



NICE Perform[®]

Insight from Interactions[™]



NICE Systems Ltd. shall bear no responsibility or liability to a client or to any other person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any NICE product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any NICE products.

Information in this document is subject to change without notice and does not represent a commitment on the part of NICE Systems Ltd. The systems described in this document are furnished under a license agreement or nondisclosure agreement.

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of NICE Systems Ltd. and protected by United States and international copyright laws.

Permission is granted to view and photocopy (or print) materials from this document for personal, non-commercial use only. Any other copying, distribution, retransmission or modification of the information in this document, whether in electronic or hard copy form, without the express prior written permission of NICE Systems Ltd., is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

All contents of this document are: Copyright © 2008 NICE Systems Ltd. All rights reserved.

This product is covered by one or more of the following US patents:

4,893,197	5,185,780	5,216,744	5,274,738	5,289,368	5,325,292	5,339,203
5,396,371	5,446,603	5,457,782	5,590,188	5,819,005	5,911,134	5,937,029
6,044,355	6,115,746	6,122,665	6,192,346	6,246,752	6,249,570	6,252,946
6,252,947	6,330,025	6,542,602	6,564,368	6,694,374	6,728,345	6,775,372
6,785,369	6,785,370	6,856,343	6,865,604	6,870,920	6,871,229	6,880,004
6,937,706	6,959,079	6,965,886	6,970,829	7,010,106	7,010,109	7,058,589
7,085,728	7,203,655	7,240,328	7,305,082			

360^o View, ACTIMIZE, Actimize logo, Alpha, Customer Feedback, Dispatcher Assessment, Encorder, eNiceLink, Executive Connect, Executive Insight, FAST, FAST alpha Blue, FAST alpha Silver, FAST Video Security, Freedom, Freedom Connect, IEX, Interaction Capture Unit, Insight from Interactions, Investigator, Last Message Replay, Mirra, My Universe, NICE, NICE logo, NICE Analyzer, NiceCall, NiceCall Focus, NiceCLS, NICE Inform, NICE Learning, NiceLog, NICE Perform, NiceScreen, NICE SmartCenter, NICE Storage Center, NiceTrack, NiceUniverse, NiceUniverse Compact, NiceVision, NiceVision Alto, NiceVision Analytics, NiceVision ControlCenter, NiceVision Digital, NiceVision Harmony, NiceVision Mobile, NiceVision Net, NiceVision NVSAT, NiceVision Pro, Performix, Playback Organizer, Renaissance, Scenario Replay, ScreenSense, Tienna, TotalNet, TotalView, Universe, Wordnet are trademarks and registered trademarks of NICE Systems Ltd. All other registered and unregistered trademarks are the property of their respective owners.

Applications to register certain of these marks have been filed in certain countries, including Australia, Brazil, the European Union, Israel, Japan, Mexico, Argentina and the United States. Some of such registrations have matured to registrations.

385A0681-01 Rev. A0

For assistance please contact your local supplier or the nearest **NICE Systems Customer Service Center**:

EMEA Region: (Europe, Middle East, Africa)

Tel: +972-9-775-3800
Fax: +972-9-775-3000
email: support@nice.com

APAC Region: (Asia/Pacific)

Tel: +852-8338-9818
Fax: +852-2802-1800
email: support.apac@nice.com

The Americas Region: (North, Central, South America)

Tel: 1-800-NICE-611
Fax: +720-264-4012
email: support.americas@nice.com

Israel:

Tel: 09-775-3333
Fax: 09-775-3000
email: support_helpdesk@nice.com

*NICE invites you to join the **NICE User Group (NUG)**.*

Visit the NUG Website at www.niceusergroup.org, and follow the instructions.

For general information on NICE Systems products please contact your local distributor or the nearest NICE Systems office:

International Headquarters-Israel

Tel: +972-9-775-3100
Fax: +972-9-775-3070
email: info@nice.com

United Kingdom

Tel: +44-8707-22-4000
Fax: +44-8707-22-4500

France

Tel: +33-(0)1-41-38-5000
Fax: +33-(0)1-41-38-5001

North America

Tel: 1-800-663-5601
Fax: +201-356-2197
email: na_sales@nice.com

Germany

Tel: +49-(0)-69-97177-0
Fax: +49-(0)-69-97177-200

Hong-Kong

Tel: +852-2598-3838
Fax: +852-2802-1800

Please send all queries, comments, and suggestions pertaining to this document to nicebooks@nice.com

Please visit NICE at www.nice.com

Contents

1

Introduction	11
Overview	12
How does Cisco's IP Phone Active Recording work?	12
Terms and Concepts	13
You are Here	16
Cisco IP Phone-Based Active Recording Integration Workflow	17
Standard Cisco IP Phone-Based Active Recording System Architecture	18
Components	19
Cisco	19
NICE Perform Release 3	19
How Does the Integration Work?	21
System Startup	21
Step 1	21
Step 2	22
Recording Solutions	23
Total Recording	23
Overview	23
In Depth	23
Interaction-based Recording	26
Overview	26
In Depth	26

2

Configuring the CISCO Unified Communications Manager	29
Defining an End User (nicecti User)	30
Associating User Groups with the End User	33

Defining the CUCM for Cisco IP Phone-based Active Recording	35
Defining a SIP Trunk	35
Defining the Recording Profile	38
Defining a Route Group	40
Defining a New Route List	42
Defining a New Route Pattern	44
Configuring the Built In Bridge (BIB) on the IP Phone	46
Configuring the Built In Bridge on a System-Wide Level	46
Configuring the Built In Bridge on a Device Level	48
Associating the Recording Profile with the Recorded Device Number & Selecting Recording Method	50
Configuring the Phone Device Notification Tones	52
Defining Notification Tones	52

3

Installing the TSP Client on the NICE Interactions Center **57**

Installing and Configuring the Telephone Services Provider (TSP) Client .58	.58
Downloading the TSP Client	58
How Many TSP Clients Do I Need?	59
Installing the TSP Client	60
Configuring the TSP Client	64
Verifying the TSP Client Configuration	67

4

Installing and Configuring the MPCM (FLM) **69**

MPCM (FLM) System Requirements	70
Installing the MPCM (FLM)	71

5

Configuring the Logger **77**

Configuring the Active VoIP Logger	78
Configuring the Ports	79
Network Preparations	80
SIP Configuration	80

6

Configuring the CTI Integrations for Cisco IP Phone-Based Active Recording Solution **81**

Before you Begin	82
CTI Interface Configuration	82
TSAPI Ports	83
Connection Manager Configuration	83
Driver Configuration	83
SNMP Service Installation	83
Configuring the Integration Package	84
Configuring the CTI Interface	85
Monitoring ACDs (Hunt Groups)	95
Monitoring IVRs (CTI Ports)	96
Monitoring Pickup Groups	96
Configuring the Connection Manager	97
Configuring the Driver	101
Extension Mobility Guidelines	101
Creating the Driver	101
Configuring for Cisco IP Phone-based Active Recording	109
Configuring a Connection Manager for the VRSP (FSP)	109
Configuring the Media Provider Controller	114
Installing the NICE Integration Software	121

7

Using Redundancy **131**

Overview	132
Redundancy Workflow	133
VRSP (FSP) Redundancy	134
How does it function?	134
VRSP (FSP) Requirements	134
Configuring VRSP (FSP) for Redundancy	135
Configuring VRSP (FSP) Redundancy in the Cisco Environment	135
Configuring VRSP (FSP) Redundancy in the NICE Environment	137
Installing the NICE Integration Software on the Primary VRSP (FSP) ..	137

Configure the Primary VRSP (FSP)	137
Configure the Redundant VRSP (FSP) on the NICE Integrations Center ..	139

8

NICE Testing and Debugging Tools **141**

NICE Events Spy	142
Setting Up the Events Spy	142
Receiving Events	144
Saving Events	145
Setting up the SimCTILink Tool	146
NICE Debug Service	147
Setting Up the NICE Debug Service	147
Accessing the NICE Debug Service	152
Connection Manager Monitor	153
Setting Up the Connection Manager Monitor	153
Managing the Connection Manager Monitor	158
Log Manager System	159
CTI Console Viewer	159
Log Manager	162
Log Manager Services	164
Log Viewer	164
CAPI Spy	166
CAPI Spy Plug-in	166
CAPI Spy Utility	169
Changing Connection Details	171
TAPIMonitor	171

9

Troubleshooting **173**

TAPI Troubleshooting	174
VRSP (FSP) Troubleshooting	175
VRSP (FSP) Error Codes	175
VRSP SNMP Messages	175

Total Recording Troubleshooting	176
Flow of Information through the Log Files	176
VRSP (FSP) Log File	177
MPCM (FLM) Log File	177
CUCM SIP Invite to VRSP in the VRSP (FSP) Log Files	178
RCM <> Call Server <> MPCM	179
Call Server Log File	179
RCM Log File	179
RCM <> VoIP Logger <> VRSP	180
IPCapture Process Log File	181
New Call Scenario	181
VRSP (FSP) Log File - CUCM and VRSP SIP Communication	181
VRSP (FSP) Log File	182
Ethereal Sniffing Tool Examples	183
Interaction-Based Recording Troubleshooting	185
Flow of Information through the Log Files	185
New Call	186
RCM <> VoIP Logger <> VRSP	186

A

<i>Cisco Additional Parameters</i>	187
CTI Interface - Additional Switch Parameters	188
Importing Available Devices from the Switch	190
Importing Text Files	191
Reporting Levels	193
Connection Manager - Additional Parameters	195
Connection Manager - Interface Parameters	197
Configure Connection Manager - Interface Parameters	197
Driver - Additional Driver Parameters	199
Driver - CTI Analysis Parameters	201
Driver Interface - Additional Driver Switch Parameters	203

B

Defining an AXL - Application User **205**

C

Channel Mapping Guidelines **211**

Index **213**

Introduction

This guide describes the Cisco IP Phone-based integration with NICE.



NOTE: For an updated list of supported versions, refer to the Integration Description Document (IDD).

Contents

Overview	12
How does Cisco's IP Phone Active Recording work?	12
Terms and Concepts	13
You are Here	16
Cisco IP Phone-Based Active Recording Integration Workflow	17
Standard Cisco IP Phone-Based Active Recording System Architecture	18
Standard Cisco IP Phone-Based Active Recording System Architecture	18
Components	19

Overview

In Active VoIP recording solutions, a replica of the RTP packets is sent directly to the VoIP logger. As replications of many calls can be sent to one IP address (of the VoIP Logger), the calls are distinguished from one another by associating each call to a pair of ports (stereo: Rx and Tx).

In Cisco's IP Phone-based Active Recording solution, the Cisco IP phones fork the two separate voice streams of the Agent and Customer (Rx and Tx) from the agent's phone to the VoIP Logger. The agent's phone can be recorded and monitored at the same time. The agent and/or customer can be notified that they are being recorded by a beep tone. (The monitoring described here is Cisco's monitoring which is totally different from NICE's monitoring. NICE's monitoring is also available.)

Both Total recording and Interaction-based recording can be used. In addition, both internal and external calls can be recorded.

The recording can be either stereo or summed. This decision depends on the VoIP logger's configuration.

How does Cisco's IP Phone Active Recording work?

When the agent talks to the customer, the Cisco Unified Communications Manager (CUCM) sets up an additional call between the agent's phone and the NICE SIP Proxy (Voice Recording SIP Proxy - VRSP/FSP). The voice itself is replicated at the phone's BIB (Built in Bridge) and sent to the VoIP Logger IP address.

