

Agents Not Displayed on Cisco Supervisor Desktop

Document ID: 63307

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Problem

Solution

- Examples of Debugs

Related Information

Introduction

This document describes the steps to take when one of these problems occurs with agents in a Cisco IP Contact Center (IPCC) Express environment:

- specific agents do not display on a Cisco Supervisor Desktop
- agents disappear from the Cisco Supervisor Desktop
- the Supervisor Desktop does not display any agents

Prerequisites

Requirements

Readers of this document should have knowledge of these topics:

- Cisco Customer Response Solutions (CRS)
- Cisco Agent Desktop
- Cisco Supervisor Desktop

Components Used

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

- Cisco CRS version 3.x and later

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

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Problem

One of these problems occurs with agents in a Cisco IP Contact Center (IPCC) Express environment:

- specific agents do not display on a Cisco Supervisor Desktop
- agents disappear from the Cisco Supervisor Desktop
- the Supervisor Desktop does not display any agents

Solution

Complete these steps in order to resolve this problem:

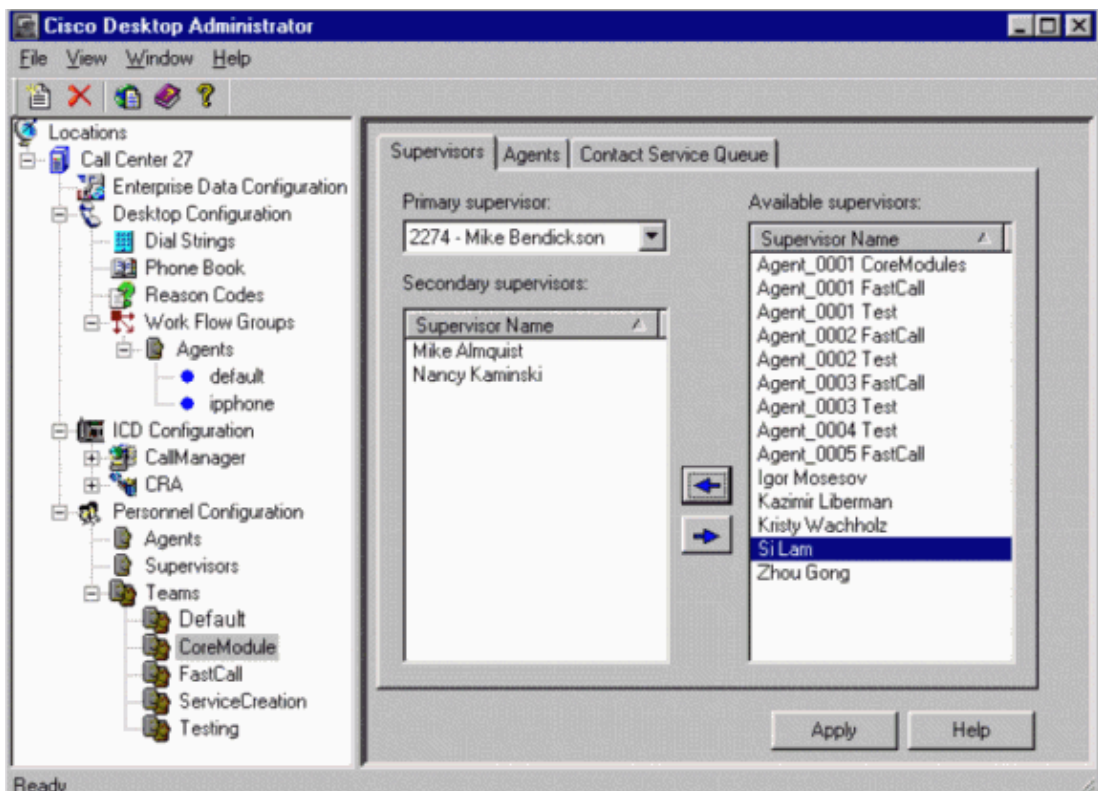
Step One

Verify the agent belongs to the "teams" that the supervisor is monitoring. Look at the Cisco Desktop Administrator in order to verify this.

