Haga clic en el enlace **Configuración** que se encuentra la parte superior de la página.

PASO 4 Para deshabilitar las conexiones remotas, desactive la opción **Permitir que VAR se conecte a dispositivos de forma remota**. Para volver a habilitar las conexiones remotas, active esta opción.

PASO 5 Haga clic en **Actualizar configuración**.

Una vez actualizada la configuración, las conexiones remotas a dispositivos del sitio del cliente a través de la Web (HTTP/HTTPS), RDP, VNC o túnel genérico se deshabilitan.

9

Administración y mantenimiento de dispositivos de Cisco

Los temas de este capítulo incluyen información sobre las tareas de mantenimiento de los dispositivos de Cisco que pueden realizarse a través de Cisco OnPlus Portal:

- **Mantenimiento automatizado del dispositivo**
- **Copia de seguridad y restauración de la configuración del dispositivo**
- **Administración del firmware para dispositivos de Cisco compatibles**
- **Instalación del firmware del dispositivo**

Mantenimiento automatizado del dispositivo

Durante el mantenimiento automatizado, el firmware de OnPlus Network Agent se actualizará si hay una nueva versión disponible. OnPlus Network Agent se reinicia automáticamente tras la actualización.

Para los dispositivos de Cisco que admiten la copia de seguridad y restauración de la configuración automáticas a través de OnPlus Portal, es necesario realizar una copia de seguridad de la configuración.

- Si no se ha modificado la configuración del dispositivo, no se crea la copia de seguridad.
- Se necesitan unas credenciales de inicio de sesión válidas (y la contraseña habilitada, si se utiliza) para realizar copias de seguridad de la configuración del dispositivo. Consulte **Credenciales, en la página 80**.

Configuración de la hora de inicio de las tareas de mantenimiento

Para establecer la hora de inicio de las tareas de mantenimiento del sitio de un cliente, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, localice el cliente que desee editar y seleccione **Perfil** > **Período de mantenimiento** desde el menú de navegación en la parte superior de la página.

PASO 2 Seleccione una **Hora de inicio local**. La hora es local en virtud de la zona horaria establecida en OnPlus Network Agent.

PASO 3 Haga clic en **Guardar**.

Copia de seguridad y restauración de la configuración del dispositivo

Las copias de seguridad de la configuración de los dispositivos que admiten esta función pueden realizarse a petición desde la ficha **Copias de seguridad** en la ventana del dispositivo. La copia de seguridad y la restauración de la configuración son compatibles con determinados dispositivos de Cisco.

Para realizar las tareas de copia de seguridad y restauración de la configuración en estos dispositivos, es necesario proporcionar unas credenciales.

Los dispositivos se reinician una vez restaurada la configuración.

Para obtener más información acerca de los archivos de copia de seguridad y restauración de la configuración, consulte **Copias de seguridad, en la página 88**.

Para obtener información sobre si un dispositivo determinado admite la copia de seguridad y la restauración de la configuración, consulte las siguientes secciones:

- **Resumen de funciones de los dispositivos, en la página 223**
- **Limitaciones específicas del dispositivo para funciones de OnPlus, en la página 225**

Administración del firmware para dispositivos de Cisco compatibles

Puede cargar en OnPlus Portal firmware para determinados dispositivos de Cisco que haya obtenido en Cisco.com. Esto le permite crear una biblioteca de imágenes de firmware de dispositivo para los dispositivos de sus clientes. El firmware puede utilizarse para actualizar dispositivos de ese tipo para sus clientes. Puede cargar varias versiones de firmware de dispositivo y designar una versión predeterminada para cada tipo de dispositivo.

No todos los dispositivos de Cisco admiten la carga de firmware. Si un dispositivo de Cisco de la red admite la carga de firmware, se mostrará la ficha Firmware en la ventana Dispositivo.

El nuevo firmware para el dispositivo OnPlus Network Agent está disponible a través de OnPlus Portal y se instala automáticamente durante las tareas de mantenimiento diario, si fuera necesario.

Para obtener más información, consulte las siguientes secciones:

- **Carga de firmware de dispositivo al portal**
- **Visualización de la información de la versión del firmware cargado**
- **Instalación del firmware del dispositivo**

Carga de firmware de dispositivo al portal

Para cargar firmware para un dispositivo de Cisco, siga estos pasos.

PASO 1 Descargue el firmware para el dispositivo desde el área de descargas de software de Cisco.com.

PASO 2 Inicie sesión en Cisco OnPlus Portal.

PASO 3 En la página **Descripción general**, haga clic en un cliente que tenga un dispositivo del tipo en cuestión.

PASO 4 Desde la vista Topología de red o la vista Lista de dispositivos del panel del cliente, abra la ventana Información de dispositivo.

PASO 5 Haga clic en la ficha **Firmware**.

Si no se muestra la ficha Firmware, significa que ese tipo de dispositivo no admite cargas de firmware.

PASO 6 Haga clic en **Cargar nuevo firmware** y acceda a la ubicación del firmware que descargó en Cisco.com.

PASO 7 En el diálogo Cargar firmware del dispositivo puede escribir una descripción.

Marque la opción **Firmware predeterminado** si quiere que esta versión del firmware sea la predeterminada para ese tipo de dispositivo. Se genera un evento del tipo Nuevo firmware disponible para todos los dispositivos de ese tipo de su sitio que actualmente no ejecutan esa versión del firmware.

La opción **Firmware predeterminado** no está disponible si se trata de la primera carga de firmware que se realiza para un dispositivo. La primera vez que se carga firmware en un dispositivo, esa carga se marca como el firmware predeterminado para el dispositivo.

PASO 8 Haga clic en **Cargar**.

La versión del firmware que cargue se incluirá en la página **Cisco** > **Firmware**. Consulte **Visualización de la información de la versión del firmware cargado, en la página 148**.

Visualización de la información de la versión del firmware cargado

Para ver una lista de cargas de firmware del dispositivo que se han cargado en el portal, vaya a la página principal Descripción general y seleccione **Cisco > Firmware** en el menú de navegación de la parte superior. Se muestra el nombre del archivo, el ID de producto de Cisco y su tamaño. Las cargas de firmware predeterminadas se identifican con una marca de verificación en la columna Predeterminado.

Instalación del firmware del dispositivo

Para instalar el firmware de dispositivos de Cisco que haya cargado previamente en el portal, siga estos pasos.

NOTA Para instalar el firmware, es necesario proporcionar las credenciales de acceso válidas para el dispositivo. Consulte **Credenciales, en la página 80**.

PASO 1 Asegúrese de que ha cargado la imagen de firmware que desea instalar y de que está incluida en la lista de la página **Cisco** > **Firmware** en el portal. Consulte **Carga de firmware de dispositivo al portal, en la página 147**.

PASO 2 Desde la vista Topología de red o la vista Lista de dispositivos, abra la ventana Información de dispositivo correspondiente al dispositivo en el que se instalará el firmware.

PASO 3 En la ventana Información de dispositivo, haga clic en la ficha **Firmware**.

PASO 4 Seleccione la versión del firmware que desee instalar y abra el cuadro de acciones.

PASO 5 En el cuadro **Acciones**, seleccione **Instalar este firmware**.

La opción **Instalar este firmware** solo se muestra en la lista de firmware para el dispositivo si lo ha cargado en el portal.

PASO 6 Haga clic en **Continuar** cuando se le solicite para confirmar la acción.

Una vez instalado el firmware, normalmente el dispositivo se reinicia.

10

Agregar y administrar agentes autorizados

Este capítulo incluye información sobre cómo invitar, aprobar y administrar agentes autorizados asociados con su cuenta de partner de Cisco OnPlus.

- Descripción general
- Invitar agentes
- Proceso de registro de agentes
- Aprobar o rechazar solicitudes de agentes pendientes
- Eliminar un agente
- Iniciar sesión como agente
- Qué pueden ver y hacer sus agentes autorizados en el portal

Descripción general

Los agentes autorizados son aquellos usuarios a los que permite ver, editar y eliminar su contenido de Cisco OnPlus Portal. Toda la información, excepto la información de su perfil de cuenta de partner, Informes y Calendario de informes, se comparte entre su cuenta y las cuentas de los agentes autorizados.

Los agentes autorizados se registran en Cisco OnPlus Portal a través de una URL especial que usted les proporciona. Cuando un agente se ha registrado, puede aprobar su cuenta. Una vez aprobada, la cuenta del agente pasa a estar activa y habilitada.

Los agentes autorizados de Cisco OnPlus Portal deben tener credenciales de inicio de sesión de Cisco.com para registrarse en el portal.

- Estas credenciales de inicio de sesión de Cisco.com deben ser únicas.
- No puede utilizar las mismas credenciales de inicio de sesión de Cisco.com para varios agentes ni reutilizar las suyas para registrar un agente.

IMPORTANTE Sólo el usuario que crea la cuenta de partner de Cisco OnPlus Portal puede invitar a otros usuarios a convertirse en agentes autorizados. Los agentes autorizados no pueden invitar a otros agentes.

Para ver instrucciones en pantalla y los pasos a seguir para invitar y administrar agentes autorizados, seleccione **Agentes** > **Descripción general del agente** en la barra de navegación de la parte superior de la página Descripción general.

Invitar agentes

Puede invitar agentes para que se registren utilizando uno de los dos métodos siguientes.

- **Envíe un correo electrónico de invitación**. En la página Descripción general, seleccione **Agentes > Agente invitado**, introduzca una o más direcciones de correo electrónico, edite el mensaje, si fuera necesario, y haga clic en **Enviar invitación**. Separe las direcciones con comas.

  o

- **Copie y pegue su URL de registro en Cisco OnPlus única en una ventana de MI o mensaje de correo electrónico**. En la página Descripción general, seleccione **Agentes > Descripción general del agente**. Copie y pegue la URL de registro en Cisco OnPlus Portal única que se muestra en esa página en un mensaje de correo electrónico o ventana de chat de MI y envíelo al agente potencial.
  - Esta URL es única para su cuenta, no para el agente potencial.
  - Utilice la misma URL para invitar a todos sus agentes autorizados.

Proceso de registro de agentes

Cuando el agente potencial recibe el correo electrónico de invitación del portal, deberá seguir estos pasos para registrar su cuenta en el portal.

PASO 1 Haga clic en el enlace de la URL de registro que se proporciona en el mensaje de correo para acceder a la página **Registrar** de Cisco OnPlus Portal.

PASO 2 Complete los campos de la página **Registrar**. La información que se debe proporcionar incluye:

- La dirección de correo electrónico para verificar el registro

- El ID de usuario y la contraseña de Cisco.com
- Información de contacto
- Código de verificación que se muestra en el gráfico de la página de registro

PASO 3 En la sección **Información de productos y privacidad**, el agente debe hacer clic en la casilla de verificación para confirmar que ha leído y aceptado la Declaración de privacidad de Cisco.

PASO 4 Haga clic en **Enviar**. Una vez finalizado el registro correctamente, aparece la página **Registro completado** y se muestra el siguiente mensaje:

```
María García:

¡Enhorabuena! Se ha registrado correctamente. Le enviaremos
una notificación al correo electrónico que ha facilitado
(correoelectrónico@dominio.com) una vez que el administrador
haya revisado y aprobado su registro.

Para volver a la pantalla de inicio de sesión, haga clic
aquí.
```

Una vez registrado el agente, debe acceder a la página Agentes pendientes y aprobar o rechazar la solicitud. Consulte **Aprobar o rechazar solicitudes de agentes pendientes, en la página 153**.

Aprobar o rechazar solicitudes de agentes pendientes

Para aprobar o rechazar solicitudes de agentes pendientes, siga estos pasos.

PASO 1 Desde la página Descripción general, acceda a **Agentes** > **Agentes pendientes**.

PASO 2 Localice un agente en la lista y haga clic en el icono de flecha para mostrar las opciones **Aprobar** o **Rechazar**.

PASO 3 Haga clic en **Aprobar** o **Rechazar**.

- Los agentes aprobados reciben un correo electrónico donde se les informa de que su cuenta está activa y se ha movido a la lista **Agentes aprobados** del portal.
- Los agentes rechazados se mueven a la lista **Agentes rechazados**.

Para volver a invitar a un agente potencial que se haya rechazado previamente, deberá eliminarlo de la lista Agentes rechazados antes de enviarle otra invitación.

Eliminar un agente

Para cancelar la cuenta de un agente aprobado o eliminar un agente de la lista de Agentes rechazados, siga estos pasos.

Puede volver a invitar a los agentes que haya eliminado.

PASO 1 Desde la página Descripción general, acceda a **Agentes** > **Agentes aprobados** o **Agentes** > **Agentes rechazados**.

PASO 2 Localice el agente que desee eliminar y haga clic en el icono de flecha para mostrar la opción **Eliminar**.

PASO 3 Haga clic en **Eliminar**.

Iniciar sesión como agente

Cuando se aprueba una solicitud de cuenta de agente, este recibe un correo electrónico similar al siguiente:

```
María García:

¡Enhorabuena! Su cuenta del portal Cisco OnPlus está activa.
Ahora puede iniciar sesión en la siguiente URL:

https://www.cisco-onplus.com

Su nombre de usuario: mgarcia
```

Para iniciar sesión, el agente hace clic en el enlace del mensaje de correo electrónico, escribe el nombre de usuario que se le ha proporcionado en el mensaje y utiliza la contraseña de su cuenta de Cisco.com para la autenticación.

Una vez que el agente ha iniciado sesión correctamente, deberá leer los **Términos y condiciones** y hacer clic en el botón **Aceptar**, que se encuentra en la parte inferior de la página.

El menú Agentes no se muestra en la barra de navegación si el usuario ha iniciado sesión como agente.

Qué pueden ver y hacer sus agentes autorizados en el portal

Toda la información, excepto la información de su perfil de cuenta de partner y cualquier informe o calendarios de informes creados por usted, se comparte entre su cuenta de partner y las cuentas de los sus agentes autorizados.

Esto significa que todos sus agentes autorizados pueden ver, editar y eliminar todos los sitios de los clientes, contactos de los clientes, eventos y notificaciones. Los agentes pueden conectarse a dispositivos de forma remota y realizar tareas de administración de dispositivos, como actualizaciones de firmware y copia de seguridad y restauración de la configuración de los dispositivos.

Los agentes autorizados no pueden invitar, aprobar, rechazar o eliminar otros agentes, y no pueden ver las listas de agentes pendientes, rechazados o aprobados.

Los agentes autorizados no tienen permiso para establecer intervalos de recordatorio de caducidad de soporte de productos. Sólo el titular de la cuenta de partner puede establecer estos recordatorios. Para obtener más información, consulte **Configuración del intervalo de los recordatorios de expiración de soporte de productos, en la página 175**.

Sólo el creador de la cuenta de partner puede invitar o administrar agentes.

11

Acceso de clientes a OnPlus Portal

En este capítulo se explica cómo añadir y gestionar inicios de sesión del cliente en OnPlus Portal. Asimismo, se incluyen instrucciones de inicio de sesión para clientes y se muestra cómo pueden usar la capacidad de acceso autorizado.

- **Descripción general**
- **Adición de inicios de sesión del cliente**
- **Proceso de activación de inicio de sesión del cliente**
- **Funciones de OnPlus disponibles para los clientes según el modo de acceso**
- **Funciones de OnPlus disponibles para los clientes según el modo de acceso**
- **Administración de inicios de sesión del cliente**

Descripción general

Los partners y sus agentes autorizados pueden proporcionar a los clientes un inicio de sesión en OnPlus Portal para permitirles ver sus propios dispositivos y redes. Tras la activación inicial del inicio de sesión de un cliente, los partners pueden modificar el nivel de acceso del cliente o terminar el acceso, según sea necesario. Se necesita un ID de inicio de sesión en Cisco.com para acceder al portal.

NOTA Para proporcionar acceso a un cliente, este deberá registrarse previamente para obtener una cuenta de Cisco.com.

Una vez que el cliente acepta la invitación y activa el acceso, podrá ver, o incluso modificar, la información sobre la red, en función del acceso que se le haya otorgado.

Existen dos niveles de acceso para los clientes: acceso de solo lectura y acceso completo.

- El acceso de solo lectura permite a los clientes ver la red sin poder cambiar ningún dato o ajuste
- El acceso completo permite a los clientes ver más información sobre la red y realizar cambios limitados en determinados datos del portal.

Se proporciona una tabla en la que se muestran las capacidades según el modo de acceso. Consulte **Funciones de OnPlus disponibles para los clientes según el modo de acceso, en la página 159**.

El proceso para proporcionar y administrar el acceso de los clientes a las redes incluye:

- Selección de un cliente y envío de una invitación de OnPlus.
- Comprobación del estado de acceso del cliente para asegurarse de que ha activado el acceso.
- Cambio del modo de acceso del cliente.
- Eliminación de clientes para terminar el acceso a la red.

Adición de inicios de sesión del cliente

Para añadir un inicio de sesión del cliente, siga estos pasos.

PASO 1 En la página Descripción general, seleccione un cliente para el que desee añadir un inicio de sesión del cliente.

PASO 2 En el menú Perfil de la parte superior de la página, seleccione **Perfil > Inicios de sesión del cliente.**

PASO 3 Haga clic en **Añadir inicio de sesión del cliente.**

PASO 4 En la ventana Añadir inicio de sesión del cliente, introduzca la información necesaria; asegúrese de introducir el **ID de usuario de Cisco.com** correcto.

PASO 5 Haga clic en **Agregar.** El cliente se incluirá en la página Inicios de sesión con el estado Pendiente y se enviará al cliente un correo electrónico de invitación si se ha activado la casilla **Enviar correo electrónico de invitación**.

Proceso de activación de inicio de sesión del cliente

Cuando el cliente recibe la invitación por correo electrónico de OnPlus, seguirá estos pasos para activar el inicio de sesión.

PASO 1 El cliente hace clic en el enlace que se proporciona en el correo electrónico de registro para ir a la página Invitación del cliente.

PASO 2 El cliente introduce la contraseña de Cisco.com y hace clic en **Activar**. Aparece la página Términos y condiciones.

PASO 3 El cliente hace clic en **Aceptar**, lo que activa al cliente en Cisco OnPlus Portal y establece su estado en Activo.

La página se actualiza para mostrar un mensaje que indica que se ha aceptado la invitación con un enlace a la página Iniciar sesión de Cisco OnPlus Portal.

PASO 4 El cliente puede hacer clic en el enlace para ver la red e introducir el nombre de usuario y la contraseña para iniciar sesión.

Cisco OnPlus Portal se abre en la página Panel. Consulte **Funciones de OnPlus disponibles para los clientes según el modo de acceso, en la página 159** para obtener más información sobre el uso de acceso de inicio de sesión del cliente.

Funciones de OnPlus disponibles para los clientes según el modo de acceso

En la tabla siguiente se muestran los privilegios de acceso asignados según el modo de acceso: acceso de solo lectura y acceso completo.

Función	Notas	Modo de acceso	
		Solo lectura	Acceso completo
Panel del cliente			
Estado	Ver el estado de la red	Sí	Sí

Función	Notas	Modo de acceso	
		Solo lectura	Acceso completo
Eventos	Ver y filtrar eventos	Sí	Sí
Perfil	Ver y modificar la información del perfil	Solo visualización	Sí (limitado)
Hacer ping en host	Probar la conectividad de red	No	Sí
Funciones de restablecimiento de datos	Restablecer la topología o volver a descubrir la red	No	Sí
Ajustes de topología	Cambiar el formato de diseño de árbol	No	Sí
Criterios de filtrado	Ajustes y capacidad de búsqueda avanzados	Sí	Sí
Modo de pantalla completa	Cambiar al modo de pantalla completa	Sí	Sí
Agregar dispositivo	Agregar dispositivos a la red	No	Sí
Vista de red	Alternar entre las vistas de topología y lista de dispositivos	Sí	Sí
Zoom	Ampliar y reducir la vista de topología	Sí	Sí
Leyenda	Tabla de iconos de barra de herramientas, distintivos, alarmas y acciones	Sí	Sí
Personalizar	Crear una vista personalizada del panel	Sí	Sí
Exportar	Exportar la lista de dispositivos de red en formatos PNG, CSV o SVG	Sí	Sí
Tarea pendiente	Ver la lista de dispositivos que requieren intervención	Sí	Sí
Dispositivos			
Ver información del dispositivo	Solo dispositivos del cliente	Sí	Sí
Modificar la configuración del dispositivo	Solo dispositivos del cliente	No	Sí
Modificar las credenciales de acceso al dispositivo	Solo dispositivos del cliente	No	Sí
Conectar con dispositivo	Solo dispositivos del cliente	No	Sí
Agregar y modificar monitores de dispositivos	Solo dispositivos del cliente	No	Sí
Ver eventos por dispositivo	Solo dispositivos del cliente	Sí	Sí
Ver información de soporte de Cisco*	*Excluida la información del contrato	Sí	Sí

Función	Notas	Modo de acceso	
		Solo lectura	Acceso completo
Copia de seguridad y restauración de la configuración		No	No
Actualización de firmware		No	No
Cambiar dispositivo raíz	Reemplazar el dispositivo raíz actual	No	Sí
Contraer/Expandir subárbol		No	Sí
Agregar dispositivo secundario	Agregar un nuevo dispositivo secundario	No	Sí
Funciones globales de cuentas de partners	Generación de informes, notificaciones, informes, aplicaciones (algunas de estas funciones no aparecerán en la página y otras aparecerán atenuadas).	No	No
Enviar invitaciones	Invitar a agentes o clientes	No	No

Consulte **Descripción general y funciones del panel, en la página 47** para obtener información detallada sobre el uso de las funciones del panel.