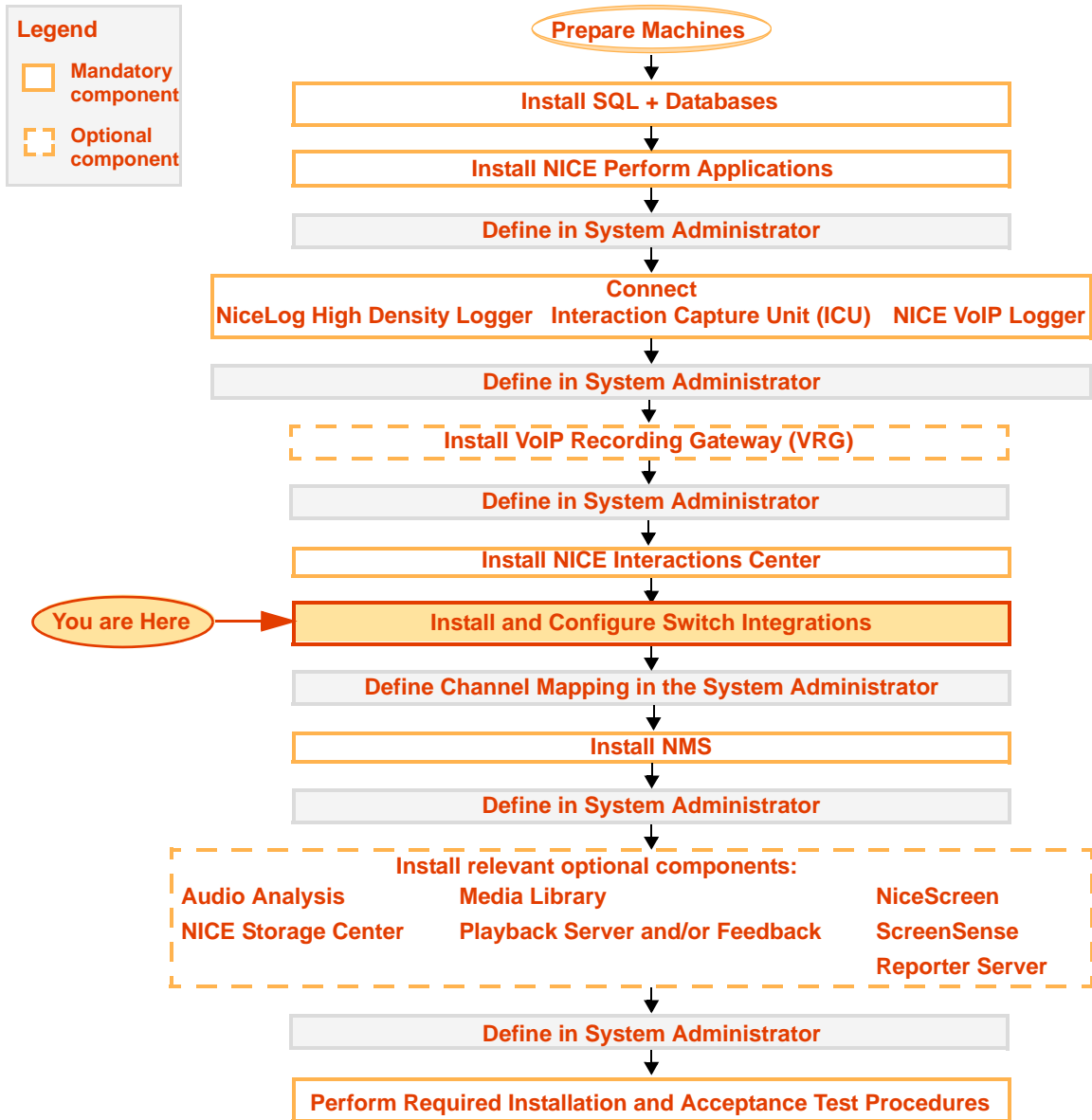
Terms and Concepts

ACD	Automatic Call Distributor. A device that distributes incoming calls to a specific group of terminals that agents use. The ACD is assigned a number which is used for referral purposes.
Active VoIP Recording	In Active VoIP Recording , audio packets are sent directly to the VoIP Logger's IP address.
AXL	<p>The AXL client is used to facilitate channel mapping. It enables the importing of <i>all</i> Unique Device IDs from the Call Manager (i.e. you import the Unique Device IDs straight from the switch).</p> <p>The AXL client does not look at which devices are attached to which TSP client. If you have several TSP clients and different devices are attached to each one, AXL ignores this and only looks at the devices that are attached to the switch.</p>
CTI port	CTI ports as virtual devices can have one or more virtual lines, and software-based CUCM applications. You configure CTI ports by using the same CUCM Administration windows as you use to configure phones. For first-party call control, you must add a CTI port for each active voice line. For more information regarding configuring CTI ports, consult your Cisco site engineer.
CTI Route Point	A CTI route point virtual device can receive multiple, simultaneous calls for application-controlled redirection. You can configure one or more lines on a CTI route point that users can call to access the application. Applications can answer calls at a route point and can also redirect calls to a CTI port or IP phone. Route points can receive multiple, simultaneous calls. Applications that want to terminate media for calls at route points must specify the media and port for the call on a per-call basis. For more information regarding configuring CTI Route Points, consult your Cisco site engineer.
CUCM	Cisco Unified Communications Manager: Software-based call-processing component of the Cisco IP telephony solution.
DN	Device Number
FLM	Forwarding Location Manager (replaced by the MPCM)
FSP (VRSP)	Forward SIP Proxy. Reflects the VoIP Logger as an end point to the CUCM. All call sessions are opened in front of it.
Hunt Group	A group of phones programmed in the PABX where calls are diverted to any phone within the group.
IP Capture	A module within NICE Perform Release 3, responsible for capturing the RTP stream, processing it, and storing it for future use in the system.

IVR	Interactive Voice Response
MAC Address	Medium Access Control Address. A MAC Address is a 48-bit number which is unique to the LAN NIC card.
Mirroring	The process whereby all received and transmitted packets are copied from one or more source ports to a predefined destination port.
MPCM	Media Provider Controller Manager
Pickup Group	Allows you to answer a call that comes in on a directory number other than your own. When you hear an incoming call ringing on another phone, you can redirect the call to your phone by using this feature.
RCM	Resource Coordination Manager. A server for allocating channels for recording.
SDP	Session Description Protocol describes streaming media initialization parameters.
SEP	Prefix that arrives before the MAC Address.
Shared lines	<p>You can set up one or more lines with a shared-line appearance. A CUCM system considers a directory number to be a shared line if it appears on more than one device in the <i>same</i> partition.</p> <p>In a shared-line appearance, for example, you can set up a shared line, so a directory number appears on line 1 of a manager phone and also on line 2 of an assistant phone. Another example of a shared line involves a single incoming 800 number that is set up to appear as line 2 on every sales representative phone in an office.</p>
SIP	Session Initiation Protocol. The SIP Protocol is a textual signalling protocol used to establish, maintain, and terminate sessions. The SIP invitation can be used to establish sessions and carry session description. The default port is 5060.
SIP Proxy	Used to set up SIP based calls. The NICE VRSP integrates Cisco's active recording protocol with NICE's SIP-based recording protocol.
SIP Trunk	Delivers the signalling of numerous calls.
SPAN	Switched Port Analyzer (Cisco term): SPAN mirrors traffic on one or more source ports to a destination port for analysis.
TAPI (Microsoft)	Telephony Application Programming Interface (Microsoft application): CTI interface used in the NICE integration with the Communications Manager.
UID	Unique Device ID that shows the physical device identity. It is constructed from SEP and MAC Address.

URI	Uniform Resource Identifier - a formatted string that identifies via name, location, or other characteristic, a resource on the Internet. Also known as URL and URN.
VRA	VoIP Recording Agent (VRA): Forwarding device or Media Provider Controller (MPC), capable of filtering and routing RTP audio packets from one IP extension on the network to a centralized active recording VoIP Logger.
VRG	VoIP Recording Gateway (VRG): Forwarding device or Media Provider Controller (MPC), capable of filtering and routing RTP audio packets from multiple IP extensions on the network to a centralized active recording VoIP Logger.
VRSP (FSP)	Voice Recording SIP Proxy: Reflects the VoIP Logger as an end point to the CUCM. All call sessions are opened in front of it.

You are Here



NOTE:

Refer to the *Site Installation Workflow Guide* for a detailed overview of the NICE Perform site installation workflow.

The *Site Installation Workflow Guide* provides general guidelines and procedures for installing NICE Perform at your site, and indicates the exact point during site installation at which to perform switch integrations.

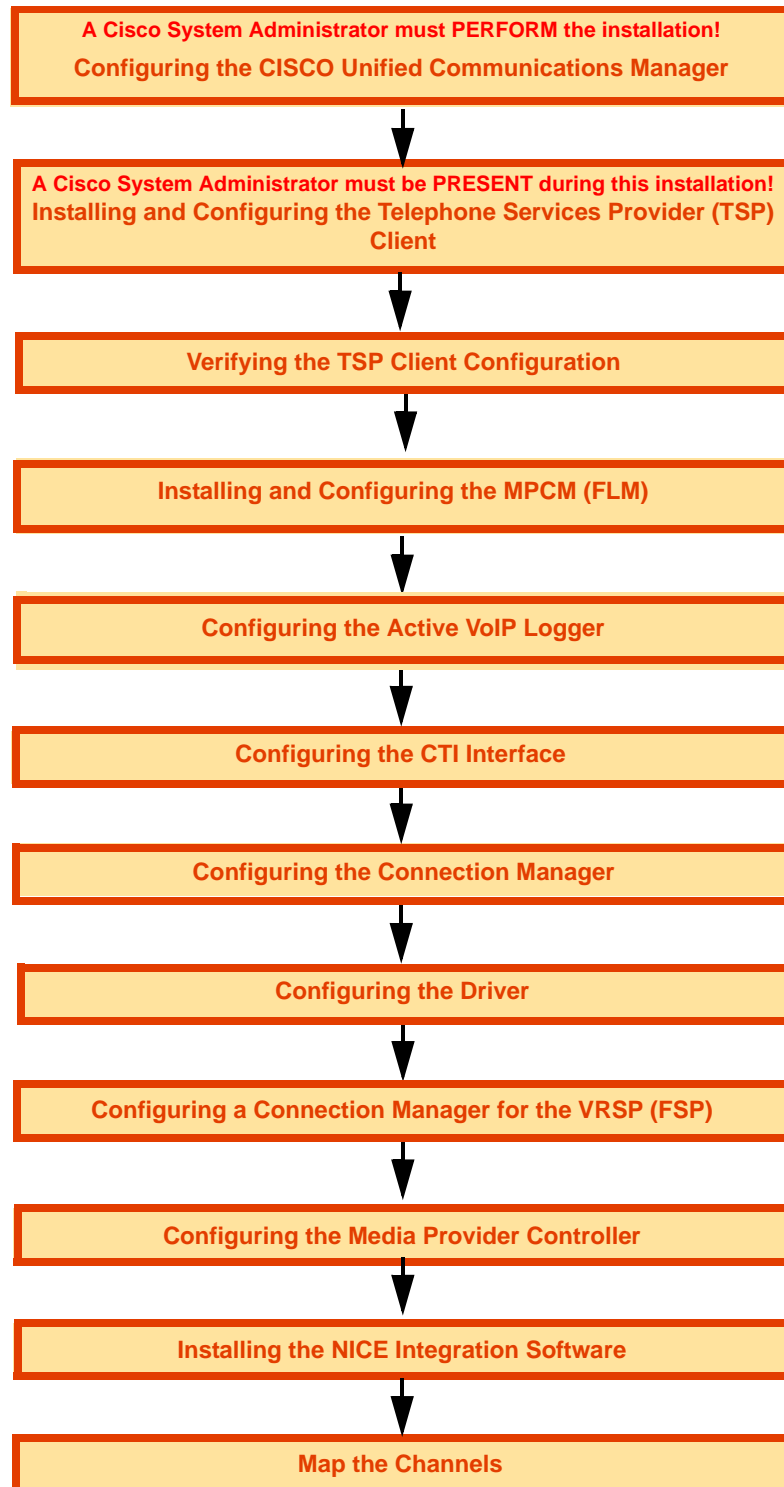
Cisco IP Phone-Based Active Recording Integration Workflow

The following flow details the components required in the Cisco Active Recording IP Phone-based integration.

Legend:

□ Mandatory component (with link to procedure in this publication)

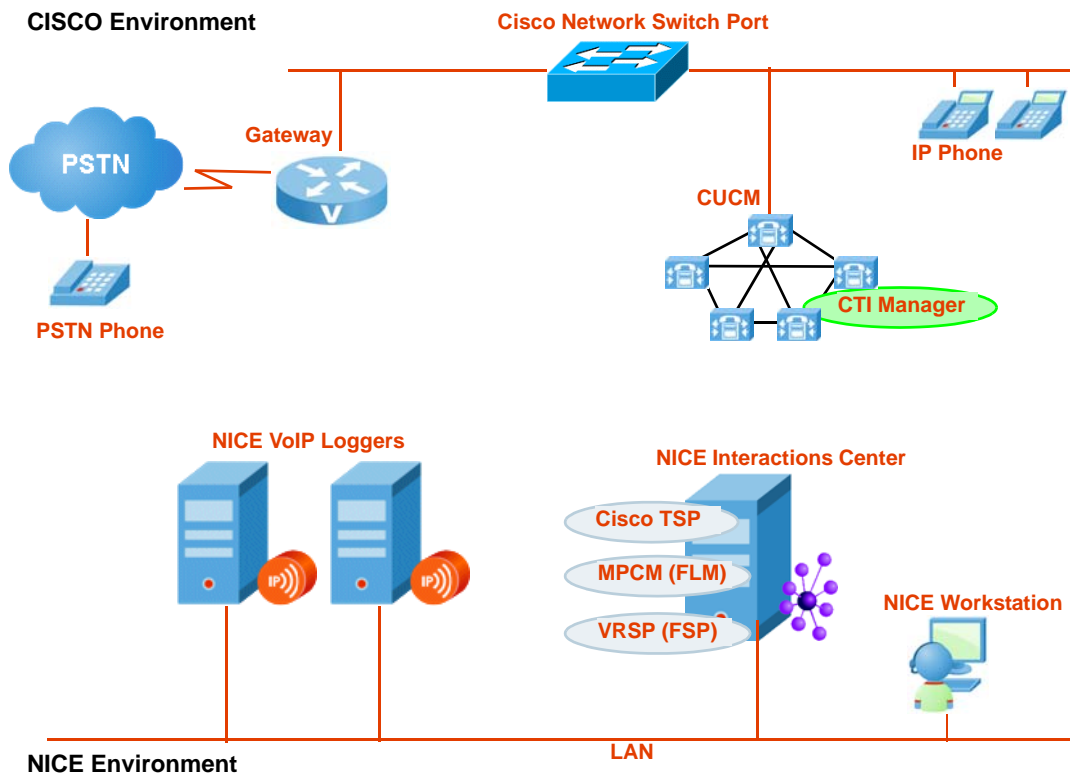
[] Optional component



Standard Cisco IP Phone-Based Active Recording System Architecture

This is the basic Cisco IP Phone-based active recording system architecture. Note, that this diagram does not show the Database Server, Application Server, and so on, but only shows the relevant components for this integration.

