

Desktop Monitoring Checklist and Troubleshooting Guide

Document ID: 71157

Introduction

Prerequisites

Requirements

Components Used

Conventions

Desktop Monitoring Checklist

Data Collection after Implementation of the Checklist

Supplementary information

Related Information

Introduction

This document describes the checklist for Desktop Monitoring failures, and also provides a troubleshooting guide in the event that the implementation of this checklist does not solve the problem in a Cisco Unified Contact Center Express environment.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified CallManager
- Cisco Unified Contact Center Express

Components Used

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

- Cisco Unified CallManager version 4.1(x) or 4.2(x)
- Cisco Customer Response Solutions version 4.0(X)

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

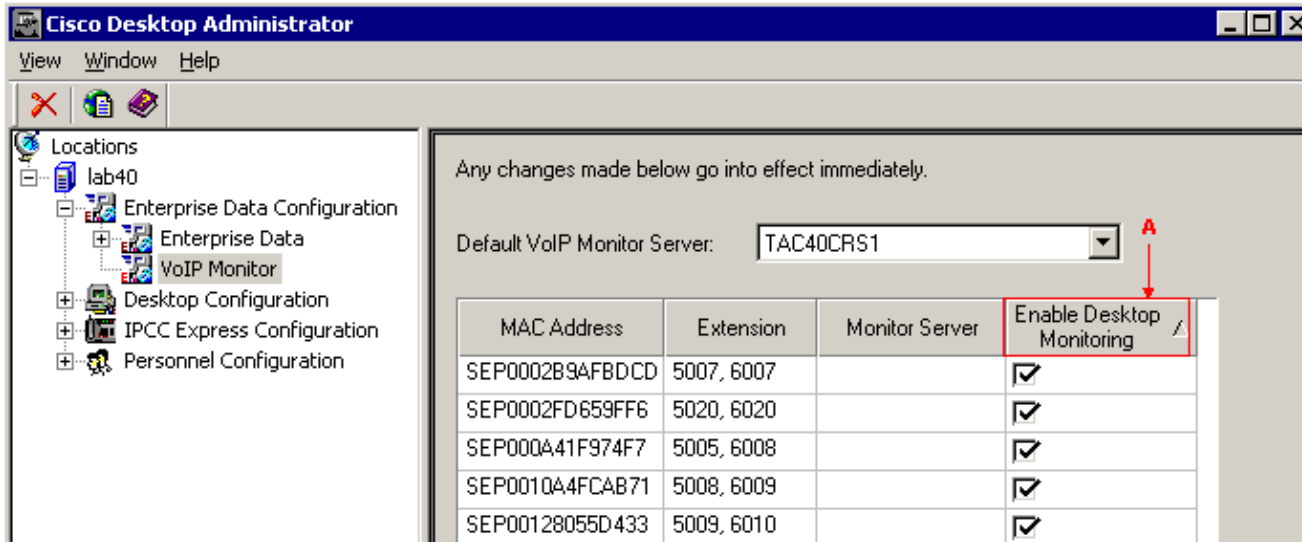
Refer to Cisco Technical Tips Conventions for more information on document conventions.

Desktop Monitoring Checklist

Check for these items in order to help isolate problems and issues with Desktop Monitoring:

- Confirm that the supervisor is able to hear other sounds on his or her PC, such as .wav files, through the PC speakers or headset.
- Confirm that **Enable Desktop Monitoring** is selected for the appropriate devices in the **VoIP Monitor** window (see arrow A in Figure 1) of Desktop Administrator.

Figure 1: Cisco Desktop Administrator



- Confirm that the Agent PC Network Interface Cards (NICs) are plugged into the backs of the IP phones (**daisy-chained**).
- If agents use IP phone models 7941, 7961, 7970, and/or 7971, be sure to enable the **Span to PC Port** setting (see arrow A in Figure 2) under the Product Specific Configuration section in the phone configuration for Cisco CallManager Administration.

Figure 2: Phone Configuration – Span to PC Port

Product Specific Configuration	
Disable Speakerphone	<input type="checkbox"/>
Disable Speakerphone and Headset	<input type="checkbox"/>
Forwarding Delay*	Disabled
PC Port*	Enabled
Settings Access*	Enabled
Gratuitous ARP*	Enabled
PC Voice VLAN Access*	Enabled
Video Capabilities*	Disabled
Auto Line Select*	Disabled
Web Access*	Enabled
Days Display Not Active	< None > Sunday Monday
Display On Time	07:30
Display On Duration	10:30
Display Idle Timeout	01:00
Span to PC Port*	Enabled
Logging Display*	PC Controlled
Load Server	