Administración de inicios de sesión del cliente

Los inicios de sesión del cliente activados y pendientes se administran en la página Inicios de sesión.

Edición de inicios de sesión del cliente

PASO 1 En la lista Nombre del cliente de la página Descripción general, seleccione el cliente.

PASO 2 En el menú Perfil de la parte superior de la página, seleccione **Perfil > Inicios de sesión del cliente.**

PASO 3 En la página Inicios de sesión, haga clic una vez en el nombre de usuario que desee editar.

PASO 4 En el cuadro de acciones, seleccione **Editar.** La opción Editar permite las siguientes funciones:

- Introducir comentarios
- Cambiar el modo de acceso.

Eliminación de inicios de sesión del cliente

PASO 1 En la lista **Nombre del cliente** de la página Descripción general, seleccione el cliente.

PASO 2 En el menú Perfil de la parte superior de la página, seleccione **Perfil > Inicios de sesión del cliente.**

PASO 3 En la página Inicios de sesión, haga clic una vez en el **nombre de usuario** que desee eliminar.

PASO 4 En el cuadro de acciones, seleccione **Eliminar**. La opción Eliminar termina el acceso del cliente al portal.

Reenvío de invitaciones a inicios de sesión del cliente

PASO 1 En la lista **Nombre del cliente** de la página Descripción general, seleccione el cliente.

PASO 2 En el menú Perfil de la parte superior de la página, seleccione **Perfil > Inicios de sesión del cliente.**

PASO 3 En la página Inicios de sesión, haga clic una vez en el nombre de usuario al que desee volver a enviar una invitación.

PASO 4 En el cuadro de acciones, seleccione **Volver a enviar invitación.**

PASO 5 Introduzca la información necesaria en la ventana de correo electrónico y vuelva a enviar la invitación al cliente.

Para obtener información sobre cómo activa el cliente el acceso al portal mediante el enlace proporcionado en la invitación, consulte **Proceso de activación de inicio de sesión del cliente, en la página 159**

12

Informes

En este capítulo se explica cómo utilizar las funciones de creación de informes de Cisco OnPlus Portal. Se tratan los siguientes temas:

- Descripción general
- Tipos de informes
- Creación de un informe
- Visualización de calendarios de informes
- Previsualización y descarga de informes
- Eliminación de informes
- Previsualización y descarga de informes

Descripción general

En la página Descripción general, seleccione **Informes** para acceder a las siguientes opciones de informe:

- **Lista de informes**. En la página Lista de informes, puede crear y programar nuevos informes, ver una lista de los informes y acceder a las opciones de previsualización, descarga y eliminación de informes individuales.
- **Calendario de informes**. En la página Calendario de informes, puede ver información de los informes programados o eliminarlos (cancelarlos).

Los informes están asociados con unas credenciales de inicio de sesión de usuario en el portal específicas:

- Solo puede ver o eliminar los informes que usted haya creado.
- No puede ver ni eliminar los informes que hayan creado sus agentes autorizados.

Al crear un informe, puede seleccionar si desea crearlo inmediatamente o programarlo como un informe periódico que se genere diariamente, semanalmente o mensualmente. También puede especificar si desea que se le notifique cuando se genere el informe. Los informes pueden tener formato PDF, CSV y XHTML.

Para los informes programados, puede especificar un destinatario entre sus contactos de entrega y que los informes se envíen por correo electrónico.

Tipos de informes

Pueden generarse los siguientes tipos de informes:

- **Informe de clientes**. Este informe incluye todos sus clientes: en línea (activos), suspendidos y nunca conectados (esperando activación). El informe muestra información de los clientes (nombre, dirección y contacto) y la fecha de activación, suspensión o creación.
- **Inventario de clientes.** Este informe se puede generar para todos los clientes o para un cliente en particular. El informe incluye tanto dispositivos de Cisco como dispositivos que no son de Cisco. Para dispositivos de Cisco, se incluye la dirección IP, el modelo, la dirección MAC y las versiones de firmware. Para los dispositivos que no son de Cisco, se incluye la dirección IP, la dirección MAC, el modelo (si se conoce) y el proveedor (si se conoce).
- **Historial de eventos, filtrado por gravedad**. Este informe se puede generar para todos los clientes o para un cliente en particular.

  El informe incluye el número total de eventos, un gráfico de la distribución de los eventos por su nivel de gravedad y la fecha, el ID de evento y el mensaje para cada evento. Los eventos aparecen ordenados por nivel de gravedad.
- **Resumen ejecutivo**. Este informe se puede generar para un cliente en particular. El informe incluye información del cliente (nombre, dirección y zona horaria), datos de conectividad a Internet (número de veces que la conexión a Internet no ha estado activa), información y estado del dispositivo Cisco OnPlus Network Agent, datos de topología de la red, nuevos dispositivos detectados, datos del resumen de eventos de la red e información de soporte de productos (garantías, contratos de servicio, final de ciclo de vida y final de la venta de los productos, avisos de campo y avisos de seguridad del producto).

- **Historial de notificaciones**. Este informe se puede generar para todos los clientes o para un cliente en particular. El informe incluye el número total de notificaciones enviadas para cada cliente y la fecha, el tipo de evento y el destino de la entrega (por ejemplo, una dirección de correo electrónico) para cada notificación.

Creación de un informe

Para crear un informe, siga estos pasos.

PASO 1 Acceda a **Descripción general >Informes >Lista de informes**.

PASO 2 En la página Lista de informes, haga clic en **+ Crear informe**.

PASO 3 Seleccione el tipo de informe que desee crear.

En función del tipo de informe que esté creando, seleccione entre las siguientes opciones.

Opción	Obligatorio	Descripción	Informes a los que se aplica
Formato	Sí	Especifique un formato para el informe. Los formatos disponibles incluyen Adobe PDF, CSV (valores separados por comas) y XHTML (Extensible Hypertext Markup Language).	Todos los informes
Idioma preferido	Sí	Especifique el idioma en el que desea que se genere el informe. Las opciones disponibles son las siguientes: Francés, alemán, italiano y español. El idioma predeterminado es el inglés.	Todos los informes
Cliente	Sí	Especifique si los datos del informe se proporcionan para todos los clientes o seleccione un cliente específico.	Inventario de clientes, Historial de eventos, Resumen ejecutivo, Historial de notificaciones
Notas de la portada	No	Escriba notas que se mostrarán en la página de título del informe. Puede introducir hasta 300 caracteres. Esta opción no se aplica a los informes creados en formato CSV.	Todos los informes

Opción	Obligatorio	Descripción	Informes a los que se aplica
Gravedad	Sí	Seleccione un nivel de gravedad. El informe incluye los eventos que tengan el nivel de gravedad seleccionado o superior.	Historial del evento

PASO 4 Haga clic en **Siguiente**.

PASO 5 En la página **Secciones**, haga clic para seleccionar o eliminar la selección de las secciones que desea incluir en el informe. Las secciones disponibles que aquí se incluyen pueden variar, en función del tipo de informe seleccionado.

PASO 6 Haga clic en **Siguiente**.

PASO 7 Especifique las opciones de notificación y programación para el tipo de informe seleccionado. Las opciones disponibles se incluyen a continuación.

Opción	Descripción
Creación de informes	Establezca la frecuencia de los informes. Seleccione **Ahora** para generar un informe inmediatamente. Seleccione **Todos los días**, **Todas las semanas** o **Todos los meses** para programar un informe periódico. ▪ Los informes diarios se generan cada día a las 00:00:00 (medianoche). ▪ Los informes semanales se generan cada 7 días, comenzando por la fecha establecida en **El primer informe se realiza el**. ▪ Del mismo modo, los informes mensuales se generan cada mes, comenzando por la fecha establecida en **El primer informe se realiza el**. ▪ Por ejemplo, si establece el 15 de junio como fecha en **El primer informe se realiza el** al programar un informe mensual, el primer informe se genera en esa fecha e incluye los datos del mes anterior. El siguiente informe mensual de la serie se generará el 15 de julio.
Inicio del período de informes **Fin del período de informes**	Si seleccionó **Ahora**, haga clic en estos campos y utilice el calendario emergente para seleccionar las fechas de inicio y fin del período de generación de informes. Este campo no se aplica a los informes de Cliente o Inventario.

Opción	Descripción
El primer informe se realiza el **El último informe se realiza el**	Si seleccionó **Todos los días**, **Todas las semanas** o **Todos los meses**, haga clic en cada uno de estos campos para abrir un calendario emergente y especificar el periodo de generación de informes seleccionando las fechas del primer y el último informe. También puede seleccionar no especificar la fecha de fin optando por **Sin fecha de finalización**. El calendario de informes se elimina automáticamente cuando se genera el último informe. La primera vez que abre el calendario emergente, la fecha actual está seleccionada.
Notificarme	Esta opción solo se aplica para programar informes periódicos. Si está marcada la opción **Notificarme**, se envía una notificación cuando se genera el informe a la dirección de correo electrónico especificada en el perfil de su cuenta del portal.
Destinatario y dirección de correo electrónico para el informe	Seleccione un contacto de cliente o un contacto global de la lista desplegable. Una vez seleccionado el destinatario, seleccione un método de entrega de la lista desplegable. Solo se muestran los contactos de cliente o globales que tengan configurada una dirección de correo electrónico de destino. El informe se envía como archivo adjunto al mensaje de correo electrónico. Para obtener más información sobre los contactos de entrega, consulte **Cómo agregar y administrar contactos de entrega, en la página 104**. Si la dirección de correo electrónico de contacto de destino está deshabilitada en la página de contactos de entrega, el informe no se envía.
Mensaje de correo electrónico	Opcional. Si se especifica un destinatario del informe y una dirección de correo electrónico, puede escribir un texto que se incluirá en el mensaje de correo electrónico y se enviará con el informe. Puede introducir hasta 300 caracteres. Los corchetes angulares de apertura (<) y los caracteres de nueva línea del mensaje de texto se eliminan del mensaje de correo electrónico.

PASO 8 Si quiere crear el informe en ese momento, haga clic en **Guardar**. El informe se pondrá en cola para su procesamiento.

Para ver el estado de su solicitud de informe o previsualizar y descargar informes completados, seleccione **Informes** > **Lista de informes**. Consulte **Previsualización y descarga de informes, en la página 168**.

Es posible que tenga que actualizar la página Lista de informes para ver el estado actual del informe, especialmente si acaba de crearlo.

PASO 9 Si está programando una serie de informes, haga clic en **Guardar** para actualizar la lista de informes programados.

Para ver información acerca de los informes programados, seleccione **Informes** > **Calendario de informes**.

Visualización de calendarios de informes

NOTA No es posible modificar un informe programado una vez creado. Debe eliminar y volver a crear el informe y su información de programación si necesita hacer cambios.

Los calendarios de informes se eliminan del portal automáticamente al principio del siguiente periodo de creación de informes, que tiene lugar tras la creación del último informe.

Solo puede ver los calendarios de informes que haya creado usted mismo.

Para ver un informe programado, siga estos pasos.

PASO 1 En la página Descripción general, seleccione **Informes** > **Calendario de informes**.

PASO 2 Haga clic en el calendario de informes que desee ver.

PASO 3 Haga clic en **Detalles** para ver información adicional y consultar la lista de todos los informes generados con esta regla. Haga clic en un informe determinado para acceder a las acciones de descarga y eliminación para el informe seleccionado.

PASO 4 Haga clic en **Atrás** para volver a la lista de calendarios de informes.

Previsualización y descarga de informes

En la página Lista de informes, puede ver información del informe y el estado del procesamiento, consultar una lista de todos los informes que se han creado y previsualizar o descargar informes completados.

Para previsualizar o descargar un informe, siga estos pasos.

PASO 1 En la página Descripción general, seleccione **Informes** > **Lista de informes**.

Haga clic en un encabezado de columna para ordenar la lista por Informe (tipo), Notas, Estado (En cola, En proceso o Error), Formato (PDF, CSV o XHTML), tamaño o fecha de creación.

Utilice los controles de la esquina inferior derecha de la página para desplazarse por la lista, si fuera necesario.

PASO 2 Haga clic en un informe de la lista para seleccionarlo y acceder al cuadro de acciones.

PASO 3 Seleccione **Previsualizar** para ver una versión en miniatura del informe completado. Haga clic en el gráfico de previsualización de la izquierda para desplazarse por las secciones del informe.

PASO 4 Seleccione **Descargar** para descargar una copia del informe completado en su equipo.

Al crear un informe en formato XHTML, se crea un archivo .zip que puede descargarse. El archivo .zip contiene el directorio raíz con el informe (index.html) y todos los recursos (imágenes en formato .png y un archivo de hoja de estilo CSS que incluye información de formato). Esta estructura de directorio permite extraer informes a un directorio de servidor web “www” para facilitar su publicación.

NOTA Para ver las imágenes, debe extraerse por completo el archivo .zip.

PASO 5 Guarde el informe en su equipo.

Eliminación de informes

Solo puede acceder o eliminar los informes que usted haya creado.

Para eliminar un solo informe de la página Lista de informes, siga estos pasos.

PASO 1 En la página de información general de la cuenta de partner, seleccione **Informes** > **Lista de informes**.

PASO 2 Haga clic en el informe que desee eliminar.

PASO 3 Haga clic en **Eliminar**.

También puede eliminar informes generados a partir de una regla de calendario de informes desde la lista de calendarios de informes. Para ello, siga estos pasos.

PASO 1 En la página de información general de la cuenta de partner, seleccione **Informes** > **Calendario de informes**.

PASO 2 Haga clic en un informe programado para abrir el cuadro de acciones.

PASO 3 Haga clic en **Detalles**.

PASO 4 En la página de detalles del calendario de informes, haga clic en **Borrar todo** para eliminar todos los informes que se generaron con esa regla de programación. Haga clic en **Aceptar** para confirmar la acción.

PASO 5 También puede eliminar un informe específico de la lista de historial. Para ello, seleccione el informe en el historial de informes para abrir el cuadro de acciones y, a continuación, haga clic en **Eliminar**. Haga clic en **Aceptar** para confirmar la acción.

Eliminación de un calendario de informes

Solo puede eliminar los calendarios de informes que haya creado usted mismo.

Para eliminar un calendario de informes, siga estos pasos.

PASO 1 En la página de información general de la cuenta de partner, seleccione **Informes** > **Calendario de informes**.

PASO 2 Haga clic en el informe programado para abrir el cuadro de opciones.

PASO 3 Haga clic en **Eliminar**.

PASO 4 Haga clic en **Aceptar**.

13

Visualización de la información de soporte de productos Cisco

En este capítulo se explica cómo ver la información de soporte en OnPlus Portal para los dispositivos de Cisco compatibles. Se tratan los siguientes temas:

- **Descripción general**
- **Visualización de la información de soporte de productos para todos los clientes**
- **Visualización de la información de soporte de productos para un dispositivo determinado**
- **Eventos de soporte de productos**
- **Incluir información de soporte de productos en los informes**
- **Configuración del intervalo de los recordatorios de expiración de soporte de productos**
- **Creación de reglas de entrega para notificaciones de soporte de productos**

Descripción general

En OnPlus Portal, puede ver los siguientes tipos de información de soporte de productos para dispositivos y software de Cisco:

- Contrato de servicio (soporte para productos Smartnet o Small Business) e información de la garantía (se requieren credenciales de acceso al dispositivo)
- Avisos de seguridad del producto (PSIRT)
- Avisos de final de ciclo de vida, de soporte y de venta del hardware
- Avisos de campo

IMPORTANTE Para obtener información sobre el Contrato de servicio y la Garantía para un dispositivo de Cisco, es necesario proporcionar las credenciales de inicio de sesión o habilitación de acceso (para ver las instrucciones, consulte **Credenciales, en la página 80**). Una vez proporcionadas las credenciales de acceso, la próxima vez que se ejecute la detección en el portal, la ficha Soporte del dispositivo debería aparecer en la ventana Información de dispositivo y estar disponible la información de soporte obtenida para el dispositivo.

NOTA Podría haber un retardo entre el momento de actualización de la base de datos de información de soporte de Cisco y el momento en el que las actualizaciones se muestran en Cisco OnPlus Portal. Dependiendo del tipo de información, el retardo puede variar entre unos días y más de una semana.

Visualización de la información de soporte de productos para todos los clientes

En el área de información general de la cuenta de partner del portal, puede visualizar la información de soporte de productos de todos sus clientes. Para acceder la información de soporte de productos, seleccione las opciones del menú de Cisco.

Categoría de información de soporte de productos	Descripción/Información incluida
Información del contrato	Estado del contrato Cliente Icono del producto, ID del producto y número de serie Programa de servicio Acuerdo de nivel de servicio Fecha de inicio y finalización
Información de la garantía	Cliente Icono del producto, ID del producto y número de serie Fecha de inicio de garantía Fecha de final de garantía Dirección MAC
Final del ciclo de vida del hardware	Estado Cliente Icono del producto, ID del producto y número de serie Descripción Fecha anunciada Fecha final de venta Fecha de renovación del servicio Fin de fecha de soporte Enlace activo al aviso publicado en Cisco.com

Categoría de información de soporte de productos	Descripción/Información incluida
Final del ciclo de vida del software (se aplica principalmente a versiones del software Cisco IOS)	Estado Cliente Icono del producto, ID del producto y número de serie SO y versión del SO Descripción Fechas de final de soporte, ciclo de vida y venta Enlace activo al aviso publicado en Cisco.com
Avisos de campo	Cliente Icono del producto, ID del producto y número de serie Descripción Enlace activo a la ubicación del aviso completo en Cisco.com Fecha de publicación Fecha de la última revisión
Avisos de seguridad del producto (PSIRT) (se aplica principalmente a versiones del software Cisco IOS)	Cliente ID del producto y número de serie Descripción Tipo SO y versión del SO Fecha de renovación del servicio Fin de fecha de soporte Enlace activo a los detalles de cada aviso, incluidos los de gravedad Descripción, fecha de publicación y enlace activo al aviso publicado en Cisco.com

Visualización de la información de soporte de productos para un dispositivo determinado

Para ver la información de soporte de productos para un determinado dispositivo, siga estos pasos.

PASO 1 En la página de información general de la cuenta de partner, haga clic en un cliente para acceder a su panel.

PASO 2 Desde la vista Topología o la vista Lista de dispositivos del panel del cliente, seleccione el dispositivo y abra la ventana Información de dispositivo.

PASO 3 Haga clic en la ficha **Soporte**.

PASO 4 En la ficha **Soporte**, haga clic en la categoría de información de soporte que desee ver. Sólo se muestran las categorías de información de soporte disponibles para ese dispositivo.

Muchas de las fichas incluyen enlaces activos a información adicional.

Eventos de soporte de productos

Los eventos de soporte de productos se generan en respuesta a:

- Expiración de la garantía y el contrato de servicio
- Avisos de seguridad del producto (PSIRT)
- Anuncios de final de la venta, del ciclo de vida y del soporte del producto
- Boletines de campo

Estos eventos de soporte de productos se generan con un nivel de gravedad de Aviso. Para obtener más información acerca de la visualización de eventos, consulte **Visualización de eventos, en la página 121**.

Los recordatorios de expiración de soporte de productos se generan con un nivel de gravedad de Advertencia. Consulte **Configuración del intervalo de los recordatorios de expiración de soporte de productos, en la página 175**.

Incluir información de soporte de productos en los informes

Al crear un informe de Resumen ejecutivo, puede seleccionar incluir secciones que ofrezcan un resumen de la siguiente información de soporte de productos para dispositivos de Cisco:

- Estado de la garantía
- Estado del contrato
- Avisos de seguridad del producto, agrupados por su gravedad
- Avisos de campo

La sección Detalles de dispositivo del informe Inventario de clientes muestra la información de soporte de productos para dispositivos de Cisco.

Para obtener más información, consulte **Creación de un informe, en la página 165**.

Configuración del intervalo de los recordatorios de expiración de soporte de productos

De forma predeterminada, los recordatorios de expiración para los eventos de contrato de servicio, garantía del producto y final de ciclo de vida de hardware o software se generan 60 días antes de la fecha de expiración.

Los recordatorios de expiración de soporte de productos se generan con una gravedad de Advertencia y las notificaciones se envían al contacto especificado en la regla de entrega predeterminada. Si elimina o deshabilita las notificaciones para la regla de entrega predeterminada sin crear otra regla para los eventos de expiración, no recibirá notificaciones de recordatorio (consulte **Creación de reglas de entrega para notificaciones de soporte de productos, en la página 176**).

Para cambiar el intervalo de recordatorio predeterminado de un evento de expiración de soporte de productos para que sea menor de 60 días antes de la fecha de expiración, siga estos pasos.

IMPORTANTE Los agentes autorizados no tienen permiso para establecer intervalos de recordatorio de expiración de soporte de productos. Sólo el titular de la cuenta de partner puede establecer estos recordatorios.

PASO 1 En la página de información general de la cuenta de partner, seleccione **Cisco** > **Información del contrato**, **Garantía**, **Final del ciclo de vida del hardware** o **Final del ciclo de vida del software**.

Puede establecer un intervalo de recordatorio diferente para cada tipo de evento de expiración de soporte de productos.

PASO 2 Haga clic en el botón **Modif** a la derecha de la etiqueta **Recordatorios**.

PASO 3 Establezca el número de días para el recordatorio.