1. Launch Desktop Administrator.
2. Drill-down to **Personnel Configuration**.
3. Choose the **Supervisors** tab.
4. Verify which "teams" the supervisor monitors. Drill-down to the **Teams** node, as shown in Figure 1.
5. Click to highlight a specific team.
6. These fields populate:

- ◆ Primary supervisor
- ◆ Secondary supervisors
- ◆ Available supervisors

Figure 1: Cisco Desktop Administrator -- Supervisors



7. Choose the **Agents** tab.
8. Verify the agents are associated to the same "teams" the supervisor monitors.

For additional information on "teams" configuration, refer to the Cisco Desktop Administrator User Guide.

Step Two

Verify all Cisco Agent Desktops and Cisco Supervisor Desktops are upgraded to the same version as the **Desktop Services** that runs on the IPCC Express server. In order to verify the versions for each application, choose **Help > About**.

Step Three

Verify the agent does not close the Chat window. The Chat window is a piece of the Agent Desktop software that sends information to the Chat server that provides the agent status. The Chat server then relays these messages to the Supervisor for display. If the agent closes the Chat window, the agent status disappears or does not display.

Step Four

Does the the Supervisor or Agent PC have multiple network interface cards (NICs)? The Call/Chat and Supervisor Desktop does not work properly on PCs with multiple IP addresses. Refer to the *Troubleshooting* section of the Service Information Cisco Desktop Product Suite 4.5 (ICD) for more information.

Step Five

Verify that there are no ports in the 59000–59030 range that are closed off by a firewall. See Step Seven for information on port tests.

Step Six

If either the Supervisor or Agent PCs run Windows XP, verify the Internet Connection Firewall is disabled. Refer to Cisco Supervisor Desktop Issues with Internet Connection Firewall on Windows XP for more information.

Step Seven

Test for blocked ports with telnet from a command line with the agent and supervisor logged in:

```
From Chat server to the agent:      telnet <agent PC IP address> 59020
From Chat server to the supervisor:  telnet <Supervisor IP address> 59021
From the agent to Chat server:      telnet <CRS server IP address> 59000
From the supervisor to Chat server:  telnet <CRS server IP address> 59000
```

If there is a failed connect error, determine why the port is blocked. Here is an example of a failed connection:

```
c:\telnet 192.168.xxx.xxx 59000
Connecting to 192.168.xxx.xxx Could not open a connection to host on port 59000
:Connect failed
```

Step Eight

If a second NIC is used for Voice over IP (VoIP) monitoring/recording on the CRS Server, verify it is configured with non-routable IP addresses and no Default Gateway as noted in Cisco Desktop Product Suite Installation Guide. This needs to be done in order to ensure that packets from the chat server are not sent to the Supervisor through the second NIC card.

Step Nine

Complete these steps to ensure that the system path includes the location of the WebAdminLib.dll. On the Unified CCX server, add the location of the WebAdminLib.dll (C:\Program Files\Cisco\Desktop\bin) to the Path environment variable.

1. Choose **Control Panel** and launch the System utility.
2. On the Advanced tab, click **Environment Variables**.
3. From the list of system variables, choose **Path** and click **Edit**.
4. In the Variable value field, locate the string **C:\Program Files\Cisco\Desktop\bin**. Use cut/paste in order to move it to the beginning of the variable value string. This results in the DLL being accessed from the correct location.
5. Click **OK** and close System utility.
6. Stop the **Cisco Unified Node Manager**.
7. On the Unified CCX server, delete the teamadmin folder from these locations: **C:\Program Files\wfavvid\tomcat_appadmin\webapps** and **C:\Program Files\wfavvid\tomcat_appadmin\work\catalina\localhost**
8. Restart the Unified Node Manager, and wait two minutes.
9. Access Cisco Desktop Administrator and verify that you can navigate to the Services **Configuration > Enterprise Data > Fields page**.

Step Ten

Gather these details and create a new Cisco Technical Assistance Center (TAC) Service Request.

1. Note the time the agent disappears from the Supervisor Desktop.
2. Gather the Agent, Chat Server, and Supervisor logs.
3. Verify that the clocks on all of the PCs from where the traces are taken are synchronized.