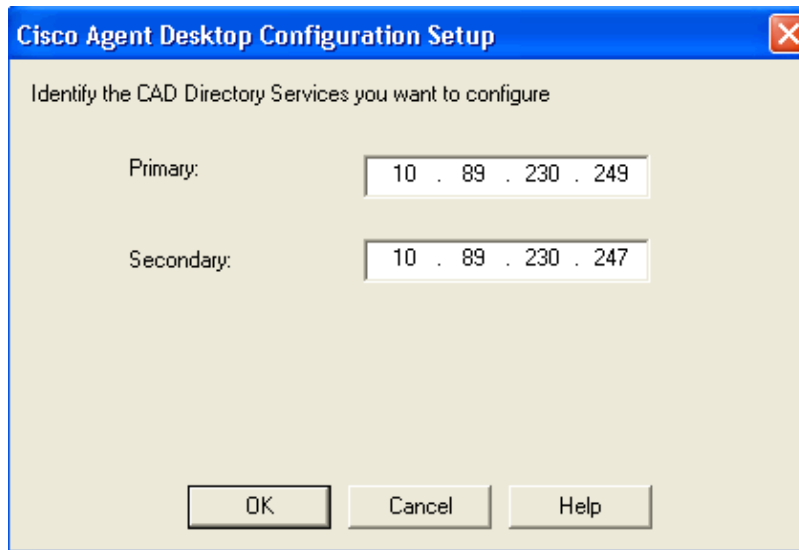
- Perform this procedure in order to confirm that the Cisco Agent Desktop registry is configured for the proper NICs:

1. Run the **ipconfig /all** command on the agent PC in order to determine the current IP address for the NIC plugged into the IP phone.
2. Launch **PostInstall.exe** from the C:\Program Files\Cisco\Desktop\bin folder on the agent PC.

Note: Desktop monitoring does not work if teaming is enabled on the NIC cards.

3. Be sure that the IP addresses of the Cisco IP Contact Center (IPCC) Express servers (see Figure 3) appear properly in the first window.

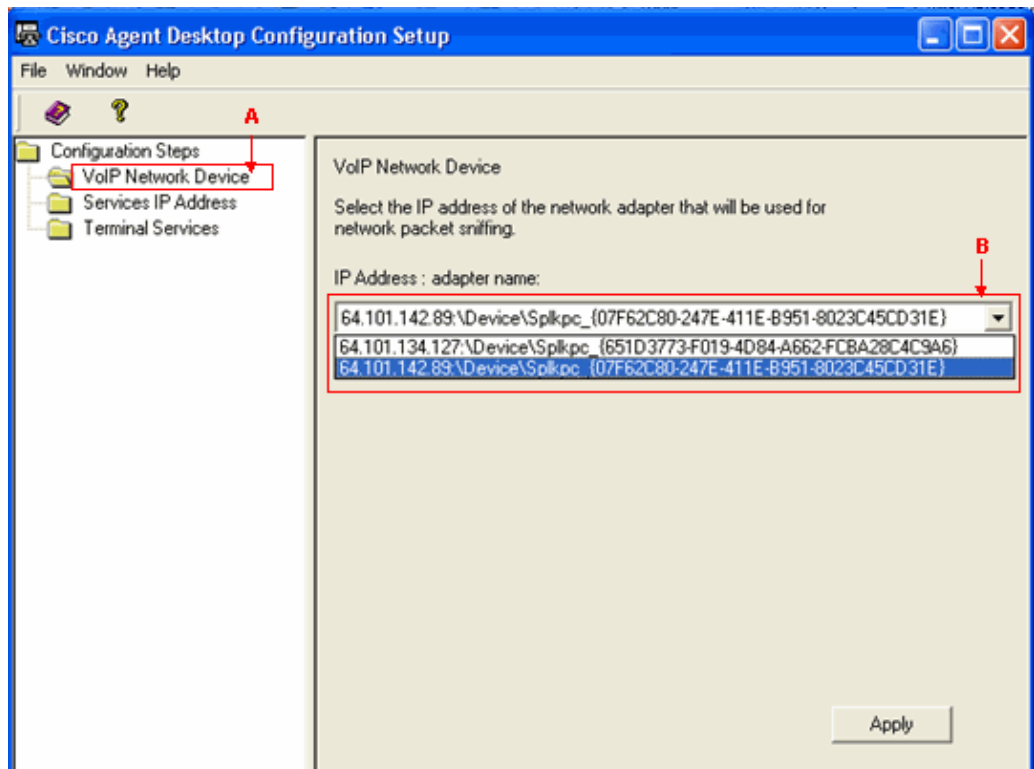
Figure 3: Cisco Agent Desktop Configuration Setup – Identify the CAD Directory Services



4. Click **OK**. The Cisco Agent Desktop Configuration Setup screen appears (see Figure 4).
5. Click the VoIP Network Device (see arrow A in Figure 4).
6. Select the proper adapter from the drop-down list (see arrow B in Figure 4) based on the current IP address.

Note: Re-select the proper device even if it already appears correctly in that field.