Si no desea recibir recordatorios de expiración de soporte de productos, establezca el número de días antes del recordatorio en **Desactivado**.

PASO 4 Haga clic en **Guardar**.

Creación de reglas de entrega para notificaciones de soporte de productos

Los eventos de soporte de productos se generan con un nivel de gravedad de Aviso. Para recibir la notificación a través de correo electrónico o mensaje de texto SMS para estos eventos (se recomienda crear una regla de entrega de notificaciones). Asegúrese de que la opción **Especificar evento** está habilitada y especifique uno de los siguientes tipos de evento de producto.

- Producto: alerta de Cisco Security (PSIRT).
- Producto: alerta de contrato de servicios de Cisco.
- Producto: aviso de final de la venta, del ciclo de vida y de soporte.
- Producto: alerta de final de garantía.

14

Mantenimiento de ON100 Network Agent

Esta sección incluye instrucciones para realizar las siguientes tareas manuales de mantenimiento de OnPlus Network Agent:

- **Modificación de la configuración de red después de la activación**
- **Restablecimiento de OnPlus Network Agent**
- **Restablecimiento de la configuración predeterminada en OnPlus Network Agent**
- **LED de estado de OnPlus Network Agent**
- **Desactivación de un sitio para sustituir OnPlus Network Agent (RMA)**
- **Transferencia de OnPlus Network Agent a otro cliente**

Modificación de la configuración de red después de la activación

Tras la activación, podrá modificar la configuración de red de OnPlus Network Agent para:

- Asignar una dirección IP estática a OnPlus Network Agent o utilizar DHCP para obtener una dirección IP
- Modificar la configuración del servidor de nombres DNS
- Modificar la configuración del servidor NTP

Para editar la configuración de red tras la activación, siga estos pasos.

PASO 1 Desde la vista Topología de red o la vista Lista de dispositivos, abra la ventana Información de dispositivo del dispositivo en cuestión.

PASO 2 En la ficha Ajustes del menú Acciones, seleccione **Conectar con dispositivo** y, a continuación, haga clic en **Confirmar**.

NOTA Si no están habilitadas las conexiones remotas con el sitio del cliente, deberá conectarse a OnPlus Network Agent desde un PC en la LAN mediante su dirección IP o a través de Bonjour, UPnP, o Cisco FindIT.

PASO 3 Inicie sesión en OnPlus Network Agent.

a. En el campo Nombre de usuario, introduzca **admin**.

b. En el campo **Contraseña**, escriba la contraseña del sitio del cliente (la misma que utilizó en la página Instalar sitio). De forma predeterminada, es una contraseña de 6 dígitos generada automáticamente.

   Si no conoce la contraseña del cliente, abra la página **Perfil** de ese cliente en el portal y consulte la sección **Información de activación**.

   Haga clic en **Iniciar sesión**.

PASO 4 Haga clic en el enlace **Configuración** en la parte superior de la página.

PASO 5 Haga clic en **Configurar ajustes de red adicionales**.

PASO 6 Edite la dirección IP, el servidor de nombres DNS o la configuración de NTP según sea necesario.

PASO 7 Haga clic en **Aplicar ajustes de red**.

Restablecimiento de OnPlus Network Agent

Cuando se restablece OnPlus Network Agent, todos los procesos se cierran de forma segura, se reinicia OnPlus y se actualiza el firmware automáticamente, si fuera necesario.

Este tipo de restablecimiento puede utilizarse para forzar a Network Agent para que busque una actualización de firmware, borre una condición secundaria o vuelva a intentar la activación. Los datos del cliente en el dispositivo y la asociación con el portal no se ven afectados por este tipo de restablecimiento.

Para restablecer OnPlus Network Agent manualmente desde OnPlus Portal, siga estos pasos.

PASO 1 Desde la vista Topología de red o la vista Lista de dispositivos del cliente, abra la ventana Información de dispositivo de OnPlus Network Agent.

PASO 2 Haga clic en la ficha **Ajustes**.

PASO 3 En el menú **Acciones**, seleccione **Reiniciar dispositivo**.

PASO 4 Haga clic en **Confirmar**.

También puede utilizar el botón **RESET** del panel posterior de OnPlus Network Agent. Mantenga presionado el botón **RESET** durante menos de 10 segundos.

Restablecimiento de la configuración predeterminada en OnPlus Network Agent

Un restablecimiento de la configuración predeterminada elimina todos los datos del cliente de OnPlus Network Agent, al igual que cualquier asociación con OnPlus Portal. Este tipo de restablecimiento está pensado para aquellos casos en los que desee restaurar el dispositivo a la configuración predeterminada o eliminar los datos existentes del cliente, de modo que pueda reactivarse el agente con otro cliente.

Puede realizar un restablecimiento de la configuración predeterminada de OnPlus Network Agent conectándolo al dispositivo (ya sea de forma remota, desde el portal o localmente) y utilizando la utilidad de administración de OnPlus Network Agent.

También puede restablecerse la configuración predeterminada en OnPlus Network Agent mediante el botón RESET, que se encuentra en el panel posterior.

Para obtener instrucciones, consulte las siguientes secciones:

- **Restablecimiento de la configuración predeterminada a través de OnPlus Portal, en la página 180**
- **Restablecimiento de la configuración predeterminada con el botón RESET, en la página 181**

Restablecimiento de la configuración predeterminada a través de OnPlus Portal

Para restablecer la configuración predeterminada de OnPlus Network Agent desde OnPlus Portal, siga estos pasos.

PASO 1 Desde la vista Topología de red o la vista Lista de dispositivos, abra la ventana Dispositivo del dispositivo en cuestión.

PASO 2 En la ficha Ajustes del menú Acciones, seleccione **Conectar con dispositivo** y, a continuación, haga clic en **Confirmar**. Una vez establecida la conexión remota, aparece la página de inicio de sesión en OnPlus Network Agent.

NOTA Si no están habilitadas las conexiones remotas con el sitio del cliente, deberá conectarse a OnPlus Network Agent desde un PC en la LAN mediante su dirección IP o a través de Bonjour, UPnP, o Cisco FindIT.

PASO 3 Inicie sesión en OnPlus Network Agent.

a. En el campo Nombre de usuario, introduzca **admin**.

b. En el campo **Contraseña**, escriba la contraseña del sitio del cliente (la misma que utilizó en la página Instalar sitio). De forma predeterminada, es una contraseña de 6 dígitos generada automáticamente.

   Si no conoce la contraseña del cliente, abra la página **Perfil** de ese cliente en el portal y consulte la sección **Información de activación**.

   Haga clic en **Iniciar sesión**.

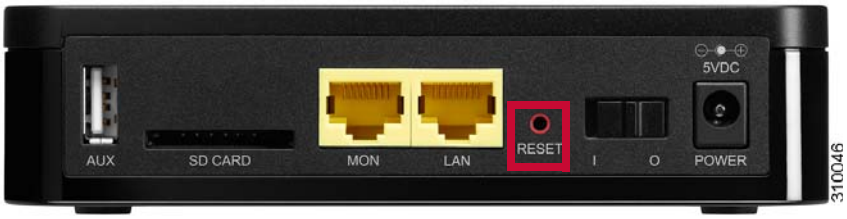
PASO 4 Haga clic en el enlace **Mantenimiento** en la parte superior de la página.

PASO 5 Haga clic en el icono **Restablecer configuración predeterminada**.

PASO 6 Haga clic en **Aceptar** cuando se le solicite, para confirmar el restablecimiento.

Restablecimiento de la configuración predeterminada con el botón RESET

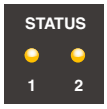
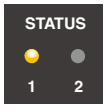
Para restablecer la configuración predeterminada de OnPlus Network Agent con el botón RESET, que se encuentra en el panel posterior del dispositivo, utilice un clip o un objeto similar para mantener presionado el botón RESET durante al menos 10 segundos.

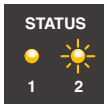
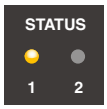
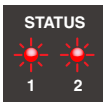
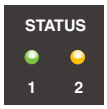
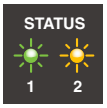
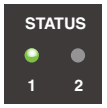
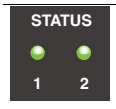


Cuando el LED STATUS 1 está iluminado en verde fijo y el LED STATUS 2 está apagado, el dispositivo está listo para apagarlo o reactivarlo. Consulte **LED de estado de OnPlus Network Agent, en la página 181**.

LED de estado de OnPlus Network Agent

Los LED STATUS 1 y STATUS 2 del panel frontal de OnPlus Network Agent indican el progreso del dispositivo durante las operaciones de encendido, reinicio, actualización y restablecimiento.

LED de estado			Descripción
Encendido e inicialización			
	1	Ámbar fijo	Secuencia de encendido.
	2	Ámbar fijo	
	1	Ámbar fijo	Comenzando la inicialización del software.
	2	Desactivado	

LED de estado			Descripción
	1	Ámbar fijo	Adquiriendo una dirección IP. Si se muestra este patrón durante más de dos minutos, significa que OnPlus Network Agent no ha podido obtener una dirección IP. Si se configura una IP estática, este patrón nunca se muestra durante más de 10 segundos.
	2	Ámbar intermitente	
	1	Ámbar fijo	Completando la inicialización del software.
	2	Desactivado	
Descarga y actualización del software			
	1	Rojo intermitente	Descargando e instalando la imagen de software base (requiere conexión a Internet). Solo verá este patrón antes de la activación (durante la primera instalación) o después de un restablecimiento de la configuración predeterminada.
	2	Rojo intermitente	
	1	Verde fijo	Actualizando el software (requiere conexión a Internet).
	2	Ámbar fijo	
Reinicio			
	1	Verde intermitente	Reiniciando OnPlus Network Agent. OnPlus Network Agent se reinicia tras un restablecimiento normal, un restablecimiento de la configuración predeterminada o una actualización de software.
	2	Ámbar intermitente	
Listo para la activación/Dispositivo en línea, sin conectividad con OnPlus Portal			
	1	Verde fijo	Si no se ha activado aún OnPlus Network Agent, este patrón de LED indica que el software del agente se está ejecutando y el dispositivo está listo para la activación. Si OnPlus Network Agent ya se ha activado, esta secuencia de LED indica que se está ejecutando el software de OnPlus Network Agent, pero que el dispositivo no tiene conexión a OnPlus Portal.
	2	Desactivado	
Funcionamiento normal (activado/en línea)			
	1	Verde fijo	Ambos LED de estado iluminados en verde fijo indican que OnPlus Network Agent está activado, en línea y comunicándose con OnPlus Portal. Este es el modo de funcionamiento normal.
	2	Verde fijo	

Desactivación de un sitio para sustituir OnPlus Network Agent (RMA)

La función de desactivación de un sitio está pensada principalmente para aquellas situaciones en las que desee sustituir o devolver (RMA) la unidad de OnPlus Network Agent de un cliente y reactivar el cliente utilizando el dispositivo de sustitución. Esta función puede utilizarse también para solucionar problemas o para hacer demostraciones, cuando desee desactivar un sitio y volver a activar el cliente con el mismo OnPlus Network Agent.

Cuando se desactiva un sitio:

- Se eliminan todos los datos del cliente del dispositivo OnPlus Network Agent.
- Siempre y cuando no se elimine el cliente, la información del cliente se conserva (por ejemplo, las credenciales del dispositivo y la configuración de los monitores del dispositivo). Cuando se reactive el cliente, esta configuración estará presente.
- La página Estado del sitio desactivado muestra el mensaje “Activación en espera”.
- OnPlus Network Agent no se podrá utilizar para comunicarse con el portal hasta que se reactive.

Para desactivar un sitio, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, haga clic en el cliente cuyo sitio desee desactivar.

PASO 2 Desde la vista Topología de red o la vista Lista de dispositivos, abra la ventana Información de dispositivo del dispositivo OnPlus Network Agent de ese cliente.

PASO 3 Seleccione la ficha **Ajustes**.

PASO 4 En el menú desplegable **Acciones** de la ficha Ajustes, seleccione **Desactivar este sitio completo**.

PASO 5 Haga clic en **Confirmar**.

Si está sustituyendo la unidad de OnPlus Network Agent, puede a continuación instalar el dispositivo ON100 de sustitución y volver a activar el cliente.

Transferencia de OnPlus Network Agent a otro cliente

Para transferir un dispositivo OnPlus Network Agent a otro cliente, siga estos pasos.

PASO 1 Restablezca la configuración predeterminada en el OnPlus Network Agent asociado con el anterior cliente. Consulte **Restablecimiento de la configuración predeterminada en OnPlus Network Agent, en la página 179**.

PASO 2 Cree una cuenta en OnPlus Portal para el nuevo cliente. Consulte **Cómo agregar un cliente, en la página 42**.

PASO 3 En el sitio del nuevo cliente, instale y active OnPlus Network Agent con la información de activación del nuevo cliente. Consulte **Instalación y activación de OnPlus Network Agent en las instalaciones del cliente, en la página 21**.

PASO 4 Elimine la cuenta del cliente anterior para borrar permanentemente de OnPlus Portal toda la información de ese cliente. Consulte **Eliminación de un cliente**.

15

Integración de la creación de vales de servicio de Autotask

Esta sección incluye instrucciones de configuración de los ajustes de las aplicaciones de Cisco OnPlus Portal y los ajustes de la aplicación Autotask, de modo que puedan crearse vales de Autotask Service Desk automáticamente, basados en los eventos y notificaciones que se generan a través del portal.

Se tratan los siguientes temas:

- **Compatibilidad de la versión de Autotask**
- **Configuración de los ajustes de Autotask**
- **Configuración de los ajustes de Cisco OnPlus Portal**
- **Generación de eventos, notificaciones y vales de servicio de prueba**
- **Comprobación de la creación de vales de servicio en Autotask**
- **Resolución de vales automatizada (solo eventos de monitor de dispositivos)**
- **Suspensión de la generación de vales de servicio para todos los clientes**
- **Actualización de la información de cuentas global**
- **Eliminación de la aplicación Autotask de un cliente**
- **Problemas conocidos**

Compatibilidad de la versión de Autotask

Cisco OnPlus Portal utiliza la versión 1.5 de Autotask API.

Autotask es compatible con Internet Explorer 7 o posterior. Si utiliza otro navegador, ciertas partes de la aplicación no estarán disponibles. Para obtener información sobre la compatibilidad con navegadores web para Autotask, consulte **Ejecutar la comprobación de navegador web de Autotask, en la página 186**.

Configuración de los ajustes de Autotask

Los temas de esta sección describen los ajustes que se deben configurar en Autotask para que se creen automáticamente vales de Autotask Service Desk basados en los eventos que se supervisan a través de Cisco OnPlus Portal.

- **Ejecutar la comprobación de navegador web de Autotask, en la página 186**
- **Crear una cola de Service Desk para el portal, en la página 187**
- **Modificar la política de flujo de trabajo para el tratamiento de vales duplicados, en la página 187**
- **Comprobar la configuración de las políticas de flujo de trabajo para los campos obligatorios, en la página 188**
- **Crear una cuenta de cliente en Autotask, en la página 188**

Ejecutar la comprobación de navegador web de Autotask

Las incompatibilidades de navegador web pueden causar problemas en la configuración de Autotask, como errores de Javascript.

Para comprobar si la configuración de su navegador web es compatible con Autotask, siga estos pasos.

PASO 1 Inicie sesión en Autotask.

PASO 2 Haga clic en **Help** > **Check My Browser Settings**.

PASO 3 Haga clic en **Begin Test**.

Tras ejecutar la prueba, los resultados le mostrarán lo que deba corregir.

PASO 4 Antes de continuar, compruebe que todas las marcas de compatibilidad son verdes.

Crear una cola de Service Desk para el portal

En Autotask, debe crear una cola de Service Desk denominada "OnPlus" y agregar a ella todos los usuarios (incluido el creador de la cola) como Resources (Recursos). Esto es necesario para que la cola OnPlus y sus vales aparezcan en la página de resumen y en las herramientas de navegación de Autotask.

IMPORTANTE La cola de Autotask Service Desk *debe* llamarse "OnPlus". De lo contrario, la integración no funcionará.

Para crear una cola en Autotask, siga estos pasos.

PASO 1 Haga clic en el icono **Admin** en la barra de herramientas de la parte superior de la ventana.

PASO 2 En el menú Admin de la izquierda, seleccione **Service Desk** > **Queues**.

PASO 3 Haga clic en **New** para crear una cola.

PASO 4 Denomine la cola **OnPlus**. Es importante denominarla OnPlus para que la integración funcione.

PASO 5 Escriba una descripción y haga clic en **Save**.

A continuación, debe agregar el usuario de Autotask que recibirá los vales generados por el portal OnPlus como Resource para la cola OnPlus en Autotask. Posteriormente, asociará el mismo usuario con la aplicación Autotask configurada en el portal OnPlus.

Para agregar un usuario como recurso, siga estos pasos.

PASO 1 Haga clic con el botón derecho del ratón en la entrada de cola OnPlus que acaba de crear y seleccione **Edit Queue Details**.

PASO 2 En el cuadro de diálogo Edit Queue Details, seleccione la ficha **Resources**, haga clic en **(+) New** y agregue el recurso.

Todos los vales de servicio asociados con la cuenta de OnPlus Portal de este usuario se crean a través de la API y se adjuntan a la cola OnPlus en Service Desk.

Modificar la política de flujo de trabajo para el tratamiento de vales duplicados

En Autotask, también debe modificar la política de flujo de trabajo para el tratamiento de vales duplicados, de modo que solo se considere un duplicado cuando se proporciona el mismo número de vale.

Para acceder a la configuración de la política de flujo de trabajo para el tratamiento de vales duplicados en Autotask, seleccione **Admin** > **Service Desk** > **Workflow Policies** y utilice el enlace [click here to edit] que se encuentra a la derecha de la opción Duplicate Ticket Handling.

En la sección **Duplicate Ticket Definition** del diálogo Duplicate Ticket Handling, desactive la opción **Any ticket with the same alert ID as an existing ticket**.

NOTA Las categorías de prioridad de los vales son totalmente personalizables en Autotask. Sin embargo, puesto que Autotask no necesita una prioridad de vale predeterminada y que actualmente hay un defecto abierto asociado con pasar información de prioridad de vale a través de la API de integración de servicios, Cisco OnPlus Portal establece la prioridad seleccionando la prioridad de vale con el valor más alto.

Comprobar la configuración de las políticas de flujo de trabajo para los campos obligatorios

Si su administrador de Autotask ha creado políticas de flujo de trabajo, debe asegurarse de que los campos adicionales (ya sean campos estándar de Autotask o campos personalizados) que estén marcados como obligatorios solo lo son en la aplicación y no en la API de servicios web. De lo contrario, no podrán crearse vales de servicio de Autotask a través de OnPlus Portal.

Para asegurarse de que los campos marcados como obligatorios a través de las políticas de flujo de trabajo de administración solo lo sean para la aplicación, vaya a **Admin** > **Service Desk** > **Dashboard** > **Workflow Policies** y compruebe que todas las políticas de campos obligatorios están marcadas como **Only required in Autotask application**. Estos son dos ejemplos:

- **Require Issue and Sub-Issue Type fields for service desk tickets** debe establecerse como **Only required in Autotask application**.
- **Require Work Type Name field for service desk tickets** debe establecerse como **Only required in Autotask application**.

Crear una cuenta de cliente en Autotask

Asegúrese de que ha creado una cuenta para su cliente en Autotask. Para crear una cuenta nueva, seleccione **Directory > Account** y haga clic en el botón **+ New Account** .

El nombre de cuenta que introduzca en Autotask debe coincidir con el nombre de cuenta que introduzca al agregar el servicio Autotask en Cisco OnPlus Portal.

Configuración de los ajustes de Cisco OnPlus Portal

Siga las indicaciones de esta sección para configurar los ajustes de Cisco OnPlus Portal, de modo que permita la integración de la creación de vales de servicio de Autotask:

- **Crear un contacto de entrega para la creación de vales de Autotask**
- **Agregar y configurar la aplicación Autotask en el portal**
- **Crear una regla de entrega para el cliente en OnPlus Portal**

Crear un contacto de entrega para la creación de vales de Autotask

Antes de agregar el servicio Autotask, debe tener un contacto de entrega global para el envío de notificaciones a Autotask.

- Puede utilizar un contacto global existente, sin embargo, es recomendable crear un contacto que se utilice específicamente para la creación de vales de Autotask. El contacto de Autotask es un contacto global que se utiliza para todos sus clientes que tengan instalada la aplicación Autotask.
- Debe crear el contacto antes de agregar la aplicación y configurar las reglas de entrega de notificaciones que utilizará el contacto de Autotask.

Para crear un nuevo contacto de entrega, siga estos pasos.

PASO 1 Acceda a la página de información general de la cuenta de partner y seleccione **Notificaciones** > **Contactos de envío**.

IMPORTANTE Al crear un contacto de entrega para Autotask, asegúrese de que el campo **Cliente** en el diálogo Agregar contacto de entrega está configurado como **Ninguno**, para convertirlo en contacto global.

PASO 2 Complete los campos obligatorios.

PASO 3 Haga clic en **Guardar**.

Agregar y configurar la aplicación Autotask en el portal

Debe agregar y configurar la aplicación Autotask para cada cliente al que quiera permitir generar vales de Autotask Service Desk automáticamente. Estos vales se basan en los eventos y notificaciones que se generan a través del portal.