Figure 1-1 Standard System Architecture



NOTE: The CTI Manager may be an independent server or it may be a service running on the Communications Manager.

Components

Cisco

Cisco Unified Communications Manager (CUCM) version 6.0 and above

CUCM version 6.0 does *not* currently support call monitoring or recording for any device that is enabled for *security*. This includes secured signalling and/or secured media.

Cisco IP Phone

The following third-generation IP phones are supported in this integration: 7911G, 7931G, 7941G, 7941G-GE, 7961G, 7961G-GE, 7970G, 7971G-GE, 7975, 7965, 7945, 7962, 7942. For a complete list of supported IP phones, consult your Cisco representative.

Cisco Softphone

Recording of the Cisco Communicator (softphone) is not supported by CUCM 6.0

NICE Perform Release 3

The new and relevant components for this integration are:

MPCM (FLM)

The MPCM (FLM) is a repository for all media sources i.e. phones reported by NICE's different forwarding devices e.g. the VRSP (FSP), VRG, VRA. The MPCM (FLM) is always installed on the NICE Interactions Center.

For more information regarding how the MPCM (FLM) and the VRSP (FSP) interact, see [System Startup](#) on [page 21](#).

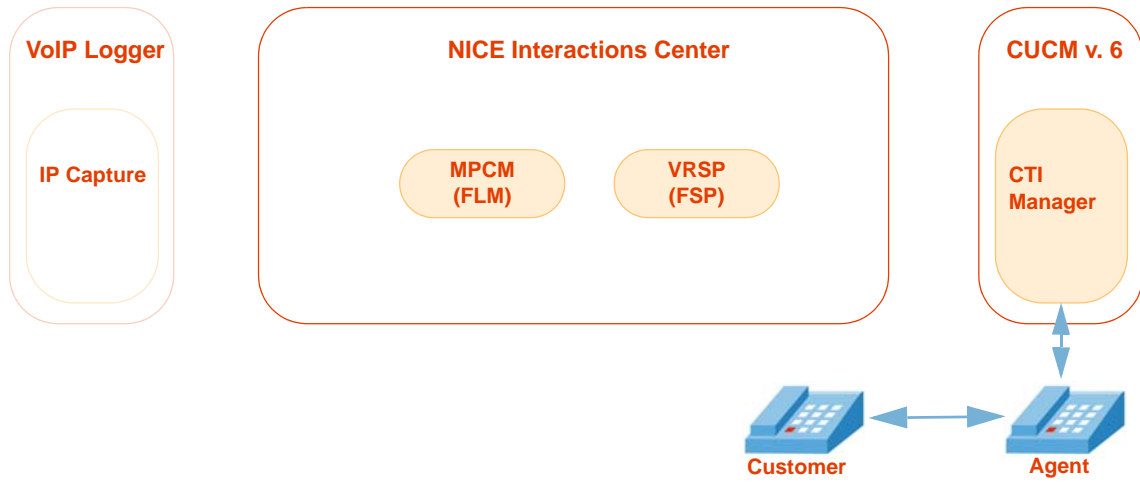
For more information, regarding the information that MPCM (FLM) saves, see [MPCM \(FLM\) Log File](#) on [page 177](#).

VRSP (FSP)

The VRSP (FSP) functions as a SIP Proxy. It is used to setup SIP-based calls between the CUCM and the NICE VoIP Logger.

In the standard configuration when VRSP (FSP) redundancy is not needed, the VRSP (FSP) is installed on the NICE Interactions Center. (When redundancy is used, a different configuration is used, see [Configuring VRSP \(FSP\) for Redundancy](#) on [page 135](#).)

Figure 1-2 VRSP (FSP) and MPCM (FLM) - Part of the NICE Interactions Center



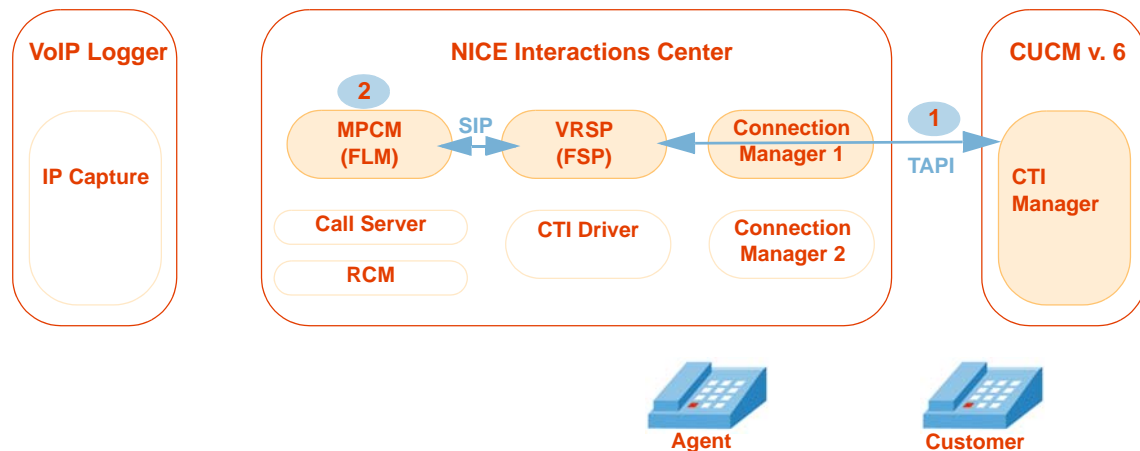
How Does the Integration Work?

System Startup

Step 1

At system startup, NICE acquires all the monitored extensions from the CUCM.

Figure 1-3 VRSP (FSP) on System Startup

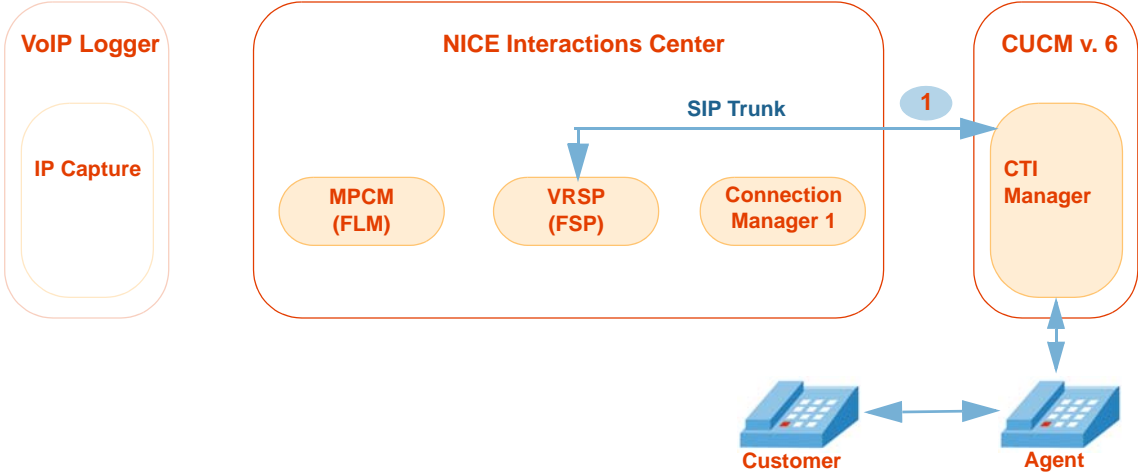


- 1 The VRSP (FSP) acquires all extension numbers from the TAPI user (**nicecti user**). For each one of these extensions, the VRSP (FSP) saves the following data:
 - Device Number (DN)
 - Unique Device ID (UID): Consisting of the SEP and MAC address
 - Recording mode - Automatic Recording or Application Invocation *only*
- 2 VRSP (FSP) then forwards this information to the MPCM (FLM).

For more information, regarding the data that VRSP (FSP) saves, see **VRSP (FSP) Log File** on [page 177](#) and **MPCM (FLM) Log File** on [page 177](#).

Step 2

Figure 1-4 VRSP Receives an Invite Message from the CUCM



- 1 An Invite message is first sent from the CUCM to the VRSP (FSP). This means that the CUCM is now waiting for the VoIP Logger information. This information will arrive at the beginning of a call as will be described in **Flow of New Call Recording** on **page 25**.

For more information, regarding the **Invite** message that VRSP (FSP) receives, see **CUCM SIP Invite to VRSP in the VRSP (FSP) Log Files** on **page 178**.

Recording Solutions

Integration of the NICE Interactions Center and the CUCM can be carried out in the following environments, each of which supports different recording solutions.

Total Recording

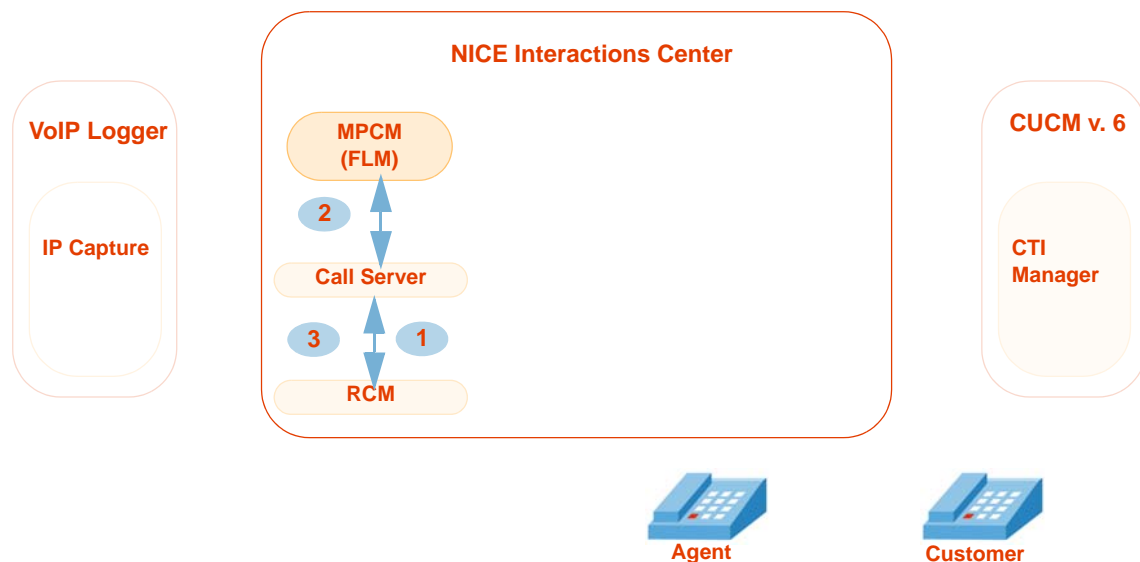
Overview

In Total recording when the agent calls the customer, the CUCM invites the VRSP (FSP) to both the customer and the agent calls (Rx and Tx) at the beginning of each call. The VRSP (FSP) accepts the calls and replies with the VoIP Logger IP address and a port for each call. The CUCM automatically sends two call setup messages to the agent phone's BIB. The first call is to the agent stream, the second call is to the customer stream. The phone then sends two RTP streams to the VoIP Logger.

In Depth

Flow of Information Between RCM, Call Server, and MPCM (FLM)

Figure 1-5 RCM <> Call Server <> MPCM (FLM)



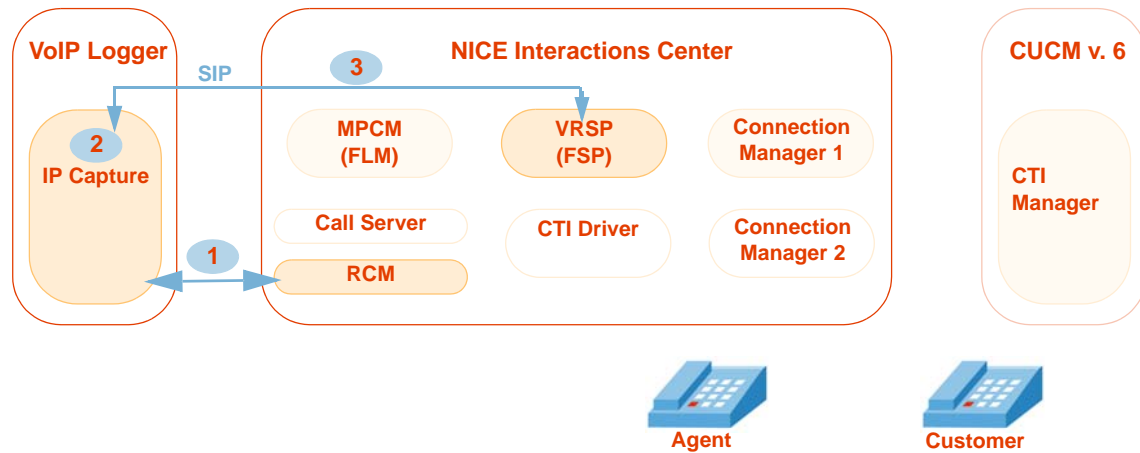
On system initiation, the following steps occur:

- 1 Channel Mapping sends a list of UIDs to the Call Server.
- 2 For each UID the Call Server asks the MPCM for the address of the VRSP that witnessed that UID.
- 3 The Call Server informs the RCM about the UID, DN and VRSP addresses.

