Logging into Cisco Supervisor Desktop Fails

Document ID: 45201

Contents

Introduction

This document describes why the Supervisor Desktop ID fails to login to Supervisor Desktop in a Cisco IP Contact Center (IPCC) Express environment. It also provides the correct configuration to resolve the issue.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco CallManager
- Cisco IPCC Express

Components Used

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

- Cisco CallManager version 3.3(2) with Service Pack B (SPB) or later
- Cisco IPCC Express version 3.0(3a) or 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

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

Problem

When you login to the Supervisor Desktop, the login fails with two different error messages.

- The Supervisor Desktop ID has **administrator** rights, login fails with this error message:

```
This ID does not have a Supervisor's rights.
```

Figure 1: No Supervisor's Rights

- If the Supervisor Desktop ID has supervisor rights, login fails with this error message:

```
Unable to find this User ID in LDAP.
```

Figure 2: Missing User ID

Solution

This is a configuration issue. In order to login to a Supervisor Desktop, the ID must belong to a team of agents. It is necessary to run the Cisco Desktop Administrator to complete two tasks:

- Add the Supervisor Desktop ID to the supervisor group.

- Add the Associate Supervisor Desktop ID to the team.

The Supervisor window (Figure 3) displays a list of the supervisors available to a team. These supervisors are chosen from the list of agents set up in the Integrated Contact Distribution (ICD) server. It is possible to add or remove a supervisor and to view supervisor properties from this window.

Figure 3: Supervisor Window

Figure 4 shows the setup of agents for a particular team.

- Agents selected for the team
- Agents available to be assigned to the team

The list of available agents includes agents who have not yet been assigned to a team. An agent can belong to only one team at a time.

Figure 4: Team – Agent Window

In Figure 5, the setup of supervisors for a particular team is displayed.

- Primary supervisor
- Secondary supervisors
- Available supervisors

The list of available supervisors includes any agent tagged as a supervisor. Supervisors can be assigned to multiple teams.

Figure 5: Team Window – Supervisor

The Teams – Contact Service Queue window (Figure 6) allows the setup of a contact service queue for a particular team These are the setup options displayed:

- Queues assigned to the team
- All available queues

The list of available queues includes every queue set up on the ICD server. Queues can be assigned to multiple teams.

Figure 6: Team – Contact Service Queue

After you assign a Supervisor Desktop ID to a team, the Supervisor Desktop ID successfully logs in to the Supervisor Desktop.

Problem

Agents keeps appearing and disappearing in Supervisor Desktop.

Solution

In order to resolve this issue, rename the existing SplkStd.dll file and apply a patched version of the SplkStd.dll file. Complete these steps for the workaround:–

1. Go to **C:\Program Files\Cisco\Desktop\bin** on the agent PC.
2. Rename the existing SplkStd.dll to SplkStd.old.
3. Extract the new SplkStd.dll file to the path mentioned in step 1 and reboot the PC.

This problem is fixed in Unified Contact Contact Center Express (UCCX) 8.0(1) and 7.0(2) versions. Referefer to CSCtd75811 (registered customers only) for more information.

Problem

When a user tries to login to Cisco Supervisor Desktop, this error is received:

```
The ID you entered was not found.
```

Solution

This can occur when a config object gets corrupt during an unclean shutdown of the system. In order to prevent this, use the CLI command to shut down the system. Depending on the config object that is corrupt, an alert gets displayed in the RTMT application syslog and looks similar to this:

```
MADM-CFG_MGR-3-CONFIG_OBJECT_CORRUPTED:Error while reading config.
Probably it was corrupt: Config Class=<config name>
```

In the log file, a message similar to this appears:

```
19475: Feb 01 16:26:35.309 PST
%MIVR-CFG_MGR-3-CONFIG_OBJECT_CORRUPTED:Error while reading config.
Probably it was corrupt: Config Class=class
com.cisco.crs.rmcm.ACMIAutoConfig,Exception=java.io.EOFException
```

This issue is documented by Cisco bug ID CSCtd87821 (registered customers only) . The workaround for this bug is to run this CLI command that will detect and fix the problem:

```
utils uccx database dbserver integrity
```

Related Information

- **Cisco Desktop Administrator User Guide**
- **Technical Support and Documentation – Cisco Systems**

Updated: Jun 22, 2011   Document ID: 45201