Mediante esta serie de pasos, será capaz de:

- Instalar la aplicación Autotask en la cuenta de un cliente en el portal.
- Asociar las credenciales de inicio de sesión en Autotask del usuario "recurso" para la cola OnPlus de Autotask que acaba de crear al contacto de entrega que ha creado para Autotask en el portal.
- Introducir el ID único para este cliente (ID de cuenta).

Para agregar y configurar la aplicación Autotask de un cliente en Cisco OnPlus Portal, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, seleccione un cliente para el que desee configurar la creación de vales de servicio de Autotask y seleccione **Aplicaciones**.

PASO 2 En Todas las aplicaciones, localice la aplicación **Autotask** y haga clic en **GRATUITO**.

Aparece el diálogo **Agregar aplicación**.

PASO 3 En la sección **Información de cuentas global** del diálogo Agregar aplicación:

- Especifique el Nombre de usuario y la Contraseña para el usuario Autotask Resource asociado con la cola OnPlus Service Queue.
- En la sección **Asociar a un contacto**, seleccione el contacto que ha creado para utilizarlo con la aplicación Autotask.

  IMPORTANTE Una vez configurada esta información de cuentas global para un cliente, se utiliza para todos los clientes que tengan habilitada la aplicación Autotask.

Si ha agregado la aplicación Autotask con anterioridad, haga clic en la opción **Hacer cambios** para poder editar los campos.

PASO 4 Introduzca el ID de cuenta en el campo correspondiente, si lo conoce.

NOTA El ID de cuenta es un identificador interno que no se muestra en la interfaz gráfica de usuario de Autotask. Puede obtener el ID de cuenta haciendo una búsqueda en el Nombre de la empresa.

PASO 5 Si no conoce el ID de cuenta de Autotask, haga clic en **Buscar**.

PASO 6 En el campo **Nombre de cuenta**, introduzca el nombre de la cuenta exactamente como se especifica en Autotask. El nombre distingue entre mayúsculas y minúsculas. El nombre se utiliza para localizar el ID de cuenta de Autotask asociado que utiliza la API.

El campo **Nombre de cuenta** aparece ya definido con el Nombre del cliente especificado para ese cliente en Cisco OnPlus Portal.

Se muestran las parejas de nombre de cuenta e ID de cuenta de Autotask que coinciden (o comienzan) con el Nombre de la empresa especificado.

Si fuera necesario, utilice de nuevo el botón **Buscar** para volver a intentar la búsqueda.

PASO 7 Haga clic en el botón **Agregar** en la parte inferior de la ventana para aplicar la configuración.

Si la aplicación se agrega correctamente, la aplicación Autotask se mueve a la sección Instalado.

Las credenciales de usuario de Autotask están vinculadas al contacto especificado en el **PASO 3** más arriba. Se agrega un método de entrega de Autotask a la información de contacto, de modo que puede habilitar o deshabilitar la creación de vales de servicio. Está habilitado la primera vez que asocia el contacto y agrega la aplicación.

Crear una regla de entrega para el cliente en OnPlus Portal

Para comenzar a generar vales de servicio de forma remota, debe crear una regla de entrega de notificaciones para especificar los eventos que generarán un vale de servicio de Autotask y seleccionar el contacto de Autotask configurado como destino para la regla de entrega.

Asegúrese de que ha configurado monitores de dispositivos, de modo que se generen eventos para el tipo de condiciones que quiera utilizar para crear vales de servicio. Por ejemplo, es posible que quiera supervisar y crear vales para eventos del tipo Dispositivo: sin conexión o eventos con un nivel de gravedad determinado.

Siga estos pasos al crear reglas de notificación para la creación de vales de servicio de Autotask.

PASO 1 Inicie sesión en Cisco OnPlus Portal y seleccione **Notificaciones** > **Reglas de envío**.

PASO 2 Haga clic en el botón **+ Agregar regla de entrega**.

PASO 3 Seleccione un cliente de la lista desplegable.

PASO 4 Puede seleccionar un nivel de gravedad o especificar el tipo de evento que generará la creación de un vale de servicio de Autotask.

PASO 5 En el campo **Contacto**, seleccione el contacto asociado con la aplicación Autotask. Si necesita buscar el contacto que se utiliza para Autotask, puede ver los detalles de configuración de Autotask en la página Aplicaciones en Cisco OnPlus Portal.

PASO 6 Una vez seleccionado el contacto, seleccione el usuario de Autotask en el menú desplegable **Método**. El usuario de Autotask se identifica en la lista por el formato "<*nombre de usuario*> (Autotask)".

Si ninguno de los métodos se muestra en la lista con este formato, significa que ha seleccionado un contacto incorrecto.

PASO 7 Haga clic en **Guardar**.

Generación de eventos, notificaciones y vales de servicio de prueba

Siga estos pasos si desea:

- Crear una regla de entrega de ejemplo.
- Asociar esa regla a su contacto y método de entrega de Autotask.
- Utilizar la función Probar monitor para generar un evento que responda a los criterios de notificaciones de eventos especificados en la regla de entrega.
- Comprobar que la notificación del evento se ha enviado a Autotask.

Para generar un evento, notificación y ticket de servicio de prueba, siga estos pasos.

PASO 1 Inicie sesión en Cisco OnPlus Portal y seleccione **Notificaciones** > **Reglas de envío**.

PASO 2 Haga clic en el botón **+ Agregar regla de entrega**.

PASO 3 En el menú desplegable **Cliente**, seleccione Todo en la lista desplegable.

PASO 4 Para el nivel de **Gravedad**, seleccione **Advertencia**.

PASO 5 Para **Contacto**, seleccione el contacto de entrega de Autotask.

PASO 6 En **Método**, seleccione el método de entrega que haya definido para el contacto de entrega de Autotask.

PASO 7 Haga clic en **Guardar**.

PASO 8 En el menú Descripción general, haga clic en uno de sus clientes Activado, En línea que tenga instalada la aplicación Autotask.

PASO 9 En la vista Topología, localice el dispositivo OnPlus Network Agent del cliente y abra la ventana Información de dispositivo.

PASO 10 En la ventana Información de dispositivo de OnPlus Network Agent, haga clic en la ficha Monitores.

El primer monitor de la lista es el monitor Rendimiento de red WAN.

PASO 11 Haga clic en el icono **Probar monitor**, que se encuentra a la derecha del monitor Rendimiento de red WAN.

PASO 12 Habilite la opción **Generar un evento**.

PASO 13 Haga clic en **Ejecutar**. El evento de prueba generará una notificación porque la prueba genera un evento con nivel Advertencia (el nivel de gravedad predeterminado del evento Monitor WAN Network es Advertencia).

PASO 14 Espere unos minutos antes de volver a la página Descripción general y seleccione **Notificaciones** > **Reglas de envío**.

PASO 15 Localice la regla de entrega que creó para la prueba de Autotask.

- Compruebe la columna **Envío de notificaciones** para ver si el número ha aumentado.
- Haga clic en el número de la columna **Envío de notificaciones** para ver los detalles del evento.
- Compruebe que el evento de prueba aparece en la lista. Puesto que se acaba de generar, debería aparecer al principio de la lista. Si se encuentra, la notificación se ha enviado a Autotask.

Comprobación de la creación de vales de servicio en Autotask

Si la regla de entrega y la información de Autotask están configuradas correctamente para el cliente, cuando tenga lugar el evento y se genere el vale correctamente, aparecerá en la aplicación Autotask en **Service Desk > Queues - All Tickets > OnPlus**.

Resolución de vales automatizada (solo eventos de monitor de dispositivos)

Los vales de Autotask Service Desk que se crean a través de reglas de entrega de notificaciones basadas en monitores de dispositivos se resuelven automáticamente en Autotask cuando el monitor de dispositivos genera un evento de recuperación posterior. Esta función se aplica a todos los monitores de dispositivos excepto a Cambio de IP y Rendimiento de red WAN.

Por ejemplo, si ha creado una regla de entrega de notificaciones que crea un vale de Service Desk cuando el monitor de dispositivos detecta que el host supervisado está desactivado, se envía una notificación a Autotask y se crea un vale de Service Desk. Si el dispositivo se activa posteriormente, el vale de servicio de Autotask asociado con dicho evento se marca automáticamente como Completo y el campo Resolución muestra información sobre el evento de recuperación del dispositivo.

Suspensión de la generación de vales de servicio para todos los clientes

Para suspender temporalmente la generación de vales de servicio a través del portal para todos los clientes, siga estos pasos:

PASO 1 En la página de información general de la cuenta de partner, seleccione **Notificaciones** > **Contactos de envío**.

PASO 2 Seleccione el contacto asociado con la entrega de notificaciones de Autotask.

PASO 3 Haga clic en el botón **Habilitar** asociado con el contacto de Autotask para cambiar la configuración a **Deshabilitado**.

Puesto que el contacto de Autotask es un contacto global para todos los clientes que tengan la aplicación instalada, esta acción suspende la creación de vales de Autotask para todos esos clientes.

Actualización de la información de cuentas global

Para actualizar la información de cuentas global de Autotask (contacto Autotask o nombre de usuario y contraseña de Autotask), siga los pasos que se indican a continuación.

PASO 1 En la página de información general de la cuenta de partner, seleccione un cliente que tenga habilitada la aplicación Autotask y seleccione **Aplicaciones**.

PASO 2 En la lista de aplicaciones **instaladas**, localice la aplicación Autotask y haga clic en **Editar**.

PASO 3 Para cambiar la información de cuentas global, haga clic en la opción **Hacer cambios** para poder editar los campos.

PASO 4 Realice los cambios.

PASO 5 Haga clic en **Actualizar**.

Los cambios se aplican a todos los clientes que tengan instalada la aplicación Autotask.

Eliminación de la aplicación Autotask de un cliente

Para eliminar la aplicación Autotask de un cliente específico, lleve a cabo los siguientes pasos.

PASO 1 En la página de información general de la cuenta de partner, seleccione el cliente y haga clic en **Aplicaciones**.

PASO 2 En la lista de aplicaciones instaladas, localice el icono de Autotask y haga clic en **Quitar**.

PASO 3 Haga clic en **Aceptar** para confirmar la acción.

Problemas conocidos

Los siguientes problemas conocidos están relacionados con la integración de Autotask con Cisco OnPlus Portal:

- Algunos cambios que pueden realizarse mediante la interfaz gráfica de usuario de Autotask (por ejemplo, la configuración de un nivel de prioridad de los vales como predeterminado) no pueden hacerse con la API.
- Al consultar el ID de cuenta mediante la API con un nombre de empresa parcial, si dos o más clientes coinciden con la cadena proporcionada, solo se muestra un resultado (en lugar de la lista completa de resultados). Esto implica que el agente deba incluir caracteres suficientes para garantizar una coincidencia única.

16

Integración de la creación de vales de servicio de ConnectWise

En esta sección se explica cómo configurar los ajustes de la aplicación ConnectWise PSA (Professional Service Automation) y Cisco OnPlus Portal de modo que puedan crearse automáticamente vales de servicio de ConnectWise basados en los eventos que se supervisan a través de Cisco OnPlus Portal.

Se tratan los siguientes temas:

- **Compatibilidad de la versión de ConnectWise**
- **Configuración de los ajustes de ConnectWise**
- **Configuración de los ajustes de Cisco OnPlus Portal**
- **Generación de eventos, notificaciones y vales de servicio de prueba**
- **Comprobación de la creación de vales de servicio en ConnectWise**
- **Resolución de vales automatizada (solo eventos de monitor de dispositivos)**
- **Suspensión de la generación de vales de servicio para todos los clientes**
- **Actualización de la información de cuentas global**
- **Eliminación de la aplicación ConnectWise de un cliente**

Compatibilidad de la versión de ConnectWise

La versión 2011.2 (10667) de ConnectWise se ha probado con Cisco OnPlus Portal. Para obtener más información, consulte www.connectwise.com.

IMPORTANTE Al configurar la integración de ConnectWise, si utiliza un servidor autoalojado, su servidor ConnectWise debe tener SSL habilitado con un certificado firmado.

Configuración de los ajustes de ConnectWise

Siga las indicaciones de esta sección para configurar los ajustes de la aplicación ConnectWise, de modo que permita la integración con Cisco OnPLus Portal para la creación de vales de servicio:

- **Configuración del inicio de sesión de integradores en ConnectWise, en la página 198**
- **Configuración de un ID de la empresa en ConnectWise para cada cliente, en la página 199**

Configuración del inicio de sesión de integradores en ConnectWise

Los administradores de ConnectWise PSA pueden asignar permisos a los integradores. El administrador de PSA debe configurar un nombre de usuario y una contraseña maestros, y permitir a los integradores acceder a las API.

Se puede permitir que los integradores accedan a todos los objetos o únicamente a aquellos que hayan creado ellos mismos.

Para ConnectWise, estos permisos se establecen desde la página de configuración de Integrator Login en el área Setup Tables.

Realice los siguientes pasos para otorgar permisos de integrador para Cisco OnPlus.

PASO 1 Inicie sesión en ConnectWise y vaya a **Setup > Setup Tables**.

PASO 2 Filtre la lista para mostrar la categoría **General** y, a continuación, haga clic en **Integrator Login**.

PASO 3 Configure los siguientes ajustes en la página Integrator Login:

- En los campos **Username y Password**, escriba el nombre de usuario y la contraseña que se utilizarán para iniciar sesión en su sitio de ConnectWise.
- Establezca **Access Level** en "Records created by integrator".

PASO 4 En Enable Available APIs, especifique estos valores:

- Active la opción **Service Ticket API**.
- En Service Ticket API, establezca **Service Board** en "Professional Services".
- Active la opción **Company API**. No se requiere ningún parámetro.
- En **Ticket Callback URL**, escriba https://www.cisco-onplus.com.

PASO 5 Haga clic en **Guardar**.

Configuración de un ID de la empresa en ConnectWise para cada cliente

Para poder crear solicitudes de vales de ConnectWise automáticamente desde OnPlus Portal, debe configurar un ID de la empresa en el cliente ConnectWise para cada uno de sus clientes de Cisco OnPlus Portal para los que desee habilitar esta función.

Para crear una empresa en ConnectWise, vaya a **Contacts > Company** y haga clic en el icono **New Item**.

Para buscar un cliente existente, vaya a **Contacts** > **Company** y haga clic en el botón **Search**.

Asegúrese de que se ha configurado un ID de la empresa para cada uno de sus clientes. Consulte la documentación de ConnectWise para obtener más información sobre esta configuración.

Registre el ID de la empresa de cada cliente, pues deberá introducirlo en el servicio ConnectWise en Cisco OnPlus Portal.

Configuración de los ajustes de Cisco OnPlus Portal

Siga las indicaciones de esta sección para configurar los ajustes de Cisco OnPlus Portal, de modo que permita la integración con ConnectWise para la creación de vales de servicio:

- **Cómo crear un contacto de entrega para la creación de vales de ConnectWise**
- **Cómo agregar y configurar la aplicación ConnectWise en el portal**
- **Creación de reglas de entrega para la generación de vales de ConnectWise**

Cómo crear un contacto de entrega para la creación de vales de ConnectWise

Antes de agregar la aplicación ConnectWise, debe crear un contacto de entrega global para el envío de notificaciones a ConnectWise.

- Puede utilizar un contacto existente, sin embargo, es recomendable crear un contacto que se utilice específicamente para la creación de vales de ConnectWise. El contacto de ConnectWise es un contacto global que se utiliza para todos sus clientes que tengan instalada la aplicación ConnectWise.

- Debe crearse siempre el contacto global antes de agregar la aplicación y configurar las reglas de entrega de notificaciones que utilizará el contacto.
- Para crear un contacto de entrega global, acceda a la página de información general de la cuenta de partner y seleccione **Notificaciones** > **Contactos de envío**. Complete los campos obligatorios y haga clic en **Guardar**.

IMPORTANTE Al crear un contacto de entrega para ConnectWise, asegúrese de que el campo **Cliente** del diálogo Agregar contacto de entrega está configurado como **Ninguno** para convertirlo en contacto global.

Cómo agregar y configurar la aplicación ConnectWise en el portal

Para agregar y configurar la integración de ConnectWise para un cliente, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, seleccione un cliente para el que desee configurar la aplicación ConnectWise y seleccione **Aplicaciones**.

PASO 2 En **Todo**, localice la aplicación **ConnectWise** y haga clic en **Gratuito**.

Aparece la ventana de diálogo **Agregar aplicación**.

PASO 3 En la sección **Información de cuentas global**, introduzca la siguiente información:

NOTA Si ha agregado la aplicación ConnectWise con anterioridad, active la opción **Hacer cambios** para poder editar los campos.

- **ID del sitio**: el ID del sitio de ConnectWise (por ejemplo, prueba.connectwise.com). Esta URL debe proporcionarla ConnectWise.
- **ID corporativo**: los datos de inicio de sesión de cuenta de ConnectWise (el valor que introduce en el campo ID de la empresa cuando inicia sesión en ConnectWise).
- **Nombre de usuario, Contraseña**: el nombre de usuario y la contraseña de ConnectWise.

  Se trata del nombre de usuario y la contraseña que configuró en Integrator Login en ConnectWise. Son las credenciales que utilizará al iniciar sesión en el sitio de ConnectWise.
- En el área **Asociar a un contacto**, seleccione un contacto que desee asociar con la aplicación ConnectWise en el portal.

Una vez configurada la **Información de cuentas global** para un cliente, se utiliza para todos los clientes que tengan habilitada la aplicación ConnectWise.

PASO 4 En el campo **ID de la empresa**, introduzca el ID de la empresa de ConnectWise que configuró en ConnectWise (**Contacts > Company**).

PASO 5 Haga clic en **Agregar**.

Si la aplicación se agrega correctamente, ConnectWise aparece en la lista de aplicaciones instaladas.

Las credenciales de usuario de ConnectWise están vinculadas al contacto especificado en el diálogo Agregar aplicación.

Se agrega un método de entrega de ConnectWise a la información del contacto, de modo que puede habilitar o deshabilitar la creación de vales de servicio. Está habilitado la primera vez que asocia el contacto y agrega la aplicación.

Creación de reglas de entrega para la generación de vales de ConnectWise

Para comenzar a generar vales de servicio de forma remota, debe crear una regla de entrega de notificaciones para especificar los eventos que generarán un vale de servicio de ConnectWise y seleccionar el contacto de ConnectWise configurado como destino para la regla de entrega.

Asegúrese de que ha configurado monitores de dispositivos, de modo que se generen eventos para el tipo de condiciones que quiera utilizar para crear vales de servicio. De forma predeterminada, solo se supervisa Cisco OnPlus Network Agent. Por ejemplo, es posible que quiera supervisar y crear vales para eventos del tipo Dispositivo: sin conexión o eventos con un nivel de gravedad determinado.

Siga estos pasos al crear reglas de notificación para la creación de vales de servicio de ConnectWise.

PASO 1 Inicie sesión en Cisco OnPlus Portal y seleccione **Notificaciones** > **Reglas de envío**.

PASO 2 Haga clic en el botón **+ Agregar regla de entrega**.

PASO 3 Seleccione un cliente de la lista desplegable.

PASO 4 Puede seleccionar un nivel de gravedad o especificar el tipo de evento que generará la creación de un vale de servicio de ConnectWise.

PASO 5 En el campo **Contacto**, seleccione el contacto asociado con la aplicación ConnectWise. Si necesita buscar el contacto que se utiliza para ConnectWise, puede ver los detalles de configuración de ConnectWise en la página Aplicaciones en el portal.

PASO 6 Una vez seleccionado el contacto, seleccione el usuario de ConnectWise en el menú desplegable **Método**. El usuario de ConnectWise se identifica en la lista por el formato "<*nombre de usuario*> (ConnectWise)".

Si ninguno de los métodos de la lista muestra esta información, significa que seleccionó un contacto que no está asociado con el usuario de ConnectWise.

PASO 7 Haga clic en **Guardar**.

Generación de eventos, notificaciones y vales de servicio de prueba

Siga estos pasos si desea:

- Crear una regla de entrega de ejemplo.
- Asociar esa regla a su contacto y método de entrega de ConnectWise.
- Utilizar la función Probar monitor para generar un evento que responda a los criterios de notificaciones de eventos especificados en la regla de entrega.
- Comprobar que la notificación del evento se ha enviado a ConnectWise.

Para generar un evento, notificación y ticket de servicio de prueba, siga estos pasos.

PASO 1 Inicie sesión en Cisco OnPlus Portal y seleccione **Notificaciones** > **Reglas de envío**.

PASO 2 Haga clic en el botón **+ Agregar regla de entrega**.

PASO 3 En el menú desplegable **Cliente**, seleccione **Todo** en la lista desplegable.

PASO 4 Para el nivel de **Gravedad**, seleccione **Advertencia**.

PASO 5 Para **Contacto**, seleccione el contacto de entrega de ConnectWise.

PASO 6 En **Método**, seleccione el método de entrega que haya definido para el contacto de entrega de ConnectWise.

PASO 7 Haga clic en **Guardar**.

PASO 8 En el menú Descripción general, haga clic en uno de sus clientes Activado, En línea que tenga instalada la aplicación ConnectWise.

PASO 9 En la vista Topología, localice el dispositivo OnPlus Network Agent del cliente y abra la ventana Información de dispositivo.

PASO 10 En la ventana Información de dispositivo de OnPlus Network Agent, haga clic en la ficha Monitores.

El primer monitor de la lista es el monitor Rendimiento de red WAN.