To view the log files of these interactions, see **Call Server Log File** on [page 179](#) and **RCM Log File** on [page 179](#).

Flow of Information Between RCM, VoIP Logger, and VRSP (FSP)

Figure 1-6 RCM <> VoIP Logger <> VRSP (FSP)

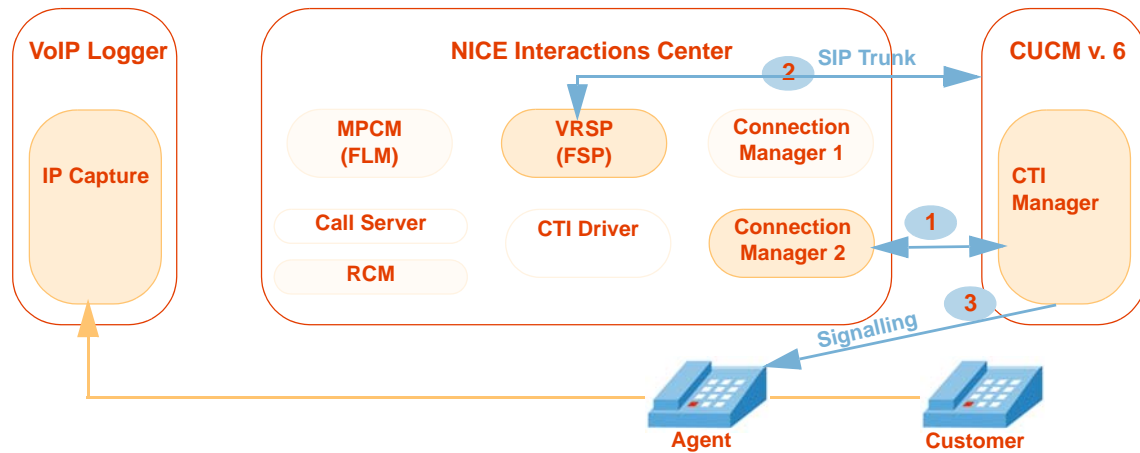


- 1 On initiation of one of the components or after changes in the Channel Mapping, the RCM forwards the UID and the VRSP information to the VoIP Logger.
- 2 The IPCapture process on the VoIP Logger allocates two ports for each UID and VRSP entry.
- 3 The IPCapture process on the VoIP Logger sends the forwarding command to the VRSP (FSP). This command contains a Session Description Protocol (SDP) which consists of the UID and VoIP Logger IP addresses and ports.

To view the log files of these interactions, see **IPCapture Process Log File** on **page 181** and **VRSP (FSP) Log File** on **page 182**.

Flow of New Call Recording

Figure 1-7 New Call Scenario



- 1 The **Start Call** event arrives via TAPI and the call is reported to the Interactions Center.
- 2 The CUCM asks the VRSP (FSP) for the VoIP Logger IP address and ports of the UID that need to be recorded. It does this by sending an **Invite** SIP message.
- 3 The CUCM instructs the phone to send two RTP streams to the VoIP Logger IP address and ports.

To view the log files and examples of these interactions, see **VRSP (FSP) Log File - CUCM and VRSP SIP Communication** on [page 181](#) and **Ethereal Sniffing Tool Examples** on [page 183](#).

Interaction-based Recording

Overview

In Interaction-based recording when the agent calls the customer, the Selective, QM or ROD recording is triggered in the NICE Interactions Center. The CUCM invites the VRSP (FSP) to both the customer and the agent calls (Rx and Tx). The VRSP (FSP) accepts the calls and replies with the VoIP Logger IP address and a ports. The CUCM automatically sends two call setup messages to the agent phone's BIB. The first call is to the agent stream, the second call is to the customer stream. The phone then sends two RTP streams to the VoIP Logger.

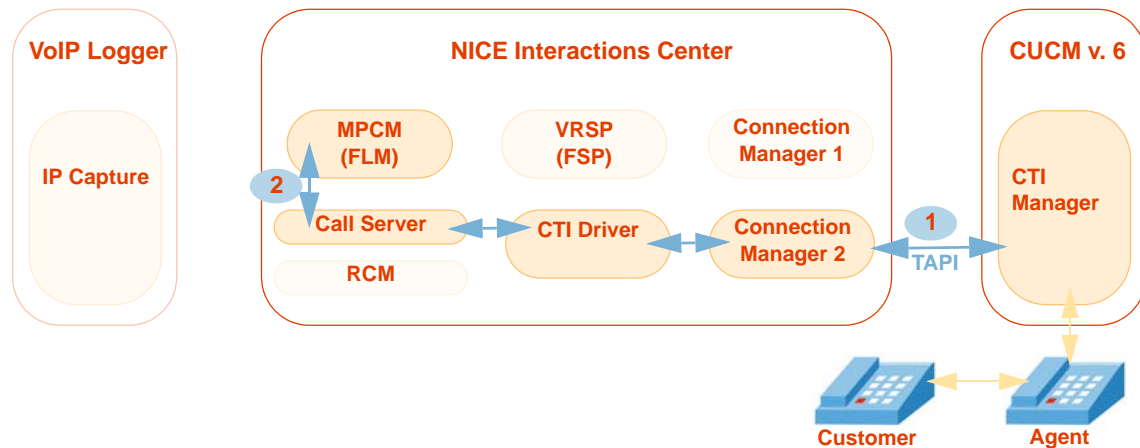
In Depth

Whenever a call is established on a line appearance that has been configured for **Application Invocation** recording (**Interaction-based recording**), the following steps occur:

- 1 After initiation, the MPCM (FLM) contains the DN, UID and Forwarding Device ID. See **MPCM (FLM) Log File** on [page 177](#).
- 2 The new call takes place, see **New Call Flow** on [page 26](#).

New Call Flow

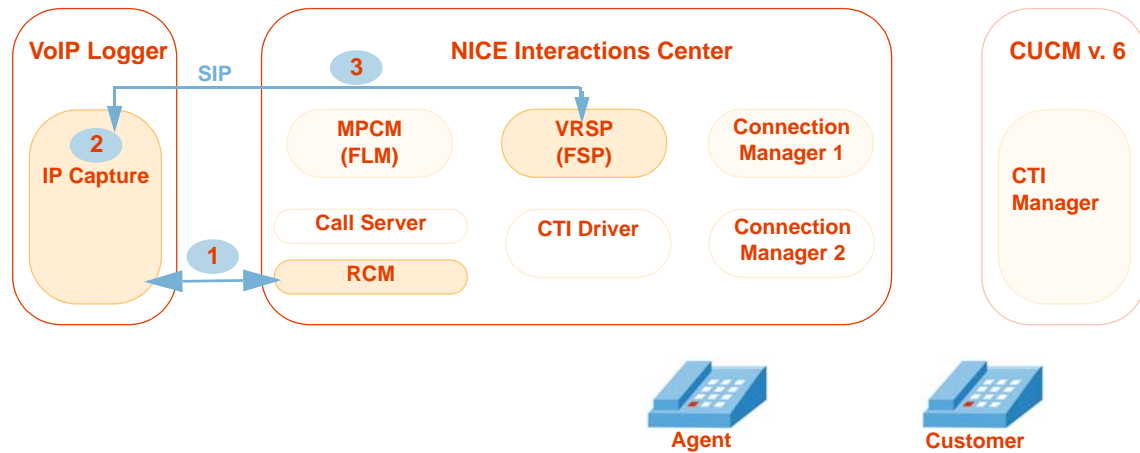
Figure 1-8 New Call Scenario



- 1 The **Start Call** event arrives at the Interactions Center via TAPI.
- 2 The Call Server asks the MPCM (FLM) for the address of the VRSP (FSP) that witnessed the **Start Call** event.

Flow of Information Between RCM, VoIP Logger, and VRSP (FSP)

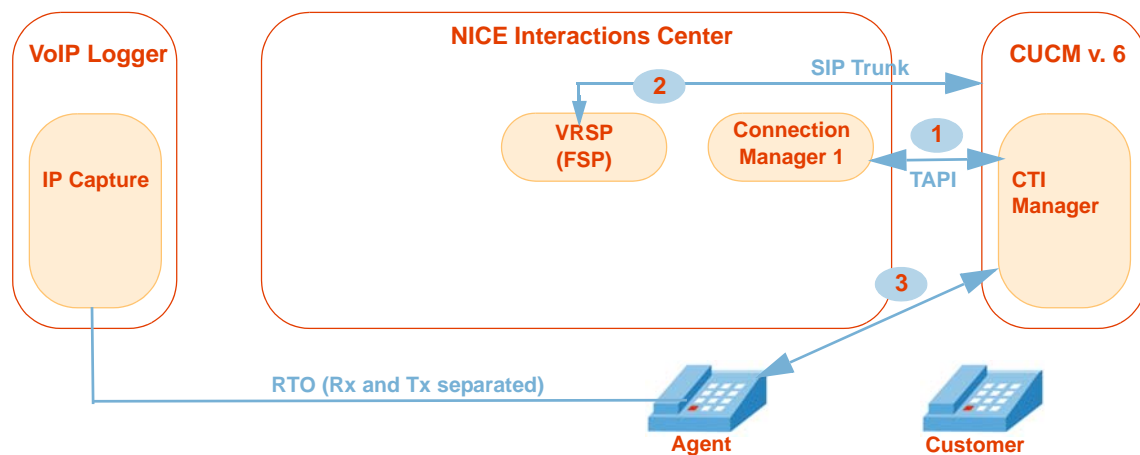
Figure 1-9 RCM <> VoIP Logger <> VRSP (FSP)



- 1 The RCM forwards the UID, DN, VRSP (FSP), and Call ID information to the VoIP Logger.
- 2 The IPCapture process on the VoIP Logger allocates two ports for each UID, DN, VRSP (FSP), and Call ID entry.
- 3 The IPCapture process on the VoIP Logger sends the forwarding command to the VRSP (FSP). This command contains a Session Description Protocol (SDP) which consists of the DN@SEP, VoIP Logger IP addresses, ports, and Call ID.

Flow of Information During “Start Record” Command

Figure 1-10 Start Record Command



- 1 The VRSP sends the **Start Record** command to CUCM, via TAPI.
- 2 The CUCM asks the VRSP (FSP) for the VoIP Logger IP address and ports of the UID to be recorded.
- 3 The CUCM instructs the phone to send two RTP streams to the VoIP Logger IP address and ports.

Configuring the CISCO Unified Communications Manager

Before you integrate Cisco's IP Phone-based Active Recording solution and NICE Perform Release 3, you need to prepare the CUCM environment. This chapter provides guidelines for configuring the Cisco Unified Communications Manager (CUCM) for integration with NICE Interactions Center.



IMPORTANT

A Cisco System Administrator must perform the CUCM configuration!

Contents

Defining an End User (nicecti User)	30
Defining a SIP Trunk	35
Defining a SIP Trunk	35
Defining the Recording Profile	38
Defining a Route Group	40
Defining a New Route List.....	42
Defining a New Route Pattern.....	44
Configuring the Built In Bridge (BIB) on the IP Phone	46
Associating the Recording Profile with the Recorded Device Number & Selecting Recording Method.....	50
Configuring the Phone Device Notification Tones	52
Defining Notification Tones.....	52

Defining an End User (nicecti User)

You now define a new end user for the CUCM. This user will be used to communicate between the CUCM and TSP Client on the NICE Interactions Center.

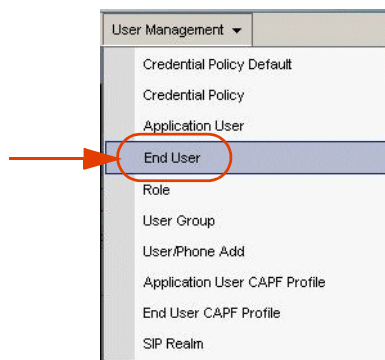


NOTE: In NICE Perform, the end user that you configure here is referred to as the nicecti user.

To define a new end user:

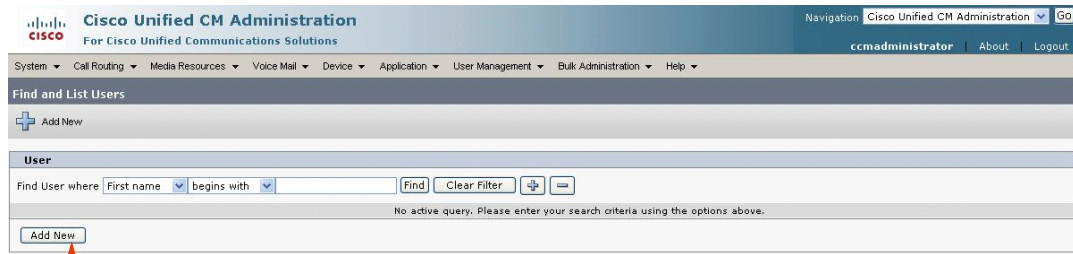
1. Log in to the CUCM Administration application.
2. From the **User Management** menu, choose **End User**.

Figure 2-1 Choosing End User



The Find and List Users window appears.