Step Eleven

Make sure that the Directory Services are Synchronized in the Cisco Desktop Administrator. If not, restart the Cisco Desktop Sync Server service. Also, refer to Failure to Synchronize Directory Services in Cisco Desktop Administrator – Reset Password for more information.

Step Twelve

Make sure that the Cisco Security Agent does not block the chat ports. Refer to Cisco CRS (IP IVR and IPCC Express) Port Utilization Guide [☞](#) for more information.

Note: Based on the version of CSA, you can add exclusions to the security policy. But, if you run the stand alone (headless) version of CSA, then you are bound by the default policy.

Examples of Debugs

This section shows portions of messages to show the debugs.

Example One

For this message, the login ID is 2272 and the extension is 2891. The Agent starts up and connects with the Chat server:

```
11:36:02 10/01/2004 DEBUG10 FCCClient::setAgentAcidState Begin. Ext: 2891,
agentState: Not Ready, stateTransitionMask: 589923
```

Here, the debug prints at level 10 in agent .dbg.

Example Two

The Chat server receives the message from the agent:

```
11:36:02 10/01/2004 DEBUG1 CChatServer::setAgentAcidState Begin.  
agentExtension: 2891, agentAcidState: Not Ready, stateTransitionMask: 589923.
```

The debug prints at level 1 on the Chat server fccserver .dbg.

Example Three

The Supervisor receives the message from the Chat server:

```
11:36:02 10/01/2004 DEBUG10 FCC_Client_impl::agentAcidState Begin.  
  
destID:2891, extension: 2891, acidState: Not Ready, stateTransitionMask: 589923.  
11:36:02 10/01/2004 DEBUG10 FCCClientAPI::insertEvent Begin. 11/36/02  
10/01/2004 DEBUG10 FCCClientAPI::PrintEvent Begin. eventType: Agent ACD State,  
destType: Unknown user type, destID: 2891, srcType: Unknown user type, srcID:  
2891, srcName: . 11:36:02 10/01/2004 DEBUG10 FCCClientAPI::PrintEvent acidState:  
Not Ready, stateTransitionMask: 589923, duration: 0. 11:36:02 10/01/2004 DEBUG10  
FCCClientAPI::PrintEventEnd. 11:36:02 10/01/2004 DEBUG10 FCCClientAPI::InsertEvent  
Inserting the event. 11:36:02 10/01/2004 DEBUG10 FCCClientAPI::insertEvent Calling  
PostMessage. 11:36:02 10/01/2004 DEBUG10 FCCClientAPI::insertEvent End. 11:36:02  
10/01/2004 DEBUG10 FCCClientAPI::getEvent Begin. 11:36:02 10/01/2004 DEBUG10  
FCCClientAPI::getEvent Getting the next event. 11:36:02 10/01/2004 DEBUG10  
FCCClientAPI::PrintEvent Begin. eventType: Agent ACD State.  
  
destType: Unknown user type, destID: 2891, srcType: Unknown user type, srcID:2891,  
srcName:. 11:36:02 10/01/2004 DEBUG10 FCCClientAPI::PrintEvent acidState: Not  
Ready, stateTransitionMask: 589923, duration: 0. 11:36:02 10/01/2004 DEBUG10  
FCCClientAPI::PrintEvent End. 11:36:02 10/01/2004 DEBUG10 FCCClientAPI::getEvent  
End. return_code:0. 11:36:02 10/01/2004 DEBUG12 Supervisor SE0288 Receiving event:  
  
FCC_ET_ACD_STATE Type: User: Ext: 2891  
  
State: Not Ready
```

Debug prints at level 10 and 12 in Supervisor debug.

Set the agent and supervisor debug to level 204 and increase the trace file size.

Related Information

- [Cisco Desktop Administrator User Guide](#)
- [Service Information Cisco Desktop Product Suite 4.5 \(ICD\)](#)
- [Cisco Supervisor Desktop Issues with Internet Connection Firewall on Windows XP](#)
- [Cisco Desktop Product Suite 4.5.5 \(ICD\) Installation Guide](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