PASO 11 Haga clic en el icono **Probar monitor**, que se encuentra a la derecha del monitor Rendimiento de red WAN.

PASO 12 Habilite la opción **Generar un evento**.

PASO 13 Haga clic en **Ejecutar**. El evento de prueba generará una notificación porque la prueba genera un evento con nivel Advertencia (el nivel de gravedad predeterminado del evento Monitor WAN Network es Advertencia).

PASO 14 Espere unos minutos antes de volver a la página Descripción general y seleccione **Notificaciones** > **Reglas de envío**.

PASO 15 Localice la regla de entrega que creó para la prueba de ConnectWise.

- Compruebe la columna **Envío de notificaciones** para ver si el número ha aumentado según lo esperado.
- Haga clic en el número de la columna **Envío de notificaciones** para ver los detalles del evento.
- Compruebe que el evento de prueba aparece en la lista de eventos. Puesto que se acaba de generar, debería aparecer al principio de la lista. Si se encuentra, la notificación se ha enviado a ConnectWise.

Comprobación de la creación de vales de servicio en ConnectWise

Si la regla de entrega y la información de ConnectWise están configuradas correctamente para el cliente, cuando tenga lugar el evento y se genere el vale correctamente, aparecerá en la aplicación ConnectWise en **Service Desk** > **Service Board**.

Resolución de vales automatizada (solo eventos de monitor de dispositivos)

Los vales de ConnectWise Service Desk que se crean a través de reglas de entrega de notificaciones basadas en monitores de dispositivos se resuelven automáticamente en ConnectWise cuando el monitor de dispositivos genera un evento de recuperación posterior. Esta función se aplica a todos los monitores de dispositivos excepto a Cambio de IP y Rendimiento de red WAN.

Por ejemplo, si ha creado una regla de entrega de notificaciones que crea un vale de Service Desk cuando el monitor de dispositivos detecta que el host supervisado está desactivado, se envía una notificación a ConnectWise y se crea un vale de Service Desk. Si el dispositivo se activa posteriormente, el vale de servicio de ConnectWise asociado con dicho evento se marca automáticamente como Completo y el campo Resolución muestra información sobre el evento de recuperación del dispositivo.

Suspensión de la generación de vales de servicio para todos los clientes

Para suspender temporalmente la generación de vales de servicio a través del portal para todos los clientes, siga estos pasos:

PASO 1 En la página de información general de la cuenta de partner, seleccione **Notificaciones** > **Contactos de entrega**.

PASO 2 Seleccione el contacto asociado con la entrega de notificaciones de ConnectWise.

PASO 3 Haga clic en el botón **Habilitar** asociado con el contacto de ConnectWise para cambiar la configuración a **Deshabilitado**.

Puesto que el contacto de ConnectWise es un contacto global para todos los clientes que tengan la aplicación instalada, esta acción suspende la creación de vales de ConnectWise para todos esos clientes.

Actualización de la información de cuentas global

Para actualizar la información de cuentas global de ConnectWise, siga estos pasos.

PASO 1 En la página de información general de la cuenta de partner, seleccione un cliente que tenga habilitada la aplicación ConnectWise y seleccione **Aplicaciones**.

PASO 2 En la lista de aplicaciones instaladas, localice la aplicación ConnectWise y haga clic en **Editar**.

PASO 3 Para modificar la información de cuentas global, haga clic en la opción **Hacer cambios** para poder editar los campos.

PASO 4 Realice los cambios.

PASO 5 Haga clic en **Actualizar**. Los cambios se aplican a todos los clientes que tengan instalada la aplicación ConnectWise.

Eliminación de la aplicación ConnectWise de un cliente

Para eliminar la aplicación ConnectWise de un cliente específico, lleve a cabo los siguientes pasos.

PASO 1 En la página de información general de la cuenta de partner, seleccione el cliente y haga clic en **Aplicaciones**.

PASO 2 En la lista de aplicaciones instaladas, localice la aplicación ConnectWise y haga clic en **Quitar**.

PASO 3 Haga clic en **Aceptar** para confirmar la acción.

17

Habilitar la aplicación Supervisión de paquetes ntop

Esta sección incluye instrucciones para habilitar la aplicación Supervisión de paquetes ntop en Cisco OnPlus Portal y configurar la supervisión de paquetes a través de NetFlow o puertos SPAN (Switch Port Analyzer), con envío del tráfico al puerto MON de OnPlus Network Agent.

NOTA Actualmente ntop es una función beta.

Se tratan los siguientes temas:

- **Descripción general**
- **Notas, limitaciones y advertencias**
- **Agregar la aplicación ntop a Cisco OnPlus Portal**
- **Uso de ntop con NetFlow**
- **Eliminación de la aplicación Supervisión de paquetes ntop**

Descripción general

ntop es una sonda de tráfico de red que analiza el uso de la red. Para obtener más información, visite www.ntop.org.

La aplicación ntop se descarga en OnPlus Network Agent y se accede a ella desde el portal. No es necesario descargar el software de la aplicación ntop.

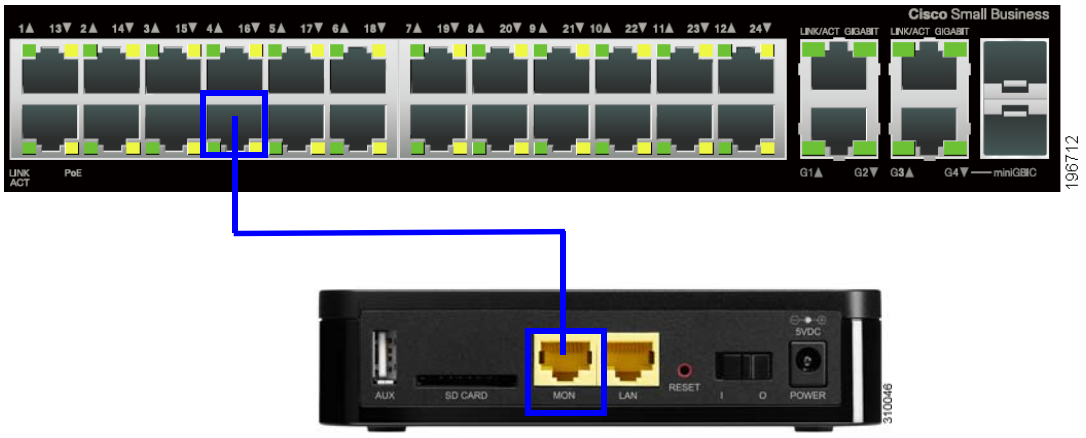
Hay dos métodos compatibles para recopilar información de la red y utilizarla con ntop:

- **SPAN**. Usando el puerto MON de OnPlus Network Agent como puerto de entrada, puede utilizar ntop para analizar el tráfico en el que está interesado. Al supervisar el tráfico del puerto span, debe proporcionar el origen del tráfico de red que se va a examinar. Algunos switches y routers

tienen la capacidad de desviar el tráfico a un puerto específico. Si tiene un tap de red o un concentrador de red simple, puede utilizarlo para acceder a la red en la que quiere controlar el tráfico.

Consulte la documentación del dispositivo que esté utilizando para ver instrucciones sobre la configuración de puertos span.

El siguiente diagrama muestra la conexión entre un puerto span de un switch de la serie 300 de Cisco Small Business y el puerto MON del panel posterior de Cisco OnPlus Network Agent.



- **NetFlow (IPFIX).** La mayoría de los routers Cisco IOS admite el protocolo NetFlow. En ese caso, sólo tiene que habilitar el protocolo en el router y dirigirlo al dispositivo OnPlus Network Agent. El protocolo NetFlow utiliza menos recursos de CPU en OnPlus Network Agent y no requiere el uso del puerto MON.

  Si utiliza NetFlow, se recomienda asignar una dirección IP estática o una asignación DHCP estática a OnPlus Network Agent, puesto que la configuración de NetFlow utiliza la dirección IP de OnPlus Network Agent. Además, debe estar activado NetFlow en ntop y el número de puerto al que escucha debe coincidir con la configuración de NetFlow del router IOS.

  Consulte **Uso de ntop con NetFlow, en la página 211**.

Notas, limitaciones y advertencias

Estas notas, limitaciones y advertencias se aplican al uso de la aplicación ntop con Cisco OnPlus Network Agent:

- OnPlus Network Agent no permite exportar datos ni escribir datos en el disco.
- Se recomienda el uso de una dirección IP estática para OnPlus Network Agent al utilizar NetFlow.
- OnPlus Portal establece **admin/admin** como el nombre de usuario y la contraseña iniciales de ntop.
- Algunos cambios en la configuración de la aplicación ntop (por ejemplo, las modificaciones de los ajustes que configuran la capacidad de acceso) pueden provocar que la aplicación ntop deje de funcionar o no lo haga correctamente.
- Si tiene problemas al utilizar la aplicación ntop con OnPlus Portal, elimine el servicio para agregarlo y habilitarlo de nuevo.
- Una vez eliminada y agregada de nuevo la aplicación, o después de instalar una nueva versión de ntop en OnPlus Network Agent a través de OnPlus Portal:
  - Se pierden todos los datos anteriores.
  - Se pierden los ajustes personalizados de la aplicación ntop.
  - La contraseña se restablece a la predeterminada (admin/admin).
- La aplicación ntop se reinicia automáticamente al reiniciar OnPlus Network Agent.
- Cuando utiliza la opción **Admin** > **Shutdown** de la herramienta de administración de ntop basada en la web, ntop se reinicia automáticamente. Elimine el servicio ntop a través de OnPlus Portal si no desea que se ejecute la aplicación.

Agregar la aplicación ntop a Cisco OnPlus Portal

Siga las indicaciones de esta sección para configurar los ajustes de Cisco OnPlus Portal para que admita la aplicación Supervisión de paquetes ntop:

- **Instalación de la aplicación Supervisión de paquetes ntop en OnPlus Network Agent**
- **Inicio de la aplicación Supervisión de paquetes ntop**

Instalación de la aplicación Supervisión de paquetes ntop en OnPlus Network Agent

Debe agregar y configurar la aplicación ntop para cada cliente.

Para agregar y habilitar la función de supervisión de paquetes de ntop para un cliente, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, seleccione un cliente para el que desee habilitar la aplicación Supervisión de paquetes ntop y seleccione **Aplicaciones**.

PASO 2 En Todas las aplicaciones, localice la aplicación **Supervisión de paquetes ntop** y haga clic en **GRATUITO**.

Aparece el diálogo **Agregar aplicación**.

PASO 3 Haga clic en **Agregar**.

La aplicación se descarga en OnPlus Network Agent y se inicia. Si la aplicación se agrega correctamente, la aplicación ntop se mueve a la sección **Instalado**.

Continúe con la siguiente sección, **Inicio de la aplicación Supervisión de paquetes ntop**.

Inicio de la aplicación Supervisión de paquetes ntop

Para iniciar ntop, siga estos pasos.

PASO 1 En el portal, en la página Descripción general, seleccione un cliente que tenga instalada la aplicación Supervisión de paquetes ntop.

PASO 2 Seleccione **Aplicaciones**.

PASO 3 Haga clic en **Instalado**.

PASO 4 Entre las aplicaciones instaladas, localice la aplicación **Supervisión de paquetes ntop** y haga clic en **Detalles**.

Si acaba de instalar la aplicación, es posible que vea un mensaje que indica que la opción de iniciar el portal de ntop no está aún disponible. Cierre el diálogo y vuelva a intentarlo después de unos minutos.

Cuando finaliza la instalación de ntop, se activa el botón **Iniciar el portal de ntop**.

PASO 5 Para abrir el portal de ntop en una ventana nueva, haga clic en **Iniciar el portal de ntop**.

La alimentación de red que desee utilizar para el origen del tráfico debe estar conectada (puerto span) o configurada (NetFlow) para poder recopilar datos útiles.

Si está utilizando NetFlow, consulte **Uso de ntop con NetFlow** para conocer los pasos de configuración adicionales.

Uso de ntop con NetFlow

Para utilizar ntop con NetFlow configurado en un router IOS, siga los procedimientos que se señalan en las siguientes secciones:

- **Configuración de NetFlow en un dispositivo Cisco IOS**
- **Configuración de los ajustes de ntop**

Configuración de NetFlow en un dispositivo Cisco IOS

El modo NetFlow utiliza el puerto WAN de OnPlus Network Agent con un router Cisco configurado para dirigir el tráfico de NetFlow a la dirección IP de OnPlus Network Agent.

La siguiente secuencia de comandos IOS pueden utilizarse como modelo para configurar NetFlow. En el ejemplo, la dirección IP de `ip flow-export destination` es la dirección IP de OnPlus Network Agent.

`2055` en el ejemplo de comando `ip flow-export destination` se corresponde con el número de Local Collector UDP Port configurado para el complemento de NetFlow. La interfaz de `flow export source` variará en función de la interfaz que proporciona el tráfico de origen.

```
router#enable
Password:*****
router#configure terminal
router-2621(config)#interface FastEthernet 0/1
router-2621(config-if)#ip route-cache flow
router-2621(config-if)#exit
router-2621(config)#ip flow-export destination <OnPlus_Network
Agent_IP_Address> 2055
router-2621(config)#ip flow-export source FastEthernet 0/1
router-2621(config)#ip flow-export version 5
router-2621(config)#ip flow-cache timeout active 1
router-2621(config)#ip flow-cache timeout inactive 15
router-2621(config)#snmp-server ifindex persist
router-2621(config)#^Z
router#write
```

Configuración de los ajustes de ntop

Si está utilizando NetFlow, debe realizar los siguientes pasos de configuración adicionales con la aplicación ntop:

PASO 1 Abra la aplicación ntop desde OnPlus Portal:

a. Inicie sesión en Cisco OnPlus Portal y seleccione su cliente.

b. Seleccione **Aplicaciones**.

c. Haga clic en **Instalado** y localice la aplicación Supervisión de paquetes ntop.

d. Haga clic en **Detalles**.

e. Haga clic en **Iniciar el portal de ntop**.

PASO 2 Cuando se le solicite realizar la autenticación, introduzca el nombre de usuario y la contraseña de administración predeterminados.

Nombre de usuario: **admin**
Contraseña: **admin**

NOTA Cuando se instala o actualiza ntop en OnPlus Network Agent, la contraseña se restablece siempre a la predeterminada.

PASO 3 Active el complemento de NetFlow. Para ello, seleccione **Plugins** > **NetFlow** > **Activate**.

PASO 4 Cree un dispositivo NetFlow. En la aplicación ntop, seleccione **Plugins** > **NetFlow** > **Configure** y haga clic en **Add NetFlow Device**.

PASO 5 Configure estos ajustes para el dispositivo NetFlow:

- **NetFlow Device**. Este ajuste es opcional, pero muy útil. Escriba el nombre de la interfaz y haga clic en **Set Device Interface Name**.
- **Local Collector UDP Port**. Introduzca el número de puerto y haga clic en **Set Port**. Este número de puerto debería corresponderse con el puerto *<Port>* configurado para el comando `ip flow-export destination` *<IP_address>* *<Port>* configurado en el router o switch.

PASO 6 Para poder ver el contenido de NetFlow, el dispositivo NetFlow debe estar seleccionado en **Admin** > **Switch NIC**.

Si no realiza este paso, podría estar examinando el tráfico en el puerto eth1 predeterminado en lugar de en el puerto NetFlow configurado en el dispositivo IOS.

Eliminación de la aplicación Supervisión de paquetes ntop

Para eliminar la aplicación Supervisión de paquetes ntop de un cliente específico, lleve a cabo los siguientes pasos.

PASO 1 En la página de información general de la cuenta de partner, seleccione el cliente y haga clic en **Aplicaciones**.

PASO 2 En la lista de aplicaciones instaladas, localice el icono de Supervisión de paquetes ntop y haga clic en **Quitar**.

PASO 3 Haga clic en **Aceptar** para confirmar la acción.

Al eliminar la aplicación, todos los datos anteriores y la configuración personalizada de ntop se pierde y la contraseña se restablece a la predeterminada (admin/admin).

18

Acceso de dispositivos móviles a OnPlus Portal

Este capítulo incluye instrucciones para acceder a Cisco OnPlus Portal desde dispositivos móviles:

- **Acceso a OnPlus Portal desde un dispositivo móvil, en la página 215**
- **Funciones de OnPlus Portal accesibles a través de la interfaz móvil, en la página 216**
- **Funciones no admitidas por la interfaz móvil, en la página 217**
- **Activación de un cliente desde un dispositivo móvil, en la página 218**

Acceso a OnPlus Portal desde un dispositivo móvil

Puede acceder al portal móvil de OnPlus desde a través del navegador web de un dispositivo móvil. El navegador web del dispositivo móvil debe ser compatible con JavaScript y CSS. El acceso móvil se ha probado con el navegador Safari en teléfonos inteligentes iPhone, Android y Blackberry (RIM) y en iPad.

Para acceder a OnPlus Portal desde un dispositivo móvil, siga estos pasos.

PASO 1 Abra un navegador web en el dispositivo móvil.

PASO 2 Acceda a la URL del portal (www.cisco-onplus.com). Se le redirigirá automáticamente a la URL del portal móvil (https://www.cisco-onplus.com/m).

PASO 3 Escriba su nombre de usuario y la contraseña del portal y haga clic en **Iniciar sesión**.

PASO 4 Seleccione un cliente o uno de sus contactos de entrega.

Cuando selecciona un cliente, puede ver su panel o lista de dispositivos y acceder a los detalles de cada dispositivo.

Para actualizar los datos de una página del portal móvil de Cisco OnPlus, actualice la página en el navegador web del dispositivo móvil.

Para ver las opciones de conexión remota a un dispositivo, seleccione Lista de dispositivos y, a continuación, seleccione el dispositivo. Los tipos de conexiones que se pueden establecer con el dispositivo se incluyen en **Establecer conexión**.

PASO 5 Para cerrar la sesión, desplácese hasta el final de cualquier página del portal móvil y haga clic en el enlace **Cierre de sesión**.

Siempre puede hacer clic en el enlace Sitio no destinado a móviles en la parte inferior de la página para iniciar sesión en el portal a través de la interfaz web habitual.

Funciones de OnPlus Portal accesibles a través de la interfaz móvil

La interfaz móvil de Cisco OnPlus Portal proporciona acceso a muchas de las importantes funciones del portal para supervisar las redes de sus clientes y acceder a ellas. Desde dispositivos móviles compatibles, puede:

- Ver una lista de todos sus clientes.
- Seleccionar un cliente para ver su topología de red o ver una lista de dispositivos de la red.
- Utilizar los controles de la pantalla táctil para desplazarse lateralmente y ampliar la vista Topología o seleccionar dispositivos.
- Seleccionar dispositivos para ver información o realizar acciones. Las acciones disponibles pueden variar, en función del tipo de dispositivo.
  - Establecer una conexión web, de escritorio remoto o VNC al dispositivo de un cliente.

    NOTA Antes de intentar establecer una conexión remota a dispositivos mediante el portal móvil, debe configurar sus ajustes de conexión en el dispositivo remoto y en la ficha Conectar de la ventana Información de dispositivo del portal. Consulte **Conexión a dispositivos desde el portal, en la página 131**.

  - Reiniciar dispositivos.
  - Hacer copias de seguridad de la configuración para dispositivos de Cisco compatibles.
  - Activar el dispositivo OnPlus Network Agent del cliente a través del portal. Sólo puede hacer esto si el dispositivo móvil se encuentra en la misma red de área local (LAN) que el dispositivo OnPlus Network Agent que está activando.

    Consulte **Activación de un cliente desde un dispositivo móvil, en la página 218**.

- Ver el historial de eventos globales y filtrar por nivel de gravedad.
- Consultar los 10 últimos eventos registrados para cualquier dispositivo.
- Ver los contactos de entrega.

  Hacer clic en la dirección de correo electrónico o SMS de un contacto para enviar un mensaje.
- Ver la dirección de un cliente y la información de su ubicación.

  Si está accediendo al portal móvil desde un iPhone y tiene instalada la aplicación Google Maps, la dirección se muestra automáticamente en la aplicación Google Maps.
  - En un teléfono Android, puede seleccionar entre mostrar el mapa en la aplicación Google Maps del teléfono o en el navegador web.
  - En un teléfono inteligente Blackberry, la información de la ubicación se abre en un navegador web.

Funciones no admitidas por la interfaz móvil

Las funciones de Cisco OnPlus Portal no compatibles con la interfaz móvil incluyen las siguientes:

- Agregar, eliminar, suspender o reanudar clientes
- Actualizar firmware en dispositivos que no sean OnPlus Network Agent
- Personalizar páginas del portal
- Agregar, editar o eliminar las credenciales de acceso a dispositivos

- Configurar ajustes de conexión remota para los dispositivos
- Agregar, eliminar o modificar los monitores de dispositivos
- Administrar agentes autorizados
- Generar, programar o visualizar informes
- Editar, eliminar, habilitar y deshabilitar contactos de entrega
- Visualizar o administrar reglas de entrega de notificaciones
- Configurar aplicaciones de integración de PSA (Autotask, ConnectWise) con OnPlus Portal

Activación de un cliente desde un dispositivo móvil

Si su dispositivo móvil tiene un navegador web y está conectado a la misma red de área local (LAN) o LAN inalámbrica (WLAN) que OnPlus Network Agent, puede utilizar la interfaz móvil para acceder al enlace **Activar ahora** en el portal y activar Network Agent.

PASO 1 Asegúrese de que ha completado todos los pasos anteriores al paso de activación. Consulte **Antes de empezar, en la página 21**.