Figure 2-2 Find and List Users Window - Add New



Click Add New

3. Click **Add New**. The End User Configuration window appears.

4. In the **User Information** area, complete the following fields:

Figure 2-3 End User Configuration - User Information Area

The screenshot shows the 'End User Configuration' interface. At the top, there are buttons for 'Save', 'Delete', and 'Add New'. Below that is a 'Status' section showing 'Status: Ready'. The main area is titled 'User Information' and contains several input fields:

- User ID***: Contains 'nicecti'. A red arrow points to this field.
- Password**: Masked with dots. An 'Edit Credential' button is to its right.
- Confirm Password**: Masked with dots. An 'Edit Credential' button is to its right.
- PIN**: Masked with dots.
- Confirm PIN**: Masked with dots.
- Last name***: Contains 'nicecti'. A red arrow points to this field.
- Mail ID**: Empty.
- Manager User ID**: Empty.
- Department**: Empty.
- User Locale**: Set to '< None >'.
- Associated PC**: Empty.
- Digest Credentials**: Empty.
- Confirm Digest Credentials**: Empty.

- a. In the **User ID** field, type **nicecti**.
 - b. in the **Password** field, type your password.
 - c. In the **PIN** field, type any number that Cisco requires. This number is not relevant to our installation.
 - d. In the **Confirm PIN** field, type the PIN number again to confirm it.
 - e. In the **Last name** field, type **nicecti**.
5. All devices, that you want to record, have to be defined here as monitored devices. The monitored devices must be associated with this new user. Perform the following steps:
 - a. Scroll down to the **Device Associations** area and click **Device Association**.

Figure 2-4 Device Associations Area

The screenshot shows the 'Device Associations' section. It has a sub-header 'Controlled Devices' and a list box containing two device IDs: 'SEP0014F245036F' and 'SEP0019306F65E7'. To the right of the list box is a button labeled 'Device Association'. A red arrow points from the text 'Click Device Association' to this button.

A new Search Options window appears.

- b. In the **Search Options** area, search for the telephones and CTI ports that need to be monitored. Click **Find**. The User Device Association window appears.

Figure 2-5 User Device Association window - Search Options Area

The screenshot shows the 'User Device Association' window. At the top, there are buttons for 'Select All', 'Clear All', 'Select All In Search', 'Clear All In Search', 'Save Selected/Changes', and 'Remove All Associat'. Below this is a 'Status' section indicating '258 records found'. The 'Search Options' section includes a search bar with 'FindUser Device Association where Name begins with' and a 'Find' button. The main area is titled 'Device association for Suzy Wong' and contains a table of devices. Red arrows point to the 'Find' button and to the checkboxes in the table.

Device Name	Directory Number	Description
IPCC_80001	80001	JTAPI Group #0-1
IPCC_80002	80002	JTAPI Group #0-1
IPCC_80003	80003	JTAPI Group #0-1
IPCC_80004	80004	JTAPI Group #0-1
IPCC_80005	80005	JTAPI Group #0-1
RP_70000	70000	RP_70000
RP_80000	80000	RP_80000
RP_80100	80100	RP_80100
SEP0002FD06EAB0	6024	Wong-6020
SEP0017E0355A6F	6018	Wong-6018
SEP003094C30FBE	6019	Wong-6019
SEP0001956AF51D	6014	Gill-6014
SEP00036BAAD439	6069	SEP00036BAAD439
SEP000B8207A7B8	6020	GXP-2000-1

6. Mark the relevant devices.
7. Click **Save Selected/Changes**.
8. In the **Extension Mobility** area, ensure that the **Allow Control of Device from CTI** checkbox is marked, see below. For information regarding setting up Extension Mobility on the NICE side, see [Extension Mobility Guidelines](#) on page 101.

Figure 2-6 Extension Mobility Area

The screenshot shows the 'Extension Mobility' section of the configuration window. It includes fields for 'Controlled Devices', 'Available Profiles', and 'Controlled Profiles'. A red arrow points to the 'Extension Mobility' section header. Another red arrow points to the 'Allow Control of Device from CTI' checkbox, which is checked.

9. Click **Save**.

A new end user is created. The new user's information appears in the End User Configuration window.

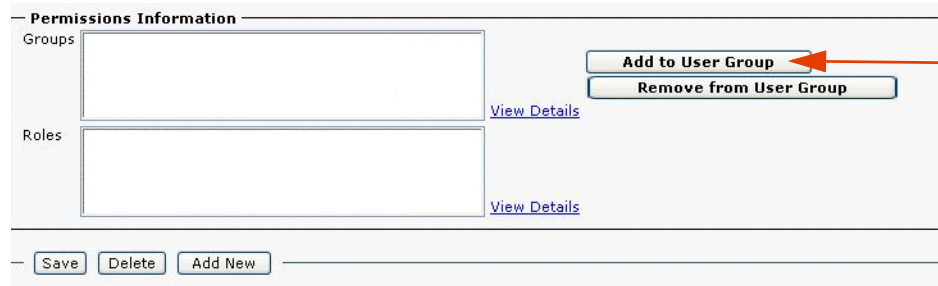
Associating User Groups with the End User

User Groups have roles associated with them. A user group can have more than one role associated with it. An end user who is attached to a specific user group, is automatically associated with the roles that are attached to that user group, i.e. User Group **A** includes Roles **1** and **2**. If User Group **A** is associated with an end user, the end user automatically receives Roles **1** and **2**.

To associate the User Group with the end user:

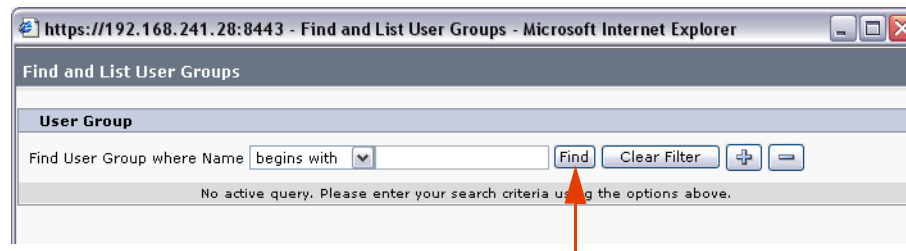
1. In the End User Configuration window, scroll down to the **Permissions Information** area.

Figure 2-7 Permissions Area



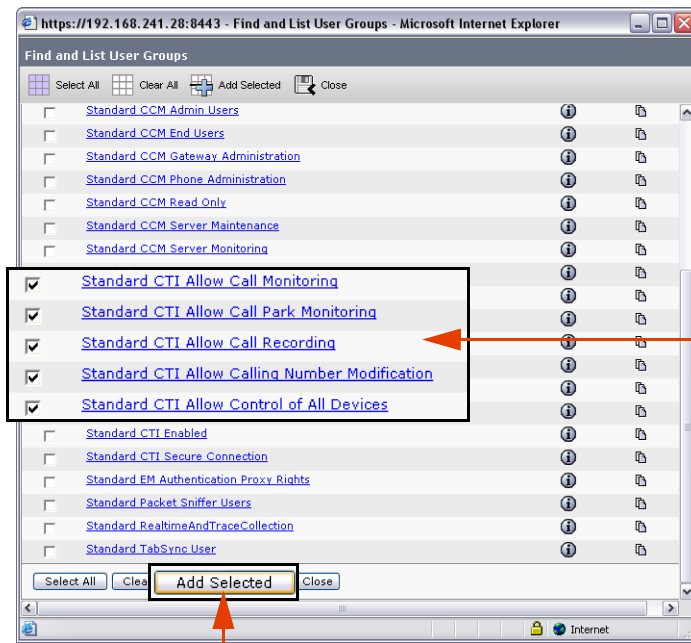
2. Click **Add to User Group**. The Find and List User Groups window appears.

Figure 2-8 Permissions Area



3. Click **Find**.

Figure 2-9 Find and List User Groups



Mark the groups that you want to associate with the end user

Click Add Selected

4. Mark the groups that you need to associate with the end user. The following groups *need* to be associated:
 - **Standard CTI Allow Call Park Monitoring** (for both secured and non-secured connection configurations)
 - **Standard CTI Enabled** (for both secured and non-secured connection configurations)
5. Click **Add Selected**. The window closes.
6. In the **Permissions Information** area, verify that all the groups and roles appear.



NOTE: Check the roles listed in the **Permissions Information** area to ensure that all relevant roles are associated with each user group.



Ensure that Standard CTI Allow Call Park Monitoring is one of the groups.



IMPORTANT

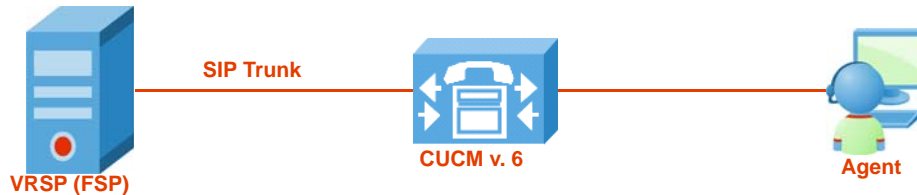
If you need to define an AXL, Application User, for the purposes of channel mapping, see [Defining an AXL - Application User](#) on page 205.

Defining the CUCM for Cisco IP Phone-based Active Recording

This section provides guidelines for defining the CUCM in preparation for the Cisco IP Phone-based Active Recording integration with NICE Perform Release 3.

Defining a SIP Trunk

You need to configure a SIP trunk to connect the CUCM to the VRSP (FSP).



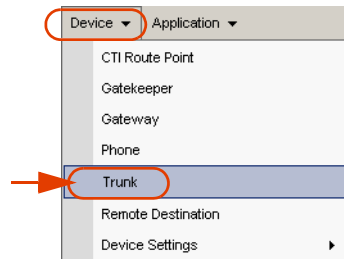
IMPORTANT

If using VRSP (FSP) redundancy, you need to configure two SIP Trunks as each VRSP (FSP) requires its own SIP Trunk. For more information regarding VRSP (FSP) Redundancy, see [VRSP \(FSP\) Redundancy](#) on [page 134](#).

To define a SIP Trunk:

1. From the **Device** menu, choose **Trunk**.

Figure 2-10 Device Menu



The Find and List Trunks window appears.

2. Click **Add New**. The Trunk Configuration window appears.

Figure 2-11 Trunk Configuration Window

The screenshot shows the 'Trunk Configuration' window. At the top, there is a 'Next' button with a green arrow. Below that is a 'Status' section with an information icon and the text 'Status: Ready'. The main section is 'Trunk Information', which is circled in red. It contains two dropdown menus: 'Trunk Type*' set to 'SIP Trunk' and 'Device Protocol*' set to 'SIP'. Red arrows point to the downward-pointing arrows of both dropdown menus. At the bottom, there is another 'Next' button.

- a. In the **Trunk Information** area, click the **Trunk Type** arrow and choose **SIP Trunk**.
- b. Click the **Device Protocol** drop-down list and choose **SIP**.
3. Click **Next**. The Trunk Configuration window displays the **Device Information** area.

Figure 2-12 Device Information Area

The screenshot shows the 'Device Information' section of the 'Trunk Configuration' window. It includes a 'Save' button at the top left. Below is the 'Status' section with 'Status: Ready'. The 'Device Information' section is circled in red and contains the following fields: 'Product' (SIP Trunk), 'Device Protocol' (SIP), 'Device Name*' (SIPForActiveREC, circled in red with an arrow), 'Description' (any description), 'Device Pool*' (Cluster G711-DP, circled in red with an arrow), 'Common Device Configuration' (< None >), 'Call Classification*' (Use System Default), 'Media Resource Group List' (< None >), 'Location*' (Hub_None), 'AAR Group' (< None >), 'Packet Capture Mode*' (None), and 'Packet Capture Duration' (0). There are also several checkboxes: 'Media Termination Point Required' (unchecked), 'Retry Video Call as Audio' (checked), 'Transmit UTF-8 for Calling Party Name' (unchecked), and 'Unattended Port' (unchecked).

- a. In the **Device Information** area, in the **Device Name** field type a meaningful name.



NOTE: If using VRSP (FSP) redundancy, be sure to use two different names that convey the functions of the different servers where the primary VRSP (FSP) and the redundant VRSP (FSP) reside.

- b. In the **Description** field, type a description of the device.
- c. Click the **Device Pool** drop-down list and choose the relevant device pool according to your network requirements.

Figure 2-13 SIP Information Area

The screenshot shows the 'SIP Information' configuration page. The fields and their values are as follows:

Field	Value	Annotation
Destination Address*	192.168.241.100	VRSP IP Address
Destination Port*	5062	Use this number to configure the SIP Port
MTP Preferred Originating Codec*	711ulaw	
Presence Group*	Standard Presence group	
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile	
Rerouting Calling Search Space	< None >	
Out-Of-Dialog Refer Calling Search Space	< None >	
SUBSCRIBE Calling Search Space	< None >	
SIP Profile*	Standard SIP Profile	
DTMF Signaling Method*	No Preference	

A 'Save' button is located at the bottom left of the form.

- d. In the **SIP Information** area, in the **Destination Address** field, type the IP address of the VRSP (FSP).



NOTE: If you are using VRSP (FSP) redundancy, each SIP Trunk must be configured with its corresponding VRSP (FSP) IP Address. See [VRSP \(FSP\) Redundancy](#) on [page 134](#).