Figure 4: Cisco Agent Desktop Configuration Setup – VoIP Network Device



7. Click **Apply**, and shutdown the window.

Note: The NIC does NOT have to be configured with a static IP address. The IP address appears in the PostInstall tool simply as a reference in order to make it easier to identify the proper adapter.

- If the CRS server that runs the Voice over IP (VoIP) monitor has two NICs installed, the NIC for normal CRS traffic should be on the top of the TCP/IP bind order and the NIC for VoIP monitor traffic should be bound to TCP/IP behind the other NIC. If you experience a CRA engine start failure,

the root cause could be an incorrect NIC binding order. In order to change the NIC binding order, refer to the *Background Information* section of CRA Engine Not Starting with Second NIC Installed.

Note: Incorrect NIC binding order can result in high CPU utilization on the Cisco Agent desktop client PC.

- Certain NICs are configured by default to strip VLAN tags, which does not allow Desktop Monitoring to work. These NICs have published instructions for how to manually configure them to pass VLAN tags:

Note: If your NIC is not listed here, refer to your NIC and/or PC manufacturer's documentation.

- ◆ Intel PRO/100 and Intel PRO/1000
- ◆ Broadcom NetXtreme Gigabit
- In order to perform VoIP Monitoring on an agent's phones, the IPCC server needs to know the MAC address of the phones which in turn requires the IPCC server to access the Cisco CallManager database. In order to get access to the Cisco CallManager database, the IPCC server uses the CCMSERVICE account as the credential. There is a CCMSERVICE account on the Cisco CallManager and there is a CCMSERVICE account on the IPCC server. The password for this service should be the same for both servers. If not, the Cisco Desktop Administrator receives the `unable to connect to odbc client on PC` error message while the administrator tries to view the VoIP Monitor configuration. In order to synchronize the CCMSERVICE password on both servers, you need to use the **AdminUtility** on the Cisco CallManager server and the **Customer Response Solutions AdminUtility** on the IPCC server. You cannot use Windows user management to reset the password (because the password is encrypted).
- If you receive the error message that states `splk_pcap_open_live() failed. errorBuf = driver error: not enough memory to allocate the kernel buffer` in the Event log, it indicates that your VoIP Monitor points to a NIC that is either disconnected or disabled. You can fix this when you run the **Post Install Tool (PostInstall.exe)** on the CRS server as mentioned earlier in this document.

Data Collection after Implementation of the Checklist

If Desktop Monitoring still does not work after the checklist is implemented, collect and send this information:

- Can any supervisor monitor any agent at this site? Describe in details.
- Do the agent and supervisor PCs have more than one NIC enabled on their respective PC?
- Who manufactures the NICs, and what is the model and driver version of the NICs installed in those agent and supervisor PCs?
- Which Operating System (OS) is Cisco Agent Desktop and Supervisor Desktop running on at this site?
- Which IP phone model is used by the supervisors and agents at this site?
- Choose one agent that cannot be monitored and collect this information from his or her PC:
 - ◆ The output of the **ipconfig /all** command
 - ◆ Export these registry keys, including all subkeys, to .txt files but not to .reg files:

```
\HKEY_Local_Machine\SYSTEM\ControlSet001
\HKEY_Local_Machine\SYSTEM\CurrentControlSet
\HKEY_Local_Machine\SOFTWARE\Spanlink
```

Supplementary information

These are some other Desktop Monitoring–related links that can also be of assistance:

- [Qualifying Ethernet Cards for Cisco Agent Desktop Monitoring](#) contains the procedure for how to qualify NICs, which requires two client PCs, a hub, SnifferPro (or some other package that can SEND a frame), and the **VLANSamplePackets.cap** file

Download the VLANSamplePackets.cap from Software Downloads (registered customers only) .

- [Network Interface Cards \(NICs\) tested with Cisco CTI/OS and Cisco Agent Desktop Silent Monitor — Reference Information](#) lists some NIC/driver/OS combinations that Cisco has tested.
- If the agents and/or supervisors are on Windows 2000, consider enabling Quality of Service (QoS) on their NICs. On some NICs, QoS forces the NICs not to discard the VLAN tags. Refer to [QoS Traffic Control in Windows 2000](#) for details.

Related Information

- [Intel PRO/100 and Intel PRO/1000](#)
- [Broadcom NetXtreme Gigabit](#)
- [Cisco Unified Contact Center Express End–User Guides](#)
- [Cisco Unified Contact Center Express Install and Upgrade Guides](#)
- [Qualifying Ethernet Cards for Cisco Agent Desktop Monitoring](#)
- [Network Interface Cards \(NICs\) tested with Cisco CTI/OS and Cisco Agent Desktop Silent Monitor — Reference Information](#)
- [QoS Traffic Control in Windows 2000](#)
- [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.](#)

Updated: May 28, 2007

Document ID: 71157