PASO 2 En el dispositivo móvil conectado a la misma LAN que OnPlus Network Agent, inicie sesión en el portal móvil.

PASO 3 Seleccione el cliente que desee activar.

PASO 4 Haga clic en el enlace **Perfil** para acceder al perfil de ese cliente y a la información de activación.

PASO 5 Desplácese a la sección **OnPlus Network Agent** de la página.

PASO 6 Seleccione **Activar ahora** y siga las instrucciones en pantalla.

Si tiene problemas al utilizar la interfaz móvil para activar el cliente, siempre puede conectarse al portal mediante un navegador web en un equipo conectado a la LAN o WLAN y realizar la activación como lo haría normalmente.

19

Comentarios y soporte

Este capítulo incluye información sobre cómo acceder a la comunidad de soporte de Cisco OnPlus y cómo enviar comentarios sobre Cisco OnPlus Portal:

- **Comunidad de soporte de Cisco OnPlus**
- **Acceso de soporte a registros de OnPlus Network Agent y sitios de los clientes**
- **Comprobación del estado de OnPlus Service**
- **Envío de comentarios sobre Cisco OnPlus**

Comunidad de soporte de Cisco OnPlus

Desde OnPlus Portal, los partners de Cisco pueden acceder a los recursos de soporte de Cisco.com y al área de la comunidad de soporte de OnPlus.

Haga clic en el enlace **Soporte** en la parte superior de OnPlus Portal para acceder a la comunidad de soporte. La página de inicio de sesión de Cisco.com se muestra en el portal.

Al iniciar sesión en Cisco.com, se le redirige al área de OnPlus de la Comunidad de soporte de Cisco.

Acceso de soporte a registros de OnPlus Network Agent y sitios de los clientes

Los agentes del Centro de soporte para productos Cisco Small Business (SBSC) pueden recopilar registros de aplicaciones y resultados de tiempo de ejecución desde el dispositivo OnPlus Network Agent. Estos datos se recopilan con la aprobación del cliente durante llamadas de soporte activas. Los datos

recopilados se envían al personal de soporte de Cisco tal y como se han recogido durante la llamada. El acceso a estos datos está protegido por contraseña para uso exclusivo del personal de soporte de Cisco. El personal de soporte de Cisco debe tener su autorización explícita para utilizar esta función.

Se puede acceder a las Herramientas de soporte de Cisco desde la barra de herramientas del panel.

Haga clic en el icono de la caja de herramientas y seleccione la categoría Soporte de Cisco.

Si las tareas de soporte requieren una conexión de túnel a un dispositivo remoto a través del portal, el agente de soporte deberá:

- Pedir permiso para compartir el escritorio de forma remota durante la llamada de soporte.
- Pedirle que cree la conexión de túnel durante la llamada de soporte.

Comprobación del estado de OnPlus Service

Para comprobar el estado de Cisco OnPlus Service, visite:

www.checkonplus.com

En esta página encontrará comunicaciones sobre el estado del servicio y actualizaciones. Si tiene problemas con Cisco OnPlus Portal, visite esta página para determinar si el problema está relacionado con una interrupción del servicio conocida.

Envío de comentarios sobre Cisco OnPlus

Utilice el área Cisco OnPlus del servicio de soporte para productos Cisco Small Business para preguntar, iniciar discusiones y publicar comentarios y sugerencias sobre Cisco OnPlus Portal. Visítenos en https://supportforums.cisco.com/community/netpro/small-business/onplus.

También puede enviar sus comentarios y sugerencias. Haga clic en el enlace **Comentario** en la parte inferior derecha de cualquier página del portal, seleccione una categoría, escriba sus comentarios y haga clic en **Enviar**.

A

Recursos adicionales

Cisco proporciona una amplia gama de recursos para ayudarle a usted y a su cliente a sacar el máximo partido de Cisco OnPlus Service y de los productos Small Business.

Comunidad	
Comunidad de soporte de Cisco Small Business para OnPlus Service	https://supportforums.cisco.com/community/netpro/small-business/onplus
Vídeos y podcasts de OnPlus Training Library	https://supportforums.cisco.com/docs/DOC-17701
Matriz de compatibilidad de dispositivos	https://supportforums.cisco.com/docs/DOC-17501
Soporte	
Soporte y recursos para productos Cisco Small Business	www.cisco.com/go/smallbizhelp
Página principal de Cisco Small Business	www.cisco.com/smb
Centro de soporte para productos Cisco Small Business	www.cisco.com/go/sbsc
Descargas de software de Cisco	
Centro de descargas de software de Cisco	Hay descargas disponibles para todos los productos Cisco Small Business en el área de descargas de Cisco.com en www.cisco.com/go/software (se requiere registro/inicio de sesión).
OnPlus Portal y documentación	
Toda la documentación técnica de Cisco OnPlus	www.cisco.com/go/onplus

Documentación sobre OnPlus de la comunidad de soporte para productos Small Business	https://supportforums.cisco.com/docs/DOC-17447
Para partners	
Registro e inicio de sesión en la cuenta de partner de Cisco OnPlus Portal	www.cisco-onplus.com
Central de partners de Cisco para Small Business (requiere inicio de sesión como partner)	www.cisco.com/web/partners/sell/smb

B

Compatibilidad con funciones y dispositivos de Cisco

Este apéndice incluye los dispositivos de Cisco compatibles con OnPlus Portal, junto con las funciones del portal disponibles para cada dispositivo, así como las limitaciones o restricciones aplicables.

- **Resumen de funciones de los dispositivos**
- **Limitaciones específicas del dispositivo para funciones de OnPlus**
- **Acceso remoto a través de una conexión de túnel genérico**

Resumen de funciones de los dispositivos

SUGERENCIA Para ver notas, advertencias y limitaciones específicas de cada dispositivo, haga clic en el enlace de la columna Dispositivo de Cisco/Modelo.

Dispositivo de Cisco/ Modelo	Tipo de dispositivo	Icono del producto	Copia seg./ Restauración	Actualización de FW	Acceso remoto
AP521	Punto de acceso	Sí	Sí	Sí	Sí
AP541	Punto de acceso	Sí	Sí	Sí	Sí
AP801	Punto de acceso	Sí	Sí	Sí	Sí[1]
AIR-AP1142	Punto de acceso	Sí	Sí	Sí	Sí
WAP4410N	Punto de acceso	Sí	Sí	Sí	Sí
PVC2300	Cámara IP	Sí	Sí	Sí	Sí
PVC300	Cámara IP	Sí			Sí
VC220	Cámara IP	Sí			Sí

Dispositivo de Cisco/ Modelo	Tipo de dispositivo	Icono del producto	Copia seg./ Restauración	Actualización de FW	Acceso remoto
VC240	Cámara IP	Sí			Sí
Teléfonos IP de la serie SPA300 y SPA500	Teléfono IP	Sí			Sí
Teléfonos IP de las series 6900, 7900, 8900 y 9900 de Cisco	Teléfono IP	Sí			Sí
Cisco 2800	Router	Sí	Sí	Sí	Sí1.
Cisco Catalyst 3750	Router	Sí	Sí	Sí	Sí1.
ISR de la serie 1800 de Cisco	Router	Sí	Sí	Sí	Sí1.
IAD880	Router	Sí	Sí	Sí	Sí1.
Router de servicios integrados ISR1900	Router	Sí	Sí	Sí	Sí1.
ISR870	Router	Sí	Sí	Sí	Sí1.
ISR890	Router	Sí	Sí	Sí	Sí1.
RV042/RV082/ RV016 V. 2	Router	Sí	Sí	Sí	Sí
RV042/RV082/ RV016 V. 3	Router	Sí	Sí	Sí	Sí
SRP500	Router	Sí	Sí	Sí	Sí
ASA5505	Dispositivo de seguridad	Sí	Sí	Sí	Sí
SA520	Dispositivo de seguridad	Sí	Sí	Sí	Sí
NSS300	Almacenamiento	Sí	Sí	Sí	Sí
Serie ESW500	Switch	Sí	Sí	Sí	Sí
SG300 o SF300 (versión 1.0 del firmware)	Switch	Sí	Sí* (requiere cadena de comunidad SNMP)	Sí* (requiere cadena de comunidad SNMP)	Sí
SG300 o SF300 (versión 1.1 del firmware)	Switch	Sí	Sí	Sí	Sí

Dispositivo de Cisco/ Modelo	Tipo de dispositivo	Icono del producto	Copia seg./ Restauración	Actualización de FW	Acceso remoto
WS-CE520	Switch	Sí	Sí	Sí	Sí
UC320	Sistema de voz	Sí	Sí	Sí	Sí
UC500	Sistema de voz	Sí			Sí

1. El método de conexión web habitual no es compatible con CP Express. Utilice SSH, Telnet o HTTP a través de una conexión de túnel genérico. Consulte Acceso remoto a través de una conexión de túnel genérico, en la página 254.

Limitaciones específicas del dispositivo para funciones de OnPlus

Consulte las siguientes secciones para ver información importante sobre las limitaciones y advertencias que se aplican a la compatibilidad de las funciones de Cisco OnPlus Portal.

- ASA5505
- UC320
- ISR890
- ISR de la serie 1800 de Cisco
- IAD880
- Cisco 2800
- Cisco BE3000
- Cisco Catalyst 3750
- UC500
- SRP500
- ISR870
- SA520
- Router de servicios integrados ISR1900
- Serie ESW500
- WAP4410N

- PVC2300
- AP521
- RV042/RV082/RV016 V. 2
- RV042/RV082/RV016 V. 3
- IAD2400
- SG300 o SF300 (versión 1.0 del firmware)
- SG300 o SF300 (versión 1.1 del firmware)
- WS-CE520
- WS-C2960
- WS-C4948
- AP541
- AP801
- AIR-AP1142
- Teléfonos IP de las series 6900, 7900, 8900 y 9900 de Cisco
- Teléfonos IP de la serie SPA300 y SPA500
- PVC300
- VC220
- VC240
- NSS300

ASA5505

Función	Restricciones/Notas
Detección	Los routers de la serie ASA5505 no admiten CDP, Bonjour, UPnP ni ningún otro protocolo de detección compatible con el portal. Se detectarán sus direcciones MAC e IP, pero se mostrarán en la topología como Dispositivo desconocido. Para poder interactuar correctamente con el dispositivo, debe asignar un controlador de dispositivo y realizar entonces el proceso de detección (Información de dispositivo > ficha Credenciales, Controlador de dispositivo). La interfaz de comando al dispositivo ASA5505 utiliza la interfaz HTTP, que debe estar habilitada en la VLAN a la que está asociado OnPlus Agent. El proceso de detección utiliza la tabla ARP de la VLAN a la que está asociado OnPlus Agent con el fin de detectar los dispositivos asociados. Los dispositivos asociados a otras VLAN no se detectan. El dispositivo ASA no tiene un puerto WAN definido; la configuración canónica crea una VLAN que se utiliza para el acceso WAN y la asocia a uno o más puertos del switch. El resto de los puertos normalmente se asociarán a otra VLAN definida en el lado de la LAN. OnPlus Agent debe estar conectado a la VLAN de la LAN.
Actualización de firmware	Los routers de la serie ASA5505 tienen dos paquetes de firmware significativos que residen en su controlador: una carga de software del sistema y una carga de administrador del dispositivo. La función de actualización de firmware de OnPlus Portal admite ambos, pero con las siguientes restricciones: ▪ Los únicos archivos que se aceptarán para la actualización serán aquellos que coincidan con los dos nombres con caracteres comodín: asa*.bin y adsm*.bin. ▪ Si un archivo de firmware coincide con asa*.bin, se entenderá que es una carga de software del sistema. ▪ Si un archivo de firmware coincide con adsm*.bin, se entenderá que es una carga de administrador del dispositivo. ▪ El software del sistema no se actualizará si hay un comando de imagen de arranque ('boot image') en el archivo de configuración de arranque startup-config, pues es probable que el administrador del router no desee que este se sobrescriba. ▪ El software de administrador del dispositivo no se actualizará si hay un comando de imagen adsm ('adsm image') en el archivo de configuración de arranque startup-config. ▪ No se actualizará ningún paquete si no hay suficiente espacio en la unidad de arranque para almacenar el archivo actualizado durante la actualización. ▪ Una actualización de firmware de cualquiera de los dos tipos provoca un reinicio del dispositivo. ▪ Cuando cualquiera de los tipos de firmware se actualiza, el archivo al que sustituye se elimina.

Función	Restricciones/Notas
Acceso remoto	El administrador de dispositivos ASA5505 no puede ejecutarse a través de un túnel creado por el dispositivo Cisco OnPlus Agent. Puede realizarse la administración remota de ASA si está habilitado el acceso a SSH y Cisco OnPlus Agent ha creado una conexión de túnel genérico para SSH para la administración de línea de comandos. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**.

UC320

Función del portal	Restricciones/Notas
Detección	El proceso de detección de OnPlus Portal iniciará sesión en el dispositivo para sondear la información de la red. Para evitar que los usuarios administradores sean expulsados de la GUI de administración de UC320 durante el proceso de detección, elimine la selección de la opción **Permitir acceso de inicio de sesión** en la ficha Credenciales de la ventana Información de dispositivo.
Copia de seguridad/ Restauración de la configuración del dispositivo	La copia de seguridad de un sistema de voz/router de la serie UC300 consiste en la recuperación de un binario formado por una combinación de archivos y ajustes del dispositivo UC300. ▪ Las operaciones de copia de seguridad y restauración a través del portal requieren credenciales de acceso al dispositivo para el UC300. ▪ La restauración de la configuración requiere el uso de la GUI de administración en el dispositivo UC300. ▪ La copia de seguridad del buzón de voz y otros archivos de audio no puede realizarse a través del portal. Debe configurarse mediante la GUI de administración de UC300 utilizando la opción de copia de seguridad a USB y la ventana de mantenimiento diario. La restauración es un proceso largo. Requiere dos reinicios del dispositivo (con una duración de 2,5 - 3 minutos cada uno). Debe reiniciarse el dispositivo antes de abrir la GUI de administración del dispositivo UC300 y después de aplicar la configuración. Otras funciones de la vista Topología no están disponibles mientras la GUI está abierta.
Actualización de firmware	La actualización de firmware requiere el uso de la GUI de administración del UC300. Cuando se solicita una actualización de firmware, se abre un diálogo emergente que guía al usuario durante el proceso de actualización. Otras funciones de la vista Topología no están disponibles mientras este diálogo está abierto.

ISR890

Función del portal	Restricciones/Notas
Detección	Los dispositivos ISR de la serie 800 de Cisco deben tener CDP habilitado para que el dispositivo OnPlus Agent los detecte. Si utiliza Cisco CP o Cisco CP Express para configurar el router, es muy probable que CDP no esté habilitado, ya que esa es la configuración recomendada. Si CDP está deshabilitado, el router de la serie 800 aparecerá en la vista Topología como Dispositivo desconocido. Abra la ventana Información de dispositivo para el dispositivo, seleccione la ficha Credenciales, haga clic en Controlador de dispositivo y seleccione la serie 800 de Cisco. Si CDP está habilitado, la detección del dispositivo se realizará correctamente.
Acceso/ Información de dispositivo	Si no se proporcionan credenciales de acceso al dispositivo, se muestra la dirección MAC y la dirección IP del dispositivo. Si el ISR de la serie 800 tiene acceso a SSH y se introducen credenciales de nivel 15 en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo del portal, se mostrará información adicional del dispositivo y se utilizarán las tablas CAM y ARP del dispositivo para detectar dispositivos adicionales.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad de un ISR de la serie 800 consiste únicamente en guardar una copia del archivo startup-config. Otros elementos, como los usuarios definidos en la base de datos AAA, no se incluyen en la copia de seguridad. Para restaurar la configuración, el archivo guardado se copia en startup-config, se reinicia el dispositivo y se carga la nueva configuración. Tanto la copia de seguridad como la restauración requieren credenciales de acceso al dispositivo (inicio de sesión y habilitación de acceso).
Actualizar firmware	Si el administrador de ISR800 ha definido una carga de arranque con el comando de arranque del sistema, las actualizaciones de firmware no tienen lugar.
Acceso remoto	Una conexión web normal no funcionará. Si tiene CP Express cargado en el router, intentará cargar ese programa y ejecutarlo. Se trata de un programa Java y no funciona correctamente a través del túnel HTTP que se está creando. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**.

ISR de la serie 1800 de Cisco

Función del portal	Restricciones/Notas
Detección	Los dispositivos ISR de la serie 1800 de Cisco deben tener CDP habilitado para que el dispositivo OnPlus Agent los detecte. Si utiliza Cisco CP o Cisco CP Express para configurar el router, es muy probable que CDP no esté habilitado, ya que esa es la configuración recomendada. Si CDP está deshabilitado, el router de la serie 1800 aparecerá en la vista Topología como Dispositivo desconocido. Abra la ventana Información de dispositivo para el dispositivo, seleccione la ficha Credenciales, haga clic en Controlador de dispositivo y seleccione la serie 1800 de Cisco. Si CDP está habilitado, la detección del dispositivo se realizará correctamente.
Acceso e información	Si no se proporcionan credenciales de acceso al dispositivo, se muestra la dirección MAC y la dirección IP del dispositivo. Si el ISR de la serie 1800 tiene acceso a SSH y se introducen credenciales de nivel 15 en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo del portal, se mostrará la información del dispositivo recopilada y se utilizarán las tablas CAM y ARP del dispositivo para detectar dispositivos adicionales.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad de un ISR de la serie 1800 consiste únicamente en guardar una copia del archivo startup-config. Otros elementos, como los usuarios definidos en la base de datos AAA, no se incluyen en la copia de seguridad. Para restaurar la configuración, el archivo guardado se copia en startup-config, se reinicia el dispositivo y se carga la nueva configuración. Tanto la copia de seguridad como la restauración requieren credenciales de acceso al dispositivo (inicio de sesión y habilitación de acceso).
Actualizar firmware	Si el administrador ha definido una carga de arranque con el comando de arranque del sistema, las actualizaciones de firmware no tienen lugar.
Acceso remoto	Una conexión web normal no funcionará. Si tiene CP Express cargado en el router, intentará cargar ese programa y ejecutarlo. Se trata de un programa Java y no funciona correctamente a través del túnel HTTP que se está creando. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**.

IAD880

Función del portal	Restricciones/Notas
Detección	Los dispositivos IAD de la serie 800 de Cisco deben tener CDP habilitado para que el dispositivo OnPlus Agent los detecte. Si utiliza Cisco CP o Cisco CP Express para configurar el router, es muy probable que CDP no esté habilitado, ya que esa es la configuración recomendada. Si CDP está deshabilitado, el router de la serie 800 aparecerá en la vista Topología como Dispositivo desconocido. Abra la ventana Información de dispositivo para el dispositivo, seleccione la ficha Credenciales, haga clic en Controlador de dispositivo y seleccione la serie 800 de Cisco. Si CDP está habilitado, la detección del dispositivo se realizará correctamente.
Acceso/ Información de dispositivo	Independientemente de si se proporcionan credenciales de acceso, se detectará la dirección MAC y la dirección IP del dispositivo. Si el router de la serie IAD800 tiene acceso a SSH y se introducen credenciales de nivel 15 en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo del portal, se mostrará la información del dispositivo recopilada y se utilizarán las tablas CAM y ARP del dispositivo para detectar dispositivos adicionales.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad de un router de la serie IAD800 consiste únicamente en guardar una copia del archivo startup-config. Otros elementos, como los usuarios definidos en la base de datos AAA, no se incluyen en la copia de seguridad. Para restaurar la configuración, el archivo guardado se copia en startup-config se reinicia el router y se carga la nueva configuración. Tanto la copia de seguridad como la restauración de la configuración requieren credenciales de acceso al dispositivo (inicio de sesión y habilitación de acceso).
Actualizar firmware	Para actualizar el firmware, asegúrese de que ha introducido la contraseña y las credenciales de inicio de sesión de nivel 15.
Acceso remoto	Una conexión web normal no funcionará. Si tiene CP Express cargado en el router, intentará cargar ese programa y ejecutarlo. Se trata de un programa Java y no funciona correctamente a través del túnel HTTP que se está creando. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**.

Cisco 2800

Función del portal	Restricciones/Notas
Detección	Independientemente de si se proporcionan credenciales de acceso, se detectará la dirección MAC y la dirección IP del dispositivo. Si el router de la serie 2800 de Cisco tiene acceso a SSH y se introducen credenciales de nivel 15 en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo del portal, se mostrará la información del dispositivo recopilada y se utilizarán las tablas CAM y ARP del dispositivo para detectar dispositivos adicionales.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad de un router de la serie 2800 consiste únicamente en guardar una copa del archivo startup-config. Para restaurar la configuración, el archivo guardado se copia en startup-config, se reinicia el router y se carga la nueva configuración. Tanto la copia de seguridad como la restauración de la configuración requieren credenciales de acceso al dispositivo (inicio de sesión y habilitación de acceso).
Actualizar firmware	Para actualizar el firmware, asegúrese de que ha introducido la contraseña y las credenciales de inicio de sesión de nivel 15.
Acceso remoto	Una conexión web normal no funcionará. Si tiene CP Express cargado en el router, intentará cargar ese programa y ejecutarlo. Se trata de un programa Java y no funciona correctamente a través del túnel HTTP que se está creando. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**.