- e. In the **Destination Port** field, type **5062**.
- f. Click the **SIP Trunk Security Profile** drop-down list and choose a standard non-secure profile. (The name of the profile will vary from site to site, in the example here the profile name is **Non-Secure SIP Trunk Profile**.)



NOTE: You can create several security profiles according to your site administration requirements and network topology.

- g. Click the **SIP Profile** drop-down list and choose **Standard SIP Profile**.
4. Click **Save**.

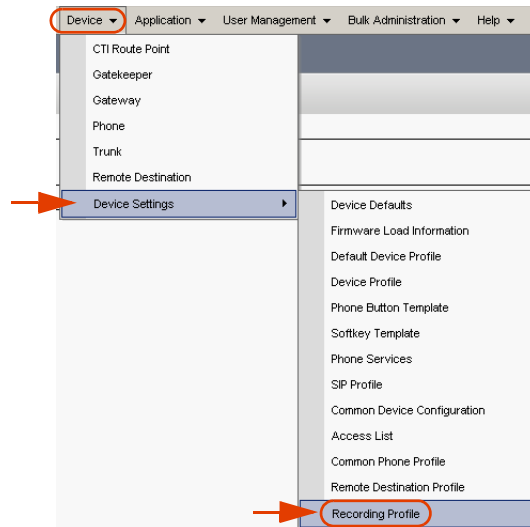
Defining the Recording Profile

Each device that needs to be recorded is associated with a recording profile that defines the number that it uses to dial the VRSP (FSP).

To define the Recording Profile:

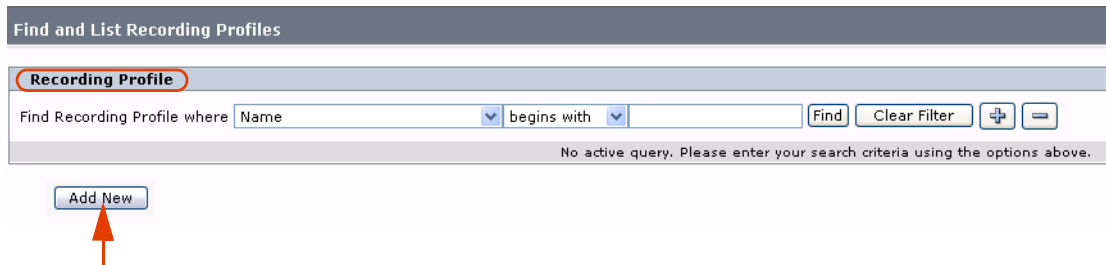
1. From the **Device** menu, point to **Device Settings** and choose **Recording Profile**.

Figure 2-14 Device Menu



The Find and List Recording Profiles window appears.

Figure 2-15 Find and List Recording Profiles Area



2. Click **Add New**. The Recording Profile Configuration window appears.

Figure 2-16 Recording Profile Configuration Window

Recording Profile Configuration

Save Delete Copy Add New

Status

Status: Ready

Put your section name here

Name* RecProfile-1

Recording Calling Search Space < None >

Recording Destination Address* 111122222

Save Delete Copy Add New

3. In the **Put your section name here** area, in the **Name** field type a meaningful name.
4. In the **Recording Calling Search Space** drop-down list, choose the Recording CSS that will be used to dial the SIP trunk.
5. In the **Recording Destination Address** field, type any unique number. This is the number that represents the NICE SIP Proxy in the CUCM.
6. Click **Save**.
7. In the Internet Explorer message box, click **OK**.

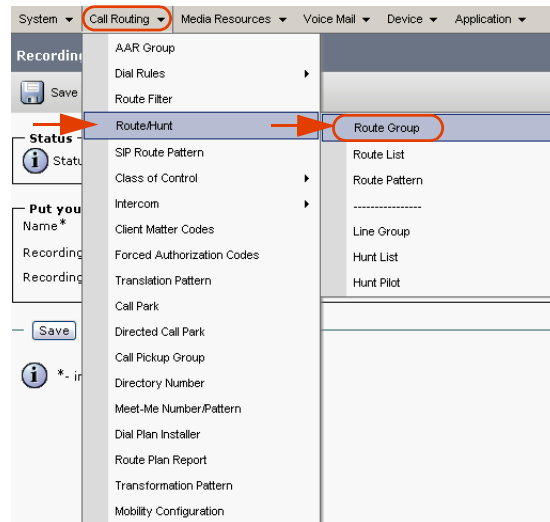
Defining a Route Group

You now need to define a new Route Group to group together all the SIP trunks (VRSPs/FSPs).

To define the new Route Group:

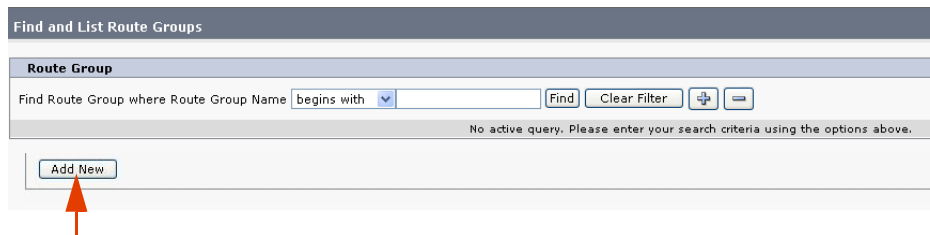
1. From the **Call Routing** menu, point to **Route/Hunt** and choose **Route Group**.

Figure 2-17 Call Routing Menu



The Find and List Route Groups window appears.

Figure 2-18 Find and List Route Groups Window



2. Click **Add New**. The Route Group Configuration page appears.

Figure 2-19 Route Group Configuration Window

Route Group Configuration

Save Delete Add New

Route Group Information

Route Group Name* Active Recording

Distribution Algorithm* Top Down

Route Group Member Information

Find Devices to Add to Route Group

Device Name contains Find

Available Devices**

- 192.168.241.244
- ActiveRecordingSIP-NagidE
- ActiveR-SIPT-Yuvals-SRV1
- ActiveR-SIPT-Yuvals-SRV2
- ActiveR-SIPTrain-130

Port(s) All

Add to Route Group

Current Route Group Members

Selected Devices***

- ActiveRecording-SIP1 (All Ports)
- ActiveRecording-SIP2 (All Ports)

Reverse Order of Selected Devices

Removed Devices****

3. In the **Route Group Information** area, in the **Route Group Name** field, type a meaningful name.
4. Click the **Distribution Algorithm** drop-down list and choose **Top Down**.
5. In the **Find Devices to Add to Route Group** area, in the **Available Devices** list, choose the SIP trunk that you created in **Defining a SIP Trunk** on [page 35](#).



NOTE: If using VRSP (FSP) redundancy, you need to select the two SIP Trunks that point to the primary VRSP (FSP) and redundant VRSP (FSP), see **Defining a SIP Trunk** on [page 35](#).

6. Click **Add to Route Group**. The selected IP trunk appears in the **Selected Devices** area.



NOTE: In VRSP (FSP) redundancy, both IP trunks appear in the **Selected Devices** area.

7. **Optional - only relevant for redundancy:**

The primary SIP Trunk *has* to be appear before the redundant one.

In the **Current Route Group Members** area, in the **Selected Devices** list, you can change the order of the SIP trunks. Select the device and click **Reverse Order of Selected Devices**.

8. To add another device to the **Current Route Group Members** area, repeat steps 5 to 6.
9. Click **Save**.

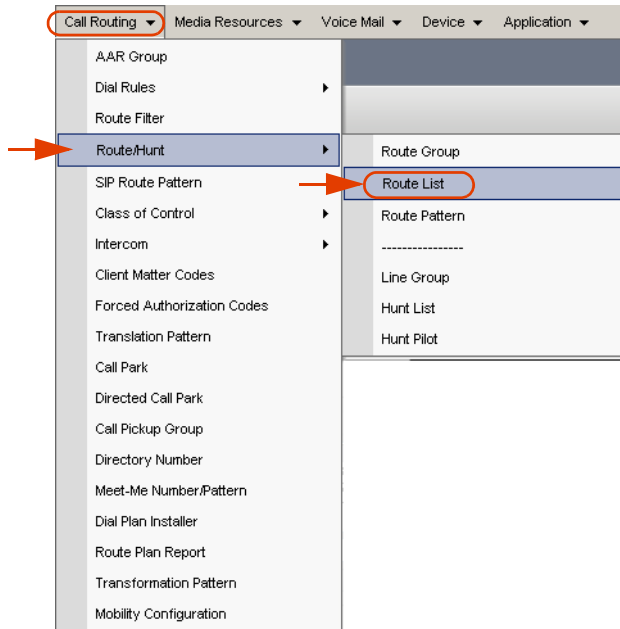
Defining a New Route List

You now need to define a new Route List that contains the Recorder Route Group. This points to the prioritized Route Group that you have just created.

To define a new Route List:

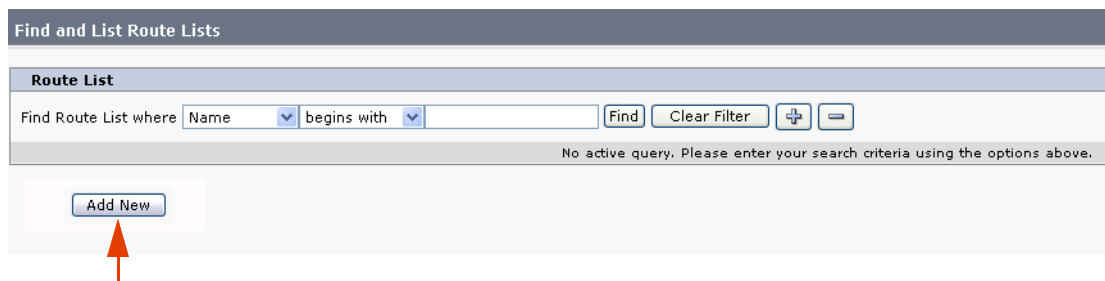
1. From the **Call Routing** menu, point to **Route/Hunt** and choose **Route List**.

Figure 2-20 Call Routing Menu



The Find and List Route Lists window appears.

Figure 2-21 Find and List Route Lists Window



2. Click **Add New**. The Route List Configuration page appears.

Figure 2-22 Route List Configuration Window

Route List Configuration

Save Delete Copy Reset Add New

Status
Add successful

Route List Information

Name* activetestlist
Description any description
Cisco Unified Communications Manager Group* Cluster-CMGroup
 Enable this Route List (change effective on Save; no reset required)

Route List Member Information

Selected Groups** activerectest
Removed Groups***
Add Route Group

Route List Details
activerectest

Save Delete Copy Reset Add New

3. In the **Route List Information** area, in the **Route List Name** field, type a meaningful name.
4. Click the **Cisco Unified Communications Manager Group** drop-down list and choose **Cluster**.



NOTE: A Cluster configuration is the recommended option. However, you should choose the option suitable for your network configuration.

5. Click **Save**. The new Route List group appears in the **Route List Member Information** area.
6. In the **Route List Member Information** area, click **Add Route Group**.
7. Choose the newly created Route Group.
8. Click **Save**.

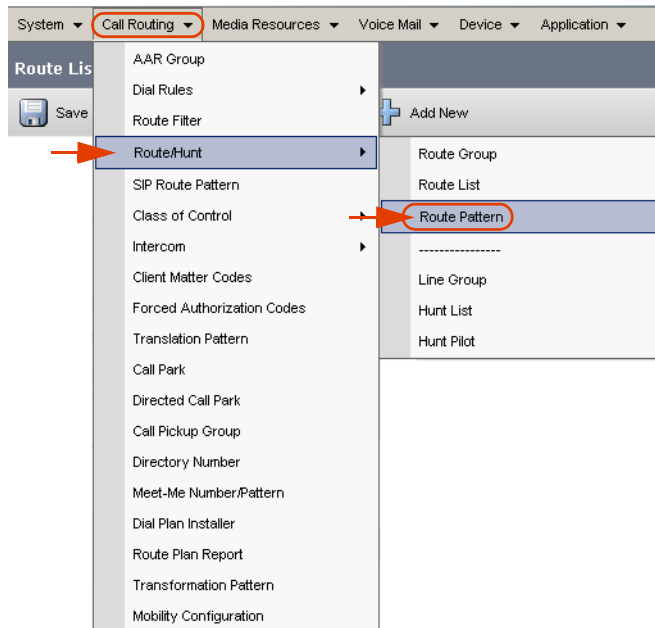
Defining a New Route Pattern

You now need to define a new Route Pattern based on the Device Number for the Recorder that you created previously, see [Defining the Recording Profile](#) on [page 38](#). The new Route Pattern should point to the Recorder Route List.

To define a new Route Pattern:

1. From the **Call Routing** menu, point to **Route/Hunt** and choose **Route Pattern**.

Figure 2-23 Call Routing Menu



The Find and List Route Patterns window appears.

