

Consola de Attendant remota a través de un Firewall

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Puertos usados por la Consola de Attendant](#)

[Comunicación entre el cliente AC y el Cisco Callmanager server](#)

[Consola de Attendant y NAT](#)

[Solución al estatus del recibe línea a través de un Firewall](#)

[Información Relacionada](#)

[Introducción](#)

La Consola de Attendant del Cisco Unified CallManager integra las funciones tradicionales de la telefonía de la multiplexión por división de tiempo (TDM) con las aplicaciones de telefonía IP y los servicios avanzados, tales como directorio del Lightweight Directory Access Protocol (LDAP). Un beneficio principal de la Consola de Attendant del Cisco Unified CallManager sobre los sistemas tradicionales de la Consola de Attendant es la capacidad de monitorear el estado de cada línea en el sistema y de enviar eficientemente las llamadas.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco CallManager 4.x
- Consola de Attendant 1.4 de Cisco

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

Puertos usados por la Consola de Attendant

Comunicación entre el cliente AC y el Cisco Callmanager server

Hay tres tipos de comunicación entre el cliente y servidor AC:

- **El cliente AC a la invocación del método remoto (RMI)** — el cliente conecta siempre con el RMI en los puertos de servidor 1099 a 1129. Entonces, el servidor dice al cliente establecer a una segunda sesión TCP con el servidor en un segundo puerto TCP. Este puerto se toma aleatoriamente y no hay manera de garantizar que un puerto TCP determinado está utilizado siempre.
- **Cliente AC a la codificación rápida del buffer (QBE) en el administrador de Integración de telefonía de computadora (CTI)** — la comunicación QBE establece a una sesión TCP con el servidor en el puerto TCP 2748.
- **El cliente AC al Line State Server (LSS)** — en este caso, allí es el tráfico UDP LSS que viene de los servidores. Esto se puede reparar en el cuadro de diálogo avanzado de las configuraciones (véase la [solución al estatus del recibe línea a través de una](#) sección del [Firewall](#)). Los puertos especificados en el cuadro de diálogo de los parámetros de los servicios son utilizados por el Cisco CallManager para escuchar las peticiones del detalle de terminación de llamada (TCD), para inicializar a los clientes AC y para ofrecer la línea información del estado a los clientes. Estos puertos TCP no deben ser cambiados.

Un Firewall no se soporta porque el AC utiliza los puertos al azar para las conexiones RMI. Solamente un puerto disponible se utiliza para iniciar la conexión RMI, que comienza con 1099. Después de que se establezca la conexión RMI, el RMI utiliza un puerto TCP al azar (normalmente el primer puerto disponible). Por lo tanto, asegúrese que los puertos TCP estén abiertos en hasta el 1129 el rango 1099. Si estos puertos al azar no están abiertos, el AC falla con este mensaje de error:

```
error communicating with the server
```

Refiera a estos documentos para más información sobre el Cisco CallManager TCP y el uso del puerto UDP para la Consola de Attendant:

- [Puertos TCP y UDP usados por el Cisco CallManager 3.3](#)
- [Cisco Unified CallManager 4.2 TCP y uso del puerto UDP](#)
- [Cisco Unified CallManager 5.1 TCP y uso del puerto UDP](#)
- [Cisco Unified CallManager 6.0 TCP y uso del puerto UDP](#)

Consola de Attendant y NAT

En una Consola de Attendant de Cisco, el línea-estado y el estatus del reenvío de llamada de la línea primaria de cada usuario se presenta con cada entrada de registro. Cuando usted utiliza el Cisco CallManager y la Consola de Attendant a través de las interfaces del Network Address

Translation (NAT), o cuando un Firewall está entre ellas, tráfico TCP trabaja correctamente con el NAT transversal. Por lo tanto, la mayor parte de los trabajos de las funciones AC. Sin embargo, el problema está para la línea estatus de la Consola de Attendant que utiliza el UDP. También, el tráfico UDP de los CallManagers no puede pasar a través de las interfaces NAT.

Solución al estatus del recibe línea a través de un Firewall

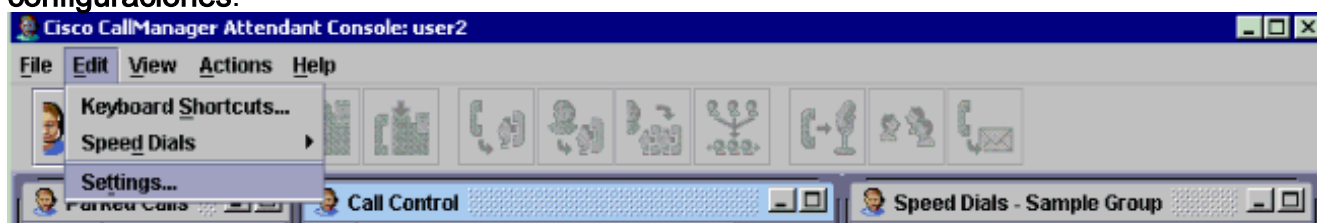
La Consola de Attendant de Cisco utiliza los puertos UDP para el línea-estado. El puerto UDP que debe ser utilizado se puede configurar en el cuadro de diálogo avanzado de las configuraciones de Consola de Attendant de Cisco. Si no se configura ningún puerto, el AC utiliza el primer puerto disponible UDP (al azar).

Si se especifica un puerto libre UDP, por ejemplo el puerto 1234 (véase el [cuadro 2](#)), se aseguran este puerto se abre en el Firewall también.

Complete estos pasos para configurar el puerto UDP usado:

1. Inicie sesión a la Consola de Attendant.

2. Elija **editan > las configuraciones.**



3. En la ventana emergente, haga clic **avanzado** y cambie el campo de la dirección IP del host local a **172.16.1.1:1234** si la dirección IP de la Consola de Attendant PC es 172.16.1.1 y el puerto UDP es

Attendant Settings

Basic **Advanced**

Use the following options only if you need to change the defaults.

Path Name of Local Directory File:

Directory Reload Interval (in seconds):

Call Processing Server Host Names or IP Addresses (comma separated):

Local Host IP Address (for line state): 172.16.1.1:2074

Enable Trace **Enable Audible Alerts**

Show Accessibility Messages **Hold Call When Dial Pad is Active**

Save **Cancel**

1234.

4. Click **Save**.
5. Termine la sesión para que las nuevas configuraciones tomen el efecto. **Nota:** El AC no fue diseñado para trabajar con un Firewall o un NAT. Sin embargo, hay un bug de la petición de la característica clasificado para bloquear abajo del rango de puertos. Refiera al Id. de bug Cisco [CSCee21603](#) ([clientes registrados solamente](#)) para más información. Por ahora, la única solución alternativa para este problema está a desbloquea los puertos TCP usados o inhabilita el Firewall.

[Información Relacionada](#)

- [Puertos TCP y UDP usados por el Cisco CallManager 3.3](#)