Cisco BE3000

Función del portal	Restricciones/Notas
Detección	Independientemente de si se proporcionan credenciales de acceso, se detectará la dirección MAC y la dirección IP del dispositivo. Si el router Cisco BE3000 tiene acceso a SSH y se especifican credenciales de nivel 15 en Credenciales > Inicio de sesión y Credenciales > Habilitar en la ventana Información de dispositivo del portal, se mostrará la información del dispositivo recopilada y se utilizarán las tablas CAM y ARP del dispositivo para detectar dispositivos adicionales.

Función del portal	Restricciones/Notas
Copia de seguridad y restauración de la configuración del dispositivo	Ejecución entre aplicaciones disponible.
Actualizar firmware	No admitido
Acceso remoto	Una conexión web normal no funcionará. Si tiene CP Express cargado en el router, intentará cargar ese programa y ejecutarlo. Se trata de un programa Java y no funciona correctamente a través del túnel HTTP que se está creando. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**.

Cisco Catalyst 3750

Función del portal	Restricciones/Notas
Detección	Independientemente de si se proporcionan credenciales de acceso, se detectará la dirección MAC y la dirección IP del dispositivo. Si el switch Cisco Catalyst 3750 tiene acceso a SSH y se introducen credenciales de nivel 15 en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo del portal, se mostrará la información del dispositivo recopilada y se utilizarán las tablas CAM y ARP del dispositivo para detectar dispositivos adicionales.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad de un switch Cisco Catalyst 3750 consiste únicamente en guardar una copa del archivo startup-config. Para restaurar la configuración, el archivo guardado se copia en startup-config, se reinicia el router y se carga la nueva configuración. Tanto la copia de seguridad como la restauración de la configuración requieren credenciales de acceso al dispositivo (inicio de sesión y habilitación de acceso).

Función del portal	Restricciones/Notas
Actualizar firmware	Para actualizar el firmware, asegúrese de que ha introducido la contraseña y las credenciales de inicio de sesión de nivel 15. El dispositivo se actualiza correctamente, pero no se muestra el mensaje que indica que se ha completado la instalación de firmware.
Acceso remoto	Una conexión web normal no funcionará. Si tiene CP Express cargado en el router, intentará cargar ese programa y ejecutarlo. Se trata de un programa Java y no funciona correctamente a través del túnel HTTP que se está creando. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**.

UC500

Función del portal	Restricciones/Notas
Acceso/ Información de dispositivo	Debe introducir las credenciales en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo en el portal para poder acceder al dispositivo. Tras introducir las credenciales, el portal puede acceder a la tabla CAM, la tabla de asociación inalámbrica, la tabla ARP y a vecinos CDP, además de determinar si hay un dispositivo CUE instalado.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad y la restauración de la configuración de dispositivos UC500 no puede realizarse a través de OnPlus Portal. Utilice Cisco Configuration Assistant (CCA) para realizar la copia de seguridad y la restauración de la configuración en UC500 y el módulo CUE.
Actualización de software	La copia de seguridad y la restauración de la configuración de dispositivos UC500 no puede realizarse a través de OnPlus Portal. Utilice Cisco Configuration Assistant (CCA) para administrar este dispositivo.
Acceso remoto	Puede acceder a este dispositivo de forma remota a través de HTTP, SSH o Telnet. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80.

SRP500

Función del portal	Restricciones/Notas
Detección	Si CDP está habilitado, la detección del dispositivo se realizará correctamente. También se realiza la detección UPnP, pero el firmware principal del dispositivo muestra una versión diferente en la detección CDP y en la detección UPnP. El portal utiliza los datos de CDP.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad de los routers de la serie SRP500 consiste únicamente en guardar una copia de los archivos config.xml, status.xml y strike.xml. Para restaurar la configuración, los archivos guardados se copian en config.xml y strike.xml, el router se reinicia, si así lo requiere el dispositivo, y carga la nueva configuración. El archivo status.xml es estático y no se restaura. Este archivo cambia cuando cambia la configuración del dispositivo. Tanto la copia de seguridad como la restauración del dispositivo requieren credenciales de acceso al dispositivo (se necesitan las credenciales de habilitación de acceso e inicio de sesión).
Acceso remoto	La conectividad web al dispositivo le conectará con la página de acceso HTTP para ese dispositivo.

ISR870

Función del portal	Restricciones/Notas
Detección	Los dispositivos ISR de la serie 800 de Cisco deben tener CDP habilitado para que el dispositivo OnPlus Network Agent los detecte. Si utiliza Cisco CP o Cisco CP Express para configurar el router, es muy probable que CDP no esté habilitado, ya que esa es la configuración recomendada. Si CDP está deshabilitado, el router de la serie 800 aparecerá en la vista Topología como Dispositivo desconocido. Abra la ventana Información de dispositivo para el dispositivo, seleccione la ficha Credenciales, haga clic en Controlador de dispositivo y seleccione la serie 800 de Cisco. Si CDP está habilitado, la detección del dispositivo se realizará correctamente.
Acceso/ Información de dispositivo	Independientemente de si se proporcionan credenciales de acceso, se detectará la dirección MAC y la dirección IP del dispositivo. Si el ISR de la serie 800 tiene acceso a SSH y se introducen credenciales de nivel 15 en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo del portal, se mostrará la información del dispositivo recopilada y se utilizarán las tablas CAM y ARP del dispositivo para detectar dispositivos adicionales.

Función del portal	Restricciones/Notas
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad de un ISR de la serie 800 consiste únicamente en guardar una copia del archivo startup-config. Otros elementos, como los usuarios definidos en la base de datos AAA, no se incluyen en la copia de seguridad. Para restaurar la configuración, el archivo guardado se copia en startup-config, se reinicia el dispositivo y se carga la nueva configuración. Tanto la copia de seguridad como la restauración requieren credenciales de acceso al dispositivo (inicio de sesión y habilitación de acceso).
Actualizar firmware	Si el administrador ha definido una carga de arranque con el comando de arranque del sistema, las actualizaciones de firmware no tienen lugar. Si no hay suficiente espacio en flash para incluir la nueva imagen y la carga actual, el firmware del dispositivo no se podrá actualizar a través del portal. Actualice el firmware manualmente.
Acceso remoto	Una conexión web normal no funcionará. Si tiene CP Express cargado en el router, intentará cargar ese programa y ejecutarlo. Se trata de un programa Java y no funciona correctamente a través del túnel HTTP que se está creando. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**.

SA520

Función del portal	Restricciones/Notas
Detección	Este dispositivo se puede detectar mediante CDP y Sonda. El usuario no puede haber iniciado sesión en la página de forma local. No es compatible con la detección UPnP.
Acceso/ Información de dispositivo	Deben proporcionarse credenciales de acceso de inicio de sesión para poder recuperar información. Si un navegador web se ha conectado con las mismas credenciales dadas al controlador, este generará un evento y no consultará el dispositivo, pues solo se permite una sesión activa simultáneamente por usuario y contraseña.
Copia de seguridad y restauración de la configuración del dispositivo	Puede realizar la copia de seguridad y la restauración de la configuración completa del dispositivo.

Función del portal	Restricciones/Notas
Actualizar firmware	OnPlus Agent tarda aproximadamente 5 minutos en conectarse una vez que el firmware vuelve a cargarse y tiene lugar el reinicio.
Acceso remoto	El acceso remoto solo está disponible a través de HTTPS (puerto 443).

Router de servicios integrados ISR1900

Función del portal	Restricciones/Notas
Detección	Los dispositivos ISR de la serie Cisco 1900 deben tener CDP habilitado para que el dispositivo OnPlus Agent los detecte. Además, deben estar conectados a un switch que proporcione información de vecinos CDP a OnPlus Agent, ya que OnPlus Agent normalmente no se conectará directamente al dispositivo ISR. Si utiliza Cisco CP o Cisco CP Express para configurar el router, es muy probable que CDP no esté habilitado, ya que esa es la configuración recomendada. Si CDP está deshabilitado, el router de la serie 1900 aparecerá en la vista Topología como Dispositivo desconocido. Abra la ventana Información de dispositivo para el dispositivo, seleccione la ficha Credenciales, haga clic en Controlador de dispositivo y seleccione la serie 1900 de Cisco. Si CDP está habilitado, la detección del dispositivo se realizará correctamente.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad de un ISR de la serie 1900 consiste únicamente en guardar una copia del archivo startup-config. Otros elementos, como los usuarios definidos en la base de datos AAA, no se incluyen en la copia de seguridad. Para restaurar la configuración, el archivo guardado se copia en startup-config, se reinicia el dispositivo ASA y se carga la nueva configuración. Tanto la copia de seguridad como la restauración requieren credenciales de acceso al dispositivo (inicio de sesión y habilitación de acceso).
Actualizar firmware	Si el administrador del router de la serie 1900 ha definido una carga de arranque determinada con el comando de arranque del sistema, las actualizaciones de firmware no se llevarán a cabo.
Acceso remoto	Una conexión web normal no funcionará. Si tiene CP Express cargado en el router, intentará cargar ese programa y ejecutarlo. Se trata de un programa Java y no funciona correctamente a través del túnel HTTP que se está creando. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80.

Serie ESW500

Función del portal	Restricciones
Detección	Los dispositivos ESW pueden detectarse de tres modos diferentes: ▪ Si están activados los anuncios de Bonjour y está habilitado el protocolo Cisco Bonjour, la detección del dispositivo se realizará correctamente. ▪ Si están activados los anuncios CDP y OnPlus Agent tiene acceso a la información de CDP, la detección del dispositivo se realizará correctamente. OnPlus Agent puede conectarse directamente al switch ESW o acceder a un dispositivo conectado al switch que proporcione información de vecinos CDP. ▪ Por último, el dispositivo ESW puede seleccionarse utilizando un controlador designado. Si se selecciona el controlador y se introducen las credenciales, la detección será correcta. Una vez detectado el dispositivo ESW, proporcionará información de CAM y vecinos CDP para facilitar el proceso de detección de dispositivos adicionales, así como a la construcción de la Topología.
Acceso al dispositivo	Tras la detección, puede recopilarse información del ESW mediante la interfaz de administración HTTP. Se necesitan credenciales válidas. Las credenciales se introducen en **Credenciales** > **Inicio de sesión** en la ventana Información de dispositivo del portal.
Actualización de software	El ESW podría no reiniciarse tras la actualización de firmware.
Acceso remoto	Para el acceso web remoto, utilice el puerto 80 y habilite la opción Reparar encabezados. Las advertencias adicionales pueden variar, en función del navegador web que utilice: ▪ **Safari**. El navegador Safari funciona correctamente, pero deberá ignorar el mensaje emergente sobre la pérdida de la conexión. ▪ **Firefox**. Al conectarse por primera vez con Firefox, verá un mensaje de error. El mensaje de error varía en función de la versión de Firefox que utilice. Para que funcione correctamente, copie la URL y péguela en una ventana nueva del navegador. Ignore el mensaje sobre la pérdida de la conexión. ▪ **Internet Explorer**. IE8 funciona sin errores.

WAP4410N

Función del portal	Restricciones/Notas
Acceso remoto	WAP4410 requiere una conexión segura (HTTPS) para establecer una conexión web remota.

PVC2300

Función del portal	Restricciones/Notas
Acceso/ Información de dispositivo	El número de versión podría tener un formato diferente en la ficha Información del portal y en el sitio web de la cámara. Por ejemplo, la ficha Información muestra V1.1.2R06, mientras que en el sitio web aparece 1.1.2.6.

AP521

Función del portal	Restricciones/Notas
Detección	Las tablas CDP y CAM detectarán este dispositivo, por lo que debe conectarlo a un switch compatible con Cisco OnPlus Portal.
Acceso/ Información de dispositivo	Hacen falta credenciales para acceder al dispositivo. Las credenciales se introducen en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo del portal. El portal no leerá información hasta que se introduzcan las credenciales correctas.
Copia de seguridad y restauración de la configuración del dispositivo	Para acceder a las funciones de copia de seguridad y restauración de la configuración, debe proporcionar las credenciales.
Actualizar firmware	Si proporciona las credenciales, las actualizaciones de firmware funcionarán correctamente. Si el dispositivo ha definido una carga de arranque con el comando de arranque del sistema, las actualizaciones de firmware no se llevarán a cabo, pues el administrador ha definido una carga específica para el dispositivo.
Acceso remoto	El acceso web normal debería funcionar correctamente con este dispositivo. Se le solicitará que introduzca un nombre de usuario/contraseña y, a continuación, verá un sitio web de configuración.

RV042/RV082/RV016 V. 2

Función del portal	Restricciones/Notas
Detección	Debe estar habilitado Bonjour en estos dispositivos.
Acceso/ Información de dispositivo	Solo se admiten credenciales de acceso HTTP.
Acceso remoto	El único acceso remoto compatible es a través de HTTP.

RV042/RV082/RV016 V. 3

Función del portal	Restricciones/Notas
Detección	Debe estar habilitado Bonjour en estos dispositivos.
Acceso/ Información de dispositivo	Solo se admiten credenciales de acceso HTTP.
Actualización de firmware	Un error conocido de RV0xx v. 3 consiste en que al realizar una actualización de firmware siempre se restablece la configuración predeterminada del dispositivo.
Acceso remoto	El único acceso remoto compatible es a través de HTTP.

IAD2400

Función del portal	Restricciones/Notas
Detección	Los dispositivos ISR de la serie 2400 de Cisco deben tener CDP habilitado para que el dispositivo OnPlus Agent los detecte. Si utiliza Cisco CP o Cisco CP Express para configurar el router, es muy probable que CDP no esté habilitado, ya que esa es la configuración recomendada. Si CDP está deshabilitado, el router de la serie 2400 aparecerá en la vista Topología como Dispositivo desconocido. Abra la ventana Información de dispositivo para el dispositivo, seleccione la ficha Acceso, haga clic en Controlador de dispositivo y seleccione la serie 2400 de Cisco. Si CDP está habilitado, la detección del dispositivo se realizará correctamente.

Función del portal	Restricciones/Notas
Acceso/ Información de dispositivo	Independientemente de si se proporcionan credenciales de acceso, se detectará la dirección MAC y la dirección IP del dispositivo. Si el router de la serie IAD2400 tiene acceso a SSH y se introducen credenciales de nivel 15 en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo del portal, se mostrará la información del dispositivo recopilada y se utilizarán las tablas CAM y ARP del dispositivo para detectar dispositivos adicionales.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad de un router de la serie IAD2400 consiste únicamente en guardar una copia del archivo startup-config. Otros elementos, como los usuarios definidos en la base de datos AAA, no se incluyen en la copia de seguridad. Para restaurar la configuración, el archivo guardado se copia en startup-config, se reinicia el router y se carga la nueva configuración. Tanto la copia de seguridad como la restauración de la configuración requieren credenciales de acceso al dispositivo (inicio de sesión y habilitación de acceso).
Actualizar firmware	Para habilitar las actualizaciones de firmware, asegúrese de que ha introducido la contraseña y las credenciales de inicio de sesión de nivel 15.
Acceso remoto	Una conexión web normal no funcionará. Si tiene CP Express cargado en el router, intentará cargar ese programa y ejecutarlo. Se trata de un programa Java y no funciona correctamente a través del túnel HTTP que se está creando. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**.

SG300 o SF300 (versión 1.0 del firmware)

Función del portal	Restricciones/Notas
Detección	Los switches gestionados de la serie SF300/SG300 con la versión 1.0 del firmware instalada pueden detectarse mediante uno de estos tres métodos: ▪ Bonjour. Si el dispositivo está configurado para emitir anuncios de Bonjour, se detectará e identificará correctamente. ▪ Controlador de dispositivo designado. Si está deshabilitada la detección mediante Bonjour, puede detectarse el dispositivo designando manualmente un controlador (ventana Información de dispositivo > ficha Credenciales, Controlador de dispositivo), siempre que se proporcionen las credenciales de inicio de sesión válidas. Si el switch utiliza la versión 1.0 del firmware y puede controlarse mediante SNMPv2, la detección es posible sin problemas. La versión 1.0 del firmware no admite CDP.
Acceso/ Información de dispositivo	Puede accederse a los switches gestionados SF/SG300 a través de SNMPv2. **SNMPv2**. Para poder trabajar con SNMPv2, debe crearse una vista adecuada con acceso de lectura/escritura para la comunidad que utilizará OnPlus Agent. La cadena de comunidad debe introducirse en el campo de credenciales de acceso a SNMP del dispositivo. Para crear las credenciales de acceso a SNMPv2 y permitir que el dispositivo funcione con OnPlus Portal, siga estos pasos: 1. En el dispositivo SG300/SF300, inicie sesión como administrador y acceda a **Seguridad** > **Servicios TCP/UDP** > **Servicio SNMP habilitado**. 2. En el dispositivo SG300/SF300, cree una cadena de comunidad SNMP de lectura/escritura. 3. En OnPlus Portal, introduzca la cadena de comunidad SNMP en Credenciales > Acceso a SNMP, en la ventana Información de dispositivo.
Copia de seguridad y restauración de la configuración del dispositivo	Para realizar la copia de seguridad y restauración de los switches gestionados de la serie SF300/SG300 con la versión 1.0 del firmware instalada, es necesario que el servicio SNMP esté habilitado en el dispositivo y que esté configurado el acceso a SNMPv2 en el portal. Si se vuelve a cargar el archivo startup-config en el dispositivo, se realiza un reinicio.

Función del portal	Restricciones/Notas
Actualizar firmware	Los switches gestionados de la serie SF/SG300 solo admiten actualizaciones de firmware mediante SNMPv2. SNMPv2 debe estar habilitado en el dispositivo y el acceso a SNMP configurado en el portal. Los switches de la serie SF300/SG300 tienen espacio para dos imágenes: una imagen activa y una imagen de reserva. Cuando se solicita una instalación de firmware, el sistema comprueba que la imagen no sea la imagen activa ni la imagen de reserva. Si coincide con alguna de estas dos imágenes, se cancela la transferencia de archivos. Si se trata de un nuevo archivo de firmware, se copia en el dispositivo. El switch copiará el nuevo archivo de imagen sobre la imagen no activa. El switch tiene una marca que indica qué imagen estará activa tras el reinicio. Esta marca se modifica para indicar que el firmware que se acaba de cargar será el activo tras el reinicio. A continuación, se envía el reinicio al dispositivo y se carga la nueva imagen. El proceso de reinicio puede durar entre 2 y 3 minutos. Durante este proceso, OnPlus Agent intenta volver a conectarse continuamente. OnPlus Agent comprueba si el dispositivo ha adquirido una nueva dirección IP.
Acceso remoto	La versión 1.0 del firmware no admite el acceso web remoto a través del portal. Se proporciona el acceso a SNMPv2 para habilitar la detección, la copia de seguridad y la restauración de la configuración a través del portal, y las actualizaciones de firmware mediante el portal. El control SNMP del dispositivo no es posible a través del acceso remoto.

SG300 o SF300 (versión 1.1 del firmware)

Función del portal	Restricciones/Notas
Detección	Los switches gestionados de la serie SF/SG300 con la versión 1.1 del firmware o posterior pueden detectarse mediante uno de estos tres métodos: ▪ Bonjour. Si el dispositivo está configurado para emitir anuncios de Bonjour, se detectará e identificará correctamente. ▪ CDP. Si el dispositivo está configurado para emitir anuncios de CDP, se detectará e identificará correctamente. ▪ Controlador de dispositivo designado. En el caso de que otros métodos de detección estén deshabilitados, puede detectarse el dispositivo designando manualmente un controlador (ventana Información de dispositivo > ficha Credenciales, Controlador de dispositivo), siempre y cuando se proporcionen unas credenciales de inicio de sesión válidas. Cuando se haya detectado el dispositivo y se hayan proporcionado las credenciales, el switch llevará a cabo la detección en otros dispositivos encontrados como vecinos CDP, así como en los dispositivos de la tabla CAM. Si el switch utiliza la versión del firmware 1.1 o posterior, puede detectarse a través de SNMP2 o mediante la interfaz HTTP.

Función del portal	Restricciones/Notas
Acceso/ Información de dispositivo	Puede accederse a los switches gestionados de las series SF300 y SG300 que tengan instalada la versión 1.1 del firmware a través e SNMPv2, SNMPv3 o HTTP. Para poder trabajar con SNMPv2 o SNMPv3, debe crearse una vista adecuada con acceso de lectura/escritura para la comunidad que utilizará OnPlus Agent. La cadena de comunidad debe introducirse en el campo de credenciales de acceso a SNMP del dispositivo. **SNMPv2**. Para crear las credenciales de acceso a SNMPv2 y permitir que el dispositivo funcione con OnPlus Portal, siga estos pasos: 1. En el dispositivo SG300/SF300, inicie sesión como administrador y acceda a **Seguridad** > **Servicios TCP/UDP** > **Servicio SNMP habilitado**. 2. En el dispositivo SG300/SF300, cree una cadena de comunidad SNMP de lectura/escritura. 3. En OnPlus Portal, introduzca la cadena de comunidad SNMP en Credenciales > Acceso a SNMP, en la ventana Información de dispositivo. **SNMPv3**. Si crea credenciales de SNMPv3 para el dispositivo y las configura para que puedan utilizarse, el controlador intentará utilizar preferentemente esos controladores en lugar de las credenciales de SNMPv2. La versión 1.1 del firmware para los switches de la serie SF300/SG300 es compatible con SNMPv3, pero con ciertas restricciones. ▪ El firmware no guarda usuarios que se han definido para SNMPv3. Esto quiere decir que, cada vez que se reinicie el dispositivo, deberá volver a introducir las credenciales de acceso. ▪ El dispositivo no admite el uso de frases de contraseña para Privacidad. Debido a que los modelos de autenticación SNMPv3 de Cisco OnPlus solo utilizan frases de contraseña (no claves), no puede utilizar Privacidad con este dispositivo. ▪ El dispositivo no admite AES para el protocolo de privacidad. Deberá utilizar DES. Para ver un ejemplo de cómo configurar el acceso a la administración de SNMPv3 para switches gestionados de la serie SF300/SG300 mediante OnPlus Portal, siga estos pasos: 1. En el sitio web del dispositivo acceda a **SNMP:ID de motor**, seleccione el botón de opción **Usar predeterminado** y haga clic en **Aplicar**. 2. En el sitio web del dispositivo, vaya a **SNMP:Grupos** y seleccione un grupo. 3. Establezca el nombre del grupo en **authnopriv**, seleccione **Modelo de seguridad SNMPv3**, marque las casillas Autenticación y Sin privacidad, y otorgue al dispositivo privilegios de lectura, escritura y notificación como DefaultSuper. 4. Haga clic en **Aplicar**. 5. En **Usuario SNMP**:Usuarios, agregue un usuario nuevo llamado admin mediante el **ID de motor local**. Establezca el nombre del grupo en authnopriv, el método de autenticación en contraseña **MD5** y la contraseña en Password01. Haga clic en **Aplicar**.