Figure 2-24 Find and List Route Patterns Window



2. Click **Add New**. The Route Pattern Configuration page appears.

Figure 2-25 Route Pattern Configuration Window - Pattern Definition Area

Save

Status
Status: Ready

Pattern Definition

Route Pattern* 111122222

Route Partition < None >

Description

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence* Default

Gateway/Route List* activetestlist (Edit)

Route Option
 Route this pattern
 Block this pattern No Error

Call Classification* OffNet

Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority

Require Forced Authorization Code

Authorization Level* 0

Require Client Matter Code

3. In the **Pattern Definition** area, in the **Route Pattern** field, type the Recording Destination Address that you defined in **Step 5** on **page 39**.
4. Click the **Gateway/Route List** drop-down arrow and select the Route List that you defined in **Defining a New Route List** on **page 42**.
5. Click **Save**.

Configuring the Built In Bridge (BIB) on the IP Phone

The Cisco IP Phone-based Active Recording solution uses the Cisco IP phones to fork the RTP media. This forking is based on the Built In Bridge (BIB) within the IP phone. To see the IP phones supported, see **Cisco IP Phone** on [page 19](#).

The default setting for the Built In Bridge is **Off**; in this setting the forking does not take place. You can configure the BIB to an **On** configuration on a system-wide level or on a device level:

- **Configuring the Built In Bridge on a System-Wide Level**
- **Configuring the Built In Bridge on a Device Level**

Configuring the Built In Bridge on a System-Wide Level

You can configure the Built In Bridge on a system-wide level.



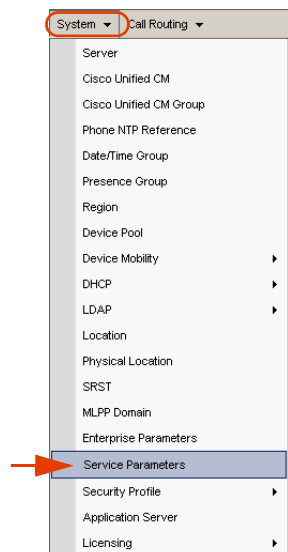
NOTE: If you configure the Built In Bridge on a system-wide level, ALL telephones registered in the server will be configured ON.

Follow the procedures below.

To configure the BIB on a system-wide level:

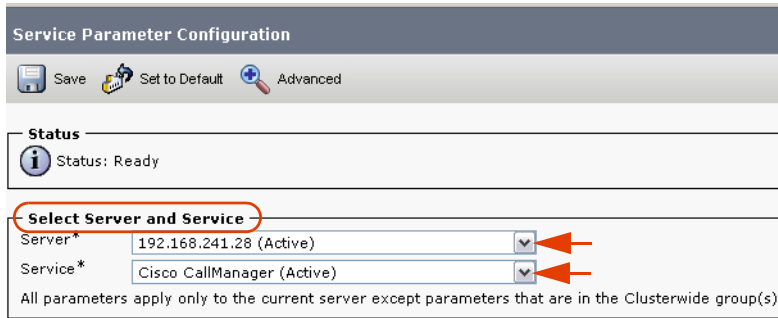
1. From the **System** menu, choose **Service Parameters**.

Figure 2-26 System Menu



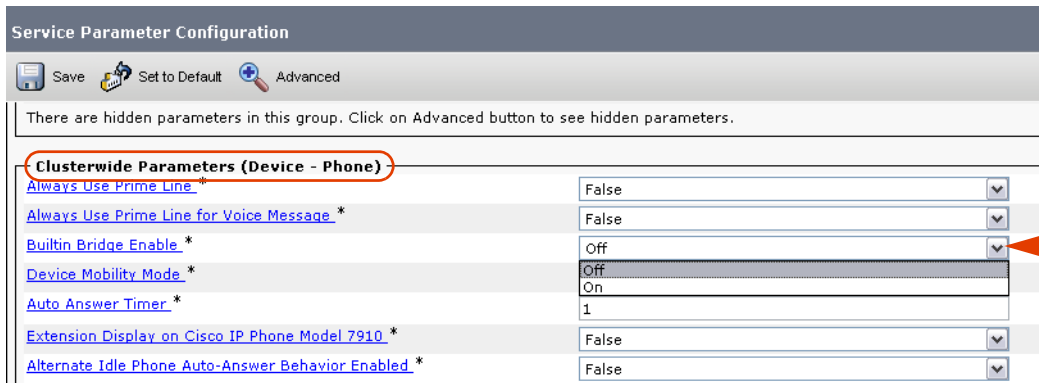
The Service Parameters Configuration window appears.

Figure 2-27 Service Parameters Configuration Window - Select Server and Service Area



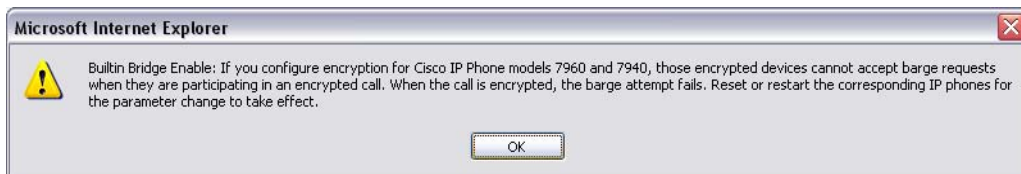
2. In the **Select Server and Service** area, click the **Server** drop-down arrow and choose the relevant server. The System Parameters Configuration window of the selected server appears.
3. Click the **Service** drop-down arrow and choose **Cisco CallManager (Active)**. The selected server and service appears.

Figure 2-28 Service Parameters Configuration Window - Clusterwide Parameters (Device - Phone)



4. Scroll down to the **Clusterwide Parameters (Device - Phone)** area.
5. Click the **Builtin Bridge Enable** drop-down list and select **On**. A warning message appears.

Figure 2-29 Microsoft Internet Explorer Warning Message



6. In the Microsoft Internet Explorer warning message, click **OK**.
7. Click **Save**.
8. If you have multiple servers, repeat this procedure from step 2 to 7 for each server.

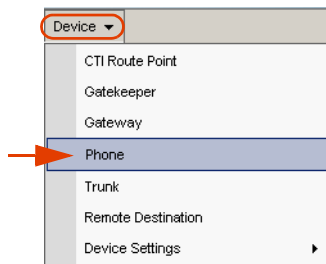
Configuring the Built In Bridge on a Device Level

You can also configure the Built In Bridge on a device level. Follow the procedures below.

To configure the Built In Bridge on the IP phone on a device level:

1. From the **Device** menu, choose **Route Group**.

Figure 2-30 Device Menu



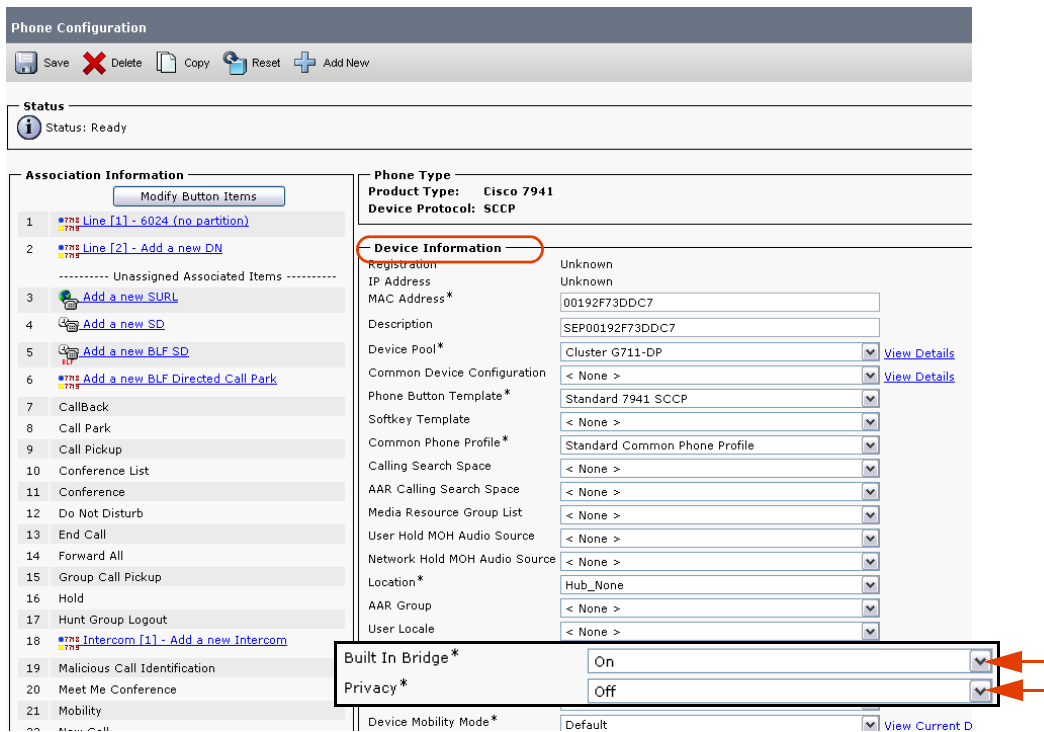
The Find and List Phones window appears.

Figure 2-31 Find and List Phones Window

Find and List Phones							
Status <i>i</i> 61 records found							
Phone (1 - 50 of 61)							
Find Phone where: Directory Number begins with <input type="text"/> <input type="button" value="Find"/> <input type="button" value="Clear Filter"/> <input type="button" value="↕"/> <input type="button" value="⇌"/>							
<input type="text" value="Select item or enter search text"/>							
<input type="checkbox"/>	Device Name(Line) ^	Description	Device Pool	Extension	Partition	Device Protocol	Status
<input type="checkbox"/>	SEP0017E0355A68	SEP0017E0355A68	Cluster G711-DP	6001		SCCP	Registered with 192.1
<input type="checkbox"/>	SEP000C85E40C00	Ofir 6002	Cluster G711-DP	6002		SCCP	Unregistered
<input type="checkbox"/>	SEP0017E0AE570A	Ofir 6003	Cluster G711-DP	6003		SCCP	Unknown
<input type="checkbox"/>	SEP00132083D967	uzi-6005	Cluster G711-DP	6005		SIP	Unknown
<input type="checkbox"/>	SEP00132083D968	uzi-6006	Cluster G711-DP	6006		SIP	Unknown
<input type="checkbox"/>	SEP123412341234	Liron-HMP	Cluster G711-DP	6007		SIP	Unknown
<input type="checkbox"/>	SEP001BD46C4460	SEP001BD46C4460	Cluster G711-DP	6009		SCCP	Unknown
<input type="checkbox"/>	SEP003094C42568	Ayalla	Cluster G711-DP	6011		SCCP	Unregistered

2. Search for the phones that you want to record.
3. Click **Find**. The Find and List Phones window appears.
4. Click the relevant phone link.

Figure 2-32 Phone Configuration Window



The Phone Configuration window appears.

5. In the **Device Information** area, click the **Built In Bridge** drop-down arrow and choose **On**.
6. Click the **Privacy** drop-down arrow and choose **Off**.
7. Click **Save**.

Associating the Recording Profile with the Recorded Device Number & Selecting Recording Method

You now need to associate the Recording Profile with the recorded Device Number.

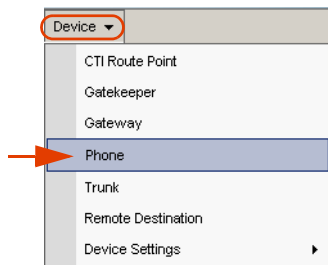
You also set the recording method here. Cisco IP Phones have multiple line appearances. Each line appearance in a phone device can be configured *separately* in the CUCM administration with its own relevant recording method. This means that you can have one line appearance configured for Total recording and another line appearance on the same phone device configured for Interaction-based recording. Cisco has their own terms for these recording methods:

- For Total recording, select **Automatic Recording**
- For Interaction-based recording, select **Application Invocation**.
- For no recording, select **Disabled**.

To associate the Recording Profile with the recorded Device Number:

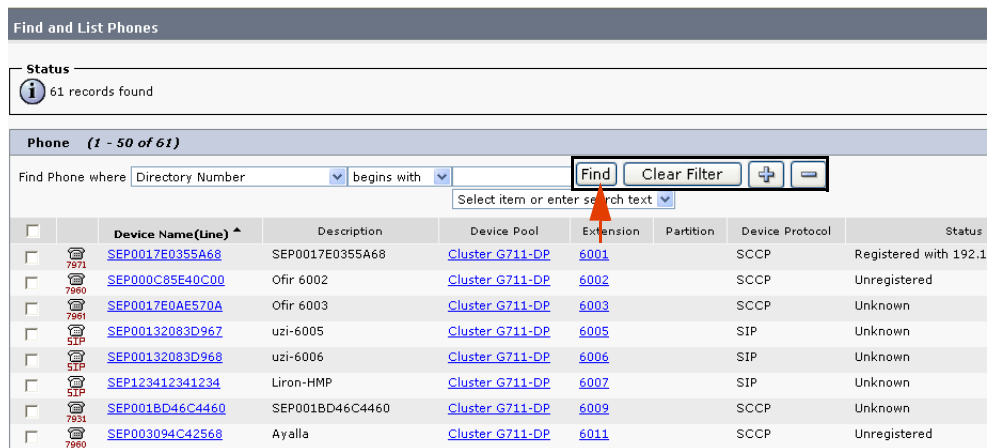
1. From the **Device** menu, choose **Phone**.

Figure 2-33 Device Menu



The Find and List Phones window appears.

