

Remote Attendant Console Across a Firewall

Document ID: 71668

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Ports Used by the Attendant Console

Communication between the AC Client and Cisco CallManager Server

Attendant Console and NAT

Solution to Receive Line Status Across a Firewall

Related Information

Introduction

Cisco Unified CallManager Attendant Console integrates traditional time-division multiplexing (TDM) telephony functions with advanced IP telephony applications and services, such as Lightweight Directory Access Protocol (LDAP) directory. A primary benefit of Cisco Unified CallManager Attendant Console over traditional attendant-console systems is the ability to monitor the state of every line in the system and to efficiently dispatch calls.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco CallManager 4.x
- Cisco Attendant Console 1.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Ports Used by the Attendant Console

Communication between the AC Client and Cisco CallManager Server

There are three types of communication between the AC client and server:

- **AC client to Remote Method Invocation (RMI)** The client always connects to RMI at server ports 1099 through 1129. Then, the server tells the client to establish a second TCP session with the server on a second TCP port. This port is randomly taken and there is no way to guarantee that a particular TCP port is always used.
- **AC client to Quick Buffer Encoding (QBE) in the Computer Telephony Integration (CTI) manager** The QBE communication establishes a TCP session with the server at TCP port 2748.
- **AC client to Line State Server (LSS)** In this case, there is UDP LSS traffic that comes from the servers. This can be fixed in the Advanced Settings dialog box (see the Solution to Receive Line Status Across a Firewall section). The ports specified in the Services Parameters dialog box are used by Cisco CallManager to listen to Termination Call Detail (TCD) requests, initialize the AC clients and offer line state information to the clients. These TCP ports must not be changed.

A firewall is not supported because the AC uses random ports for RMI connections. Only one available port is used to initiate the RMI connection, which starts with 1099. After the RMI connection is established, RMI uses a random TCP port (normally the first available port). Therefore, make sure any one the TCP ports is open in the 1099 through 1129 range. If these random ports are not open, the AC fails with this error message:

```
error communicating with the server
```

Refer to these documents for more information about the Cisco CallManager TCP and UDP port usage for Attendant Console:

- TCP and UDP Ports Used by Cisco CallManager 3.3
- Cisco Unified CallManager 4.2 TCP and UDP Port Usage
- Cisco Unified CallManager 5.1 TCP and UDP Port Usage
- Cisco Unified CallManager 6.0 TCP and UDP Port Usage

Attendant Console and NAT

In a Cisco Attendant Console, the line–state and call–forwarding status of the primary line of each user is presented with each record entry. When you use Cisco CallManager and Attendant Console across Network Address Translation (NAT) interfaces, or when a firewall is between them, TCP traffic works correctly with the NAT transversal. Therefore, most of the AC functionality works. However, the problem is for the Attendant Console line status which uses UDP. Also, the UDP traffic from the CallManagers cannot pass through the NAT interfaces.

Solution to Receive Line Status Across a Firewall

Cisco Attendant Console uses UDP ports for line–state. The UDP port that should be used can be configured in the Advanced Settings dialog box of Cisco Attendant Console. If no port is configured, the AC uses the first available UDP port (random).

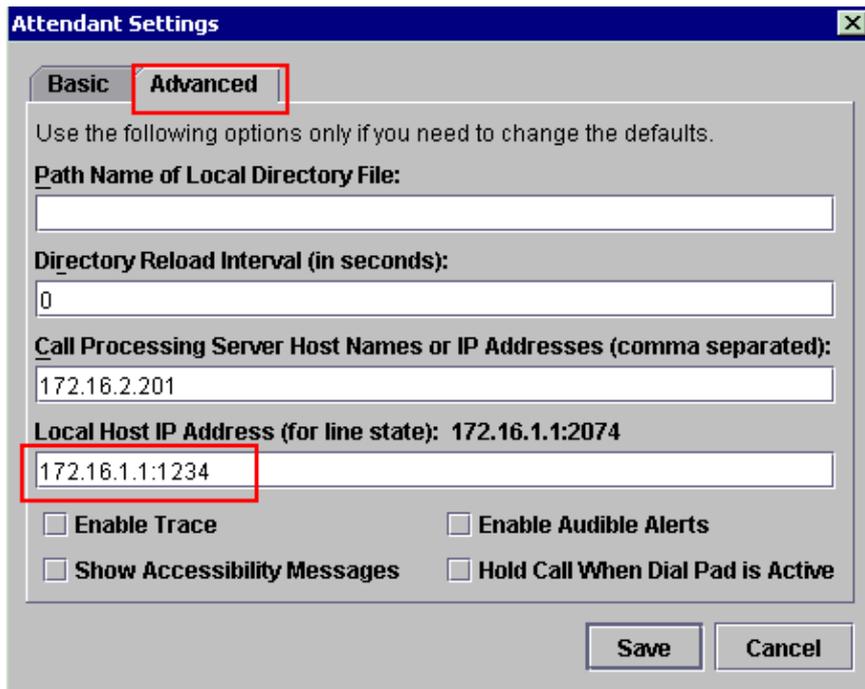
If a free UDP port is specified, such as port 1234 (see Figure 2), make sure this port is opened in the firewall too.

Complete these steps in order to configure the UDP port used:

1. Log in to Attendant Console.
2. Choose **Edit > Settings**.



3. In the pop-up window, click **Advanced** and change the Local Host IP Address field to **172.16.1.1:1234** if the IP Address of the Attendant Console PC is 172.16.1.1 and the UDP port is 1234.



4. Click **Save**.
5. Log out for the new settings to take effect.

Note: The AC was not designed to work with a firewall or NAT. However, there is a feature request bug filed to lock down the port range. Refer to Cisco bug ID CSCee21603 (registered customers only) for more information.

For now, the only workaround for this issue is to either unblock the TCP ports used or disable the firewall.

Related Information

- [Cisco CallManager 4.1 TCP AND UDP Port Usage](#)
- [TCP and UDP Ports Used by Cisco CallManager 3.3](#)
- [Voice Technology Support](#)
- [Voice and Unified Communications Product Support](#)
- [Troubleshooting Cisco IP Telephony](#) 
- [Technical Support & Documentation – Cisco Systems](#)