Función del portal	Restricciones/Notas
	6. En **Seguridad:Servicios TCP/UDP**, habilite **SNMP** y haga clic en **Aplicar**. 7. A continuación, guarde los ajustes en Admin File management. 8. En OnPlus Portal, abra la ventana Información de dispositivo para el dispositivo en cuestión, seleccione la ficha Credenciales, **Acceso a SNMP** y, a continuación, haga clic en el botón de opción **SNMPv3**. Especifique los ajustes correspondientes y haga clic en **Aceptar**. Sus credenciales deberían validarse correctamente para el dispositivo SF300/SG300.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad y la restauración de los switches gestionados de la serie SF300/SG300 pueden realizarse mediante SNMPv2 o utilizando API HTTP/XML. La versión 1.1 del firmware es completamente compatible con las funciones de copia de seguridad y restauración. Si se vuelve a cargar el archivo startup-config en el dispositivo, se realiza un reinicio.
Actualizar firmware	Las actualizaciones de firmware en los switches gestionados de la serie SF300/SG300 pueden realizarse mediante SNMPv2 o API HTTP/XML. El procedimiento es completamente compatible con la versión 1.1 del firmware. Los switches de la serie SF300/SG300 tienen espacio para dos imágenes: una imagen activa y una imagen de reserva. Cuando se solicita una instalación de firmware, el sistema comprueba que la imagen no sea la imagen activa ni la imagen de reserva. Si coincide con alguna de estas dos imágenes, se cancela la transferencia de archivos. Si se trata de un nuevo archivo de firmware, se copia en el dispositivo. El switch copiará el nuevo archivo de imagen sobre la imagen no activa. El switch tiene una marca que indica qué imagen estará activa tras el reinicio. Esta marca se modifica para indicar que el firmware que se acaba de cargar será el activo tras el reinicio. A continuación, se envía el reinicio al dispositivo y se carga la nueva imagen. El proceso de reinicio puede durar entre 2 y 3 minutos. Durante este proceso, OnPlus Agent intenta volver a conectarse continuamente. OnPlus Agent comprueba si el dispositivo ha adquirido una nueva dirección IP.
Acceso remoto	Puede accederse de forma remota a la interfaz de administración web de los switches gestionados de la serie SF/SG300 mediante una conexión web. Se proporciona el acceso a la administración de SNMPv2/v3 para habilitar la detección, la copia de seguridad y la restauración de la configuración a través del portal, y las actualizaciones de firmware mediante el portal. El control SNMP del dispositivo no es posible a través del acceso remoto.

WS-CE520

Función del portal	Restricciones/Notas
Acceso/ Información de dispositivo	Debe estar habilitado CDP en este dispositivo.
Detección	Las únicas credenciales compatibles son las credenciales de inicio de sesión HTTP.
Acceso remoto	El único acceso remoto compatible es a través de HTTP.

WS-C2960

Función del portal	Restricciones/Notas
Detección	Los dispositivos Catalyst 2900 CatOS no son compatibles. Los dispositivos compatibles deben estar basados en IOS. Si CDP está habilitado, la detección del dispositivo se realizará correctamente. Sin embargo, si los switches 2960 están apilados, el proceso de detección es más complejo. Para que funcione la detección CDP, el anuncio debe venir del principal. Esto quiere decir que debería haber una conexión desde el switch principal a OnPlus Network Agent u otro dispositivo capaz de proporcionar información de vecinos CDP a OnPlus Network Agent. Si los anuncios de CDP proceden de uno de los switches secundarios, el portal no puede asociarlos con la pila.
Acceso/ Información de dispositivo	Independientemente de si se proporcionan credenciales de acceso, se detectará la dirección MAC y la dirección IP del dispositivo. Si el router de la serie Cat 2900 tiene acceso a SSH y se introducen credenciales de nivel 15 en **Credenciales** > **Inicio de sesión** y **Credenciales** > Habilitar en la ventana Información de dispositivo del portal, se mostrará la información del dispositivo recopilada y se utilizarán las tablas CAM y ARP del dispositivo para detectar dispositivos adicionales.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad de un router de la serie Cat 2900 consiste únicamente en guardar una copia del archivo startup-config. Para restaurar la configuración, el archivo guardado se copia en startup-config, se reinicia el router y se carga la nueva configuración. Tanto la copia de seguridad como la restauración de la configuración requieren credenciales de acceso al dispositivo (inicio de sesión y habilitación de acceso).

Función del portal	Restricciones/Notas
Actualizar firmware	Para habilitar las actualizaciones de firmware, asegúrese de que ha introducido la contraseña y las credenciales de inicio de sesión de nivel 15.
Acceso remoto	Una conexión web normal no funcionará. Si tiene CP Express cargado en el router, intentará cargar ese programa y ejecutarlo. Se trata de un programa Java y no funciona correctamente a través del túnel HTTP que se está creando. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**.

WS-C4948

Función del portal	Restricciones/Notas
Detección	Los dispositivos Catalyst 4948 CatOS no son compatibles. Los dispositivos compatibles deben estar basados en IOS. Si CDP está habilitado, la detección del dispositivo se realizará correctamente.
Acceso/ Información de dispositivo	Independientemente de si se proporcionan credenciales de acceso, se detectará la dirección MAC y la dirección IP del dispositivo. Si el router de la serie C4948 tiene acceso a SSH y se introducen las credenciales de nivel 15 en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo del portal, la información del dispositivo recopilada incluirá el número de serie, el PID/VID, el tipo de dispositivo, el nombre del modelo y la descripción. Además, las tablas ARP y CAM del dispositivo se utilizarán para detectar dispositivos adicionales.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad de un router de la serie Cat 4948 consiste únicamente en guardar una copia del archivo startup-config. Para restaurar la configuración, el archivo guardado se copia en startup-config, se reinicia el router y se carga la nueva configuración. Tanto la copia de seguridad como la restauración requieren credenciales de acceso al dispositivo (inicio de sesión y habilitación de acceso).
Actualizar firmware	Para actualizar el firmware, asegúrese de que ha introducido la contraseña y las credenciales de inicio de sesión de nivel 15.

Función del portal	Restricciones/Notas
Acceso remoto	Una conexión web normal no funcionará. Si tiene CP Express cargado en el router, intentará cargar ese programa y ejecutarlo. Se trata de un programa Java y no funciona correctamente a través del túnel HTTP que se está creando. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**.

AP541

Función del portal	Restricciones/Notas
Detección	Puesto que el dispositivo se detecta mediante CDP, deberán estar establecidos siempre el firmware y la plataforma. El proceso de detección requiere que se establezca un nombre de usuario y una contraseña de inicio de sesión. Las credenciales se introducen en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo del portal. Si proporciona las credenciales, los dispositivos conectados a este dispositivo deberían aparecer en la vista Topología.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad y la restauración requieren que se establezca un nombre de usuario y una contraseña de inicio de sesión. La copia de seguridad y la restauración de la configuración del dispositivo son compatibles. Tras una restauración, el dispositivo se reinicia para que la nueva configuración tenga efecto. Las copias de seguridad que se realizan con el firmware 1.9.1 son compatibles con 1.9.2. Normalmente, las copias de seguridad solo son válidas para la carga de firmware en la que se realizan.
Actualizar firmware	Las actualizaciones de firmware requieren que se establezca un nombre de usuario y una contraseña de inicio de sesión.

AP801

Función del portal	Restricciones/Notas
Detección	El punto de acceso de la serie AP800 se detecta mediante CDP, ARP, DHCP y búsqueda en la tabla CAM. CDP es el método principal para la detección, el resto agregan información adicional.
Acceso/ Información de dispositivo	Independientemente de si se proporcionan credenciales de acceso, las direcciones MAC e IP del dispositivo se detectan. Si el punto de acceso de la serie AP800 tiene acceso a SSH y se introducen las credenciales de nivel 15 en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo del portal, la información del dispositivo recopilada incluirá el número de serie, el PID/ VID, el tipo de dispositivo y el nombre del modelo. No se establece una descripción.
Copia de seguridad y restauración de la configuración del dispositivo	La copia de seguridad de un punto de acceso de la serie AP800 consiste únicamente en guardar una copia del archivo startup-config. Otros elementos, como los usuarios definidos en la base de datos AAA, no se incluyen en la copia de seguridad. Para restaurar la configuración, el archivo guardado se copia en startup-config, se reinicia el punto de acceso y se carga la nueva configuración. Tanto la copia de seguridad como la restauración requieren credenciales de acceso al dispositivo (inicio de sesión y habilitación de acceso).
Actualizar firmware	AP801 es un módulo de IOS que se muestra como un dispositivo individual en la Topología del portal. La imagen de firmware no es un archivo de IOS .bin normal, se trata de un paquete tar que contiene la imagen IOS y los archivos de acceso a HTTP. Durante una actualización de firmware, los archivos se extraen al flash en el directorio especificado en el archivo tar, el directorio anterior se elimina y se establece la variable del entorno de arranque, de modo que el punto de acceso pueda arrancar correctamente.
Acceso remoto	Una conexión web normal no funcionará. Si tiene CP Express cargado en el router, intentará cargar ese programa y ejecutarlo. Se trata de un programa Java y no funciona correctamente a través del túnel HTTP que se está creando. Para el acceso HTTP, abra una conexión de túnel genérico en el puerto 80. Para la administración de línea de comandos IOS, habilite SSH o Telnet en el dispositivo y realice la conexión a través de un túnel genérico. Consulte **Acceso remoto a través de una conexión de túnel genérico, en la página 254**.

AIR-AP1142

Función del portal	Restricciones/Notas
Detección	Las tablas CDP y CAM detectarán este dispositivo, por lo que debe conectarlo a un switch compatible.
Copia de seguridad y restauración de la configuración del dispositivo	Deberá proporcionar las credenciales para que la configuración del dispositivo y las funciones de copia de seguridad y restauración funcionen correctamente. Las credenciales se introducen en **Credenciales** > **Inicio de sesión** y **Credenciales** > **Habilitar** en la ventana Información de dispositivo del portal.
Actualizar firmware	Si se proporcionan las credenciales de acceso, el proceso funcionará correctamente. Si el administrador ha definido una carga de arranque específica con el comando de arranque del sistema, las actualizaciones de firmware no tienen lugar.

Teléfonos IP de las series 6900, 7900, 8900 y 9900 de Cisco

Función del portal	Restricciones/Notas
Detección	Los teléfonos IP de Cisco solo pueden detectarse mediante CDP y entradas de la tabla CAM. Puesto que los teléfonos residen en otra VLAN, el dispositivo OnPlus Agent no puede detectarlos utilizando otros métodos. Si los teléfonos están conectados a un router/switch que no es compatible con OnPlus Portal, no se mostrarán en la vista Topología.
Acceso/ Información de dispositivo	Solo debe accederse a un teléfono determinado una vez. Se recopilará la siguiente información: Número de serie, información para crear un PID/VID y versión del software. No se lee ni establece ninguna otra información. La copia de seguridad/restauración y la actualización de firmware mediante el elemento de funcionalidades de administración de la ficha Información están deshabilitadas. Una vez establecido el número de serie para un teléfono, ya no se volverá a acceder a él de nuevo. En algunos casos, se accederá al teléfono varias veces hasta que toda la información de la detección se envíe al SN y de vuelta a OnPlus Agent en el archivo consumer_sani.xml. Puede accederse a un teléfono varias veces si tiene una carga predeterminada que no es compatible con el acceso a HTTP. Cuando se haya configurado el teléfono en un sistema PBX compatible con el acceso a HTTP y tenga una carga de teléfono actualizada, se accederá a él para obtener la información necesaria.

Teléfonos IP de la serie SPA300 y SPA500

Función del portal	Restricciones/Notas
Detección	Los teléfonos IP de Cisco solo pueden detectarse mediante CDP y entradas de la tabla CAM. Puesto que los teléfonos residen en otra VLAN, el dispositivo OnPlus Agent no puede detectarlos utilizando otros métodos. Si los teléfonos están conectados a un router/switch que no es compatible con OnPlus Portal, no se mostrarán en la vista Topología.
Acceso/ Información de dispositivo	La siguiente información se recopila para estos teléfonos durante la detección: número de serie, ID de producto y versión (PID/VID) y versión de software. No se lee ni establece ninguna otra información. La copia de seguridad/ restauración y la actualización de firmware mediante el elemento de funcionalidades de administración de la ficha Información están deshabilitadas. Una vez establecido el número de serie para un teléfono, ya no se volverá a acceder a él de nuevo. En algunos casos, se accederá al teléfono varias veces hasta que toda la información de la detección se envíe a OnPlus Agent. Puede accederse a un teléfono varias veces si tiene una carga predeterminada que no es compatible con el acceso a HTTP. Cuando se haya configurado el teléfono en un sistema PBX compatible con el acceso a HTTP y tenga una carga de teléfono actualizada, se accederá a él para obtener la información necesaria. Un UC320 tras un dispositivo de seguridad SA500 (la instalación de red existente) necesitará una ruta desde la red de datos VLAN 1 a la red de voz VLAN 100 (en UC320, Networking -> Routing -> static -> Destination = 10.1.1.0 /24 Interface = LAN Gateway = 192.168.75.250).

PVC300

Función del portal	Restricciones/Notas
Acceso remoto	El acceso remoto funcionará correctamente, pero esta conexión solo debe utilizarse para la configuración del sistema y no para ver vídeos. En algunos casos, el vídeo podría no funcionar, en función de la versión del navegador que se utilice, debido a los complementos que sean necesarios.

VC220

Función del portal	Restricciones/Notas
Acceso remoto	El acceso remoto funcionará correctamente, pero esta conexión solo debe utilizarse para la configuración del sistema y no para ver vídeos. En algunos casos, el vídeo podría no funcionar, en función de la versión del navegador que se utilice, debido a los complementos que sean necesarios.

VC240

Función del portal	Restricciones/Notas
Acceso remoto	El acceso remoto funcionará correctamente, pero esta conexión solo debe utilizarse para la configuración del sistema y no para ver vídeos. En algunos casos, el vídeo podría no funcionar, en función de la versión del navegador que se utilice, debido a los complementos que sean necesarios.

NSS300

Función	Notas sobre restricciones/implementación
Detección	La detección de los dispositivos de la serie NSS300 depende de la detección Bonjour. NSS300 debería tener habilitados los anuncios de Bonjour tanto para la administración web como para CSCO-SB.
Acceso a dispositivos e información	La administración de los dispositivos NAS de la serie NSS300 se realiza mediante la interfaz web. Actualmente, las versiones de firmware 1.1, 1.2 y 1.3 son compatibles. ▪ Si está disponible, la administración se realizar por medio de HTTPS en el puerto 443. ▪ Si este puerto no está disponible, la administración se realiza a través de HTTP en el puerto 8080. ▪ Si ninguno de estos dos puertos está abierto, no se podrá administrar el dispositivo.

Función	Notas sobre restricciones/implementación
Copia de seguridad y restauración	La copia de seguridad y la restauración en el dispositivo NSS300 se realizan por medio de las funciones de copia de seguridad y restauración de la interfaz web y funcionan exactamente igual que si el usuario las realizara con la interfaz administrativa convencional. La restauración de la configuración requiere un reinicio y los reinicios de NAS pueden variar en duración, en función de la cantidad de administración de almacenamiento que deba llevarse a cabo. ▪ Si el reinicio dura más de cinco minutos, OnPlus Agent podría informar de un error al reconectarse al dispositivo. ▪ Si el dispositivo obtiene una nueva dirección IP durante el reinicio, OnPlus Agent intentará volver a conectarse a la nueva dirección, pero este proceso no es del todo fiable. Se recomienda otorgar a los dispositivos administrados una dirección IP fija.
Actualización de firmware	La actualización de firmware en un dispositivo NAS300 se realiza mediante la interfaz web y funciona exactamente igual que si el usuario la realizara mediante la interfaz administrativa convencional. La actualización de firmware requiere un reinicio y los reinicios de NAS pueden variar en duración, en función de la cantidad de administración de almacenamiento que deba llevarse a cabo. ▪ Si el reinicio dura más de cinco minutos, OnPlus Agent podría informar de un error al reconectarse al dispositivo. ▪ Si el dispositivo obtiene una nueva dirección IP durante el reinicio, OnPlus Agent intentará volver a conectarse a la nueva dirección, pero este proceso no es del todo fiable. Se recomienda otorgar a los dispositivos administrados direcciones fijas.

Acceso remoto a través de una conexión de túnel genérico

Para conectar un dispositivo IOS a través de Telnet o SSH para la administración de línea de comandos IOS, siga estos pasos:

PASO 1 Localice el dispositivo en las vistas Topología o Lista de dispositivos y abra la ventana Información de dispositivo.

a. Haga clic en la ficha Conectar y seleccione Conexión genérica.

b. Para SSH, introduzca el puerto 22. Para Telnet, introduzca el puerto 23.

c. Haga clic en **Conectar con dispositivo**. Se mostrará la URL para la conexión en una ventana emergente.

d. Copie el enlace.

PASO 2 Pegue el enlace en el software de conexión de su terminal.

Por ejemplo, si está PuTTY:

a. Copie la dirección en la ventana Host (IP).

b. Seleccione SSH o Telnet.

c. Sustituya el número de puerto que se muestra en PuTTY (puerto 22 para SSH; puerto 23 para Telnet) por el número que aparece tras los dos puntos (:) en la dirección del enlace.

d. Seleccione **Abrir**.

Attachment A

End User's Consent and Obligations

Cisco OnPlus Service for End Users

(1) End User understands that Reseller has been licensed by Cisco to use an ON100 Network Agent in performance of the Cisco OnPlus Service.

(2) End User authorizes Reseller to install and use the ON100 Network Agent on End User's Network for the performance of the Cisco OnPlus Service.

(3) End User is aware that the ON100 Network Agent may be disabled at any time by End User and understands that performance of the Cisco OnPlus Service will be suspended until such time as the ON100 Network Agent is reconnected.

(4) End User acknowledges and agrees that the ON100 Network Agent will collect and transmit, via industry standard encryption (using "http" protocol) End User Network Information to Cisco. End User Network Information will be accessible by Cisco and Reseller via an online Portal. "End User Network Information" means the information about End User's Network that is collected, stored and analyzed in connection with the Cisco OnPlus Service and is related to End User Network configuration (including IP addresses) for a particular environment. The ON100 Network Agent will not collect nor transmit End User software system logins or passwords, financial or business operations data, or any other information that is not related to the End User's network.

(5) End User acknowledges and agrees that the Reseller may collect and transmit to Cisco End User contact information, including, without limitation, name, address, email addresses and telephone numbers ("End User Contact Information").

(6) By using the Cisco OnPlus Service, End User agrees and consents to the collection, use, processing and storage of End User Network Information, End User Contact Information and any other personal data according to the Cisco Privacy Statement (available at http://www.cisco.com/web/siteassets/legal/privacy.html), including the transfer of data outside End User's country of residence, where standards of data protection may be different.

(7) Cisco shall treat the End User Network Information and End User Contact Information confidentially per the terms of the confidential information provisions between Cisco and Reseller.

(8) Cisco may use End User Network Information and End User Contact Information to generate Inventory Reports, and for other commercial and business purposes, which may also be shared with Reseller. Among other things, Cisco may use End User Network Information and End User Contact Information (1) to determine if equipment is covered by Cisco support service agreements, (2) to help Cisco understand End User's network configuration, and product and other technical needs, (3) to provide proactive support services to End User through Cisco's Small Business Support Center, and (4) to support sales and marketing efforts directed at Resellers and End Users. Cisco will not share End User Network Information or End User Contact Information with any third parties, except for Cisco contractors involved in relevant Cisco business and covered under Cisco confidentiality agreements.

(9) End User may opt-out out of Cisco's marketing efforts at any time by contacting accounts-onplus@cisco.com.

(10) Upon disablement or removal of the ON100 Network Agent, End User may request Reseller to purge End User's Network Information and/or End User Contact Information.

_____

(Signature of End User)

By:_____

Name:_____

Title:_____

Date:_____