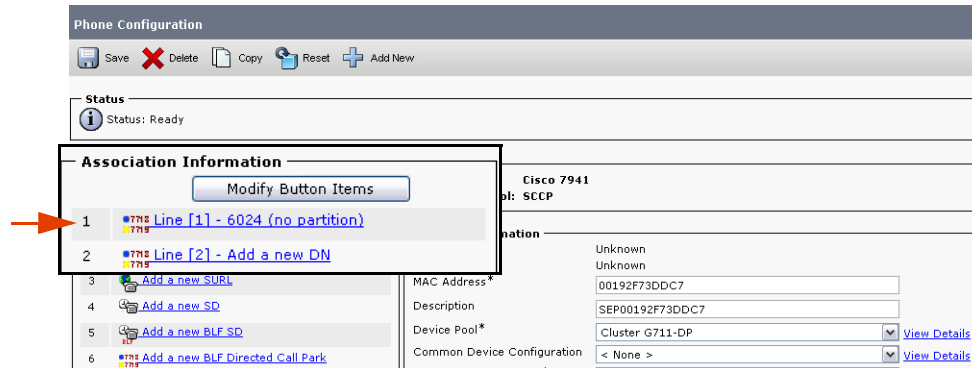
Figure 2-34 Find and List Phones Window



2. Search for the phones that you want to record.
3. Click **Find**. The Find and List Phones window appears.

- Click the relevant phone link.

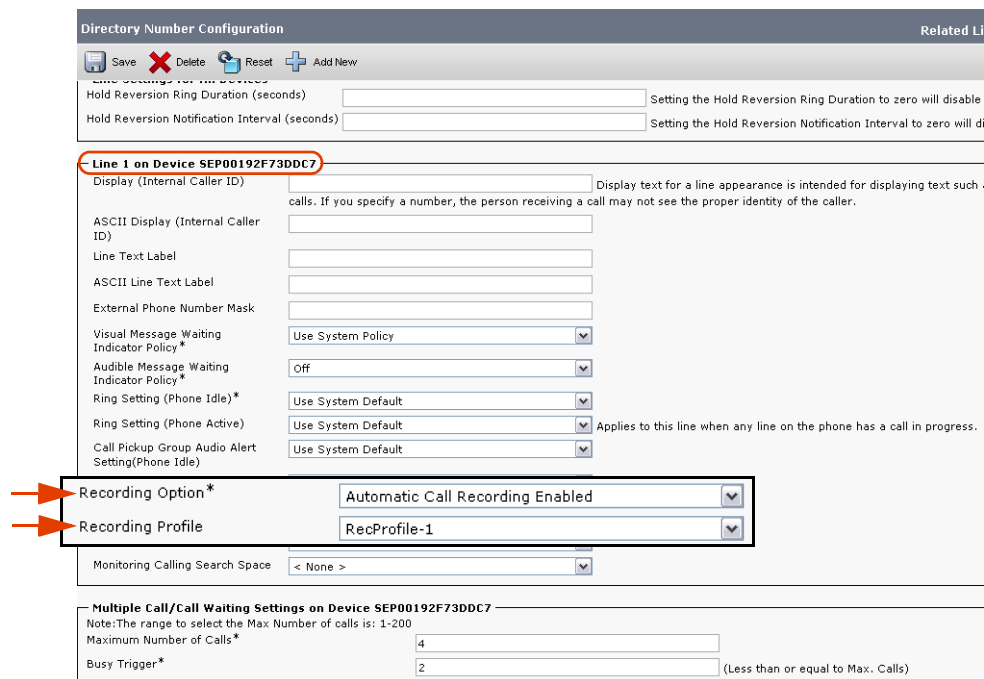
Figure 2-35 Phone Configuration Window



The Phone Configuration window appears.

- In the **Association Information** area, choose the line that you would like to record.
- Click the line link.

Figure 2-36 Directory Number Configuration Window



The Directory Number Configuration window appears.

- Click the **Recording Option** drop-down list and choose the relevant enabled option.

The **Recording Options** are:

- Call Recording Disabled:** choose this if no recording is permitted.
- Automatic Call Recording Enabled:** choose this for Total recording.

- **Application Invoked Call Recording Enabled:** choose this for Interaction-based recording.



NOTE: You can verify that these have been correctly configured in the TAPIMonitor application, see [Verifying the TSP Client Configuration](#) on [page 67](#).

8. Click the **Recording Profile** drop-down list and choose the Recording Profile that you defined earlier, see [Defining the Recording Profile](#) on [page 38](#).
9. Click **Save**.

Configuring the Phone Device Notification Tones

Cisco's IP Phone-based Active Recording provides you with an optional feature, enabling you to configure the notification tones on the phone itself. Notification tones can be configured on either a system-wide level or a device level.

Defining Notification Tones

An IP phone can be monitored and recorded at the same time. A user can be notified that he/she is being monitored and/or recorded by notification tones (beep tones).



NOTE: Cisco Monitoring and NICE monitoring have two completely different meanings. The monitoring referred to here is Cisco monitoring.

In Cisco's IP Phone-based Active Recording, the Monitoring tone and the Recording tone have different sounds and can be enabled or disabled independently. If both monitoring and recording are being used and the phone is configured to give notifications, the Recording tone always takes precedence over the Monitoring tone.

You can define notifications tones on both a system wide level or a device level, see:

- [Defining Notification Tones on a System Wide Level](#)
- [Defining Notification Tones on a Device Level](#)

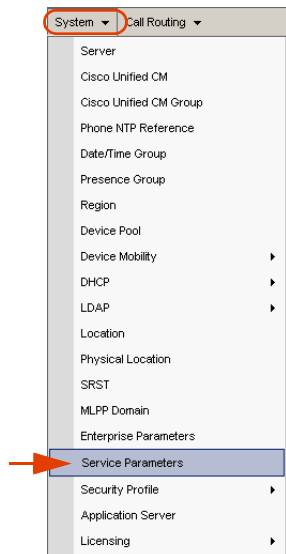
Defining Notification Tones on a System Wide Level

If the customer wants to enable notification tones on a system wide level, the following procedure should be performed.

To define notification tones on a system-wide level:

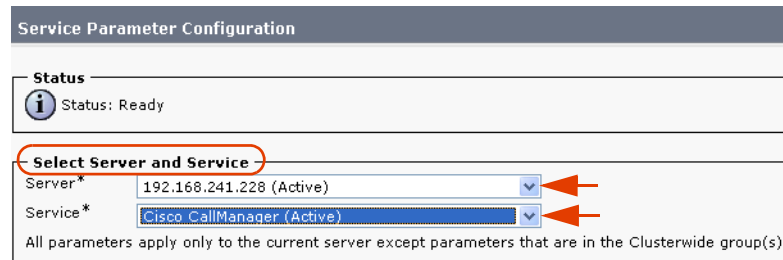
1. From the **System** menu, choose **Service Parameters**.

Figure 2-37 System Menu



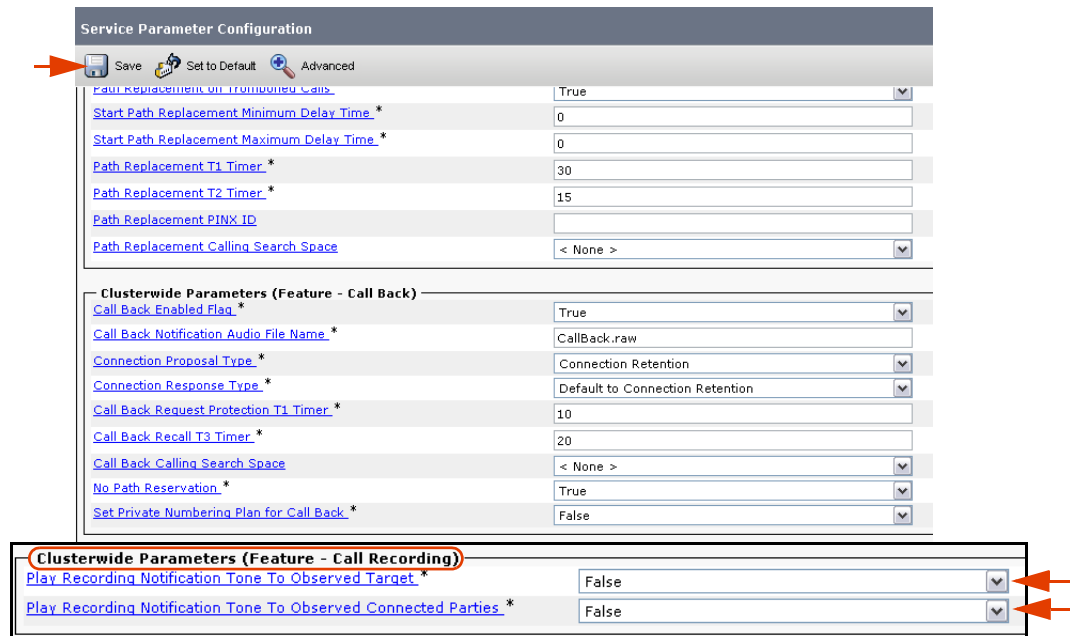
The Service Parameters Configuration window appears.

Figure 2-38 Service Parameters Configuration Window



2. In the **Select Server and Service** area, choose the service.
3. Click the **Service** drop-down arrow and choose **Cisco CallManager (Active)**. The selected server and service appears.

Figure 2-39 Service Parameters Configuration Window



4. Scroll down to the **Clusterwide Parameters (Feature - Call Recording)** area.
5. To play the notification tone to the observed target i.e. the agent, click the **Play Recording Notification Tone to Observed Target** arrow and click **True**.
6. To play the notification tone to the observed connected target i.e. the customer, click the **Play Recording Notification Tone to Observed Connected Parties** arrow and click **True**.
7. Click **Save**.

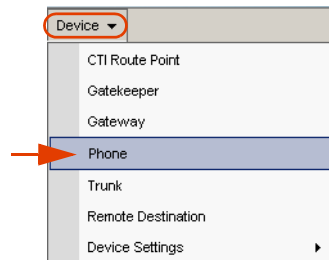
Defining Notification Tones on a Device Level

If the customer wants to enable notification tones on a device level, the following procedure should be performed. This procedure also enables you to define recording tones, recording volume, the remote volume and the recording tone duration.

To define notification tones on a device level:

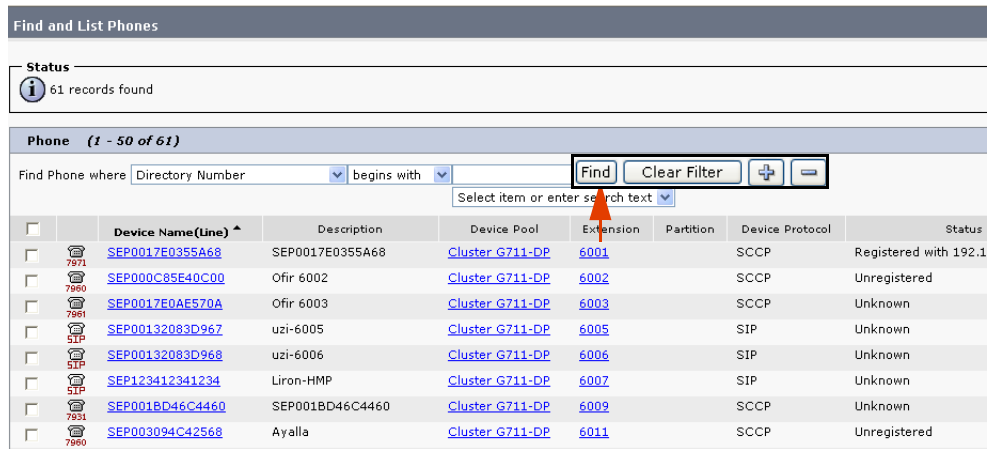
1. From the **Device** menu, choose **Phone**.

Figure 2-40 Device Menu



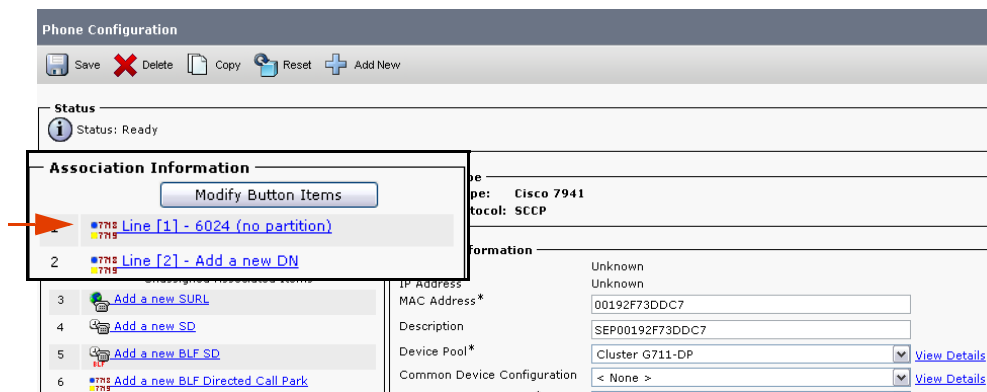
The Find and List Phones window appears.

Figure 2-41 Find and List Phones Window



2. Search for the phones that you want to record.
3. Click **Find**. The Find and List Phones page reappears.
4. Click the relevant phone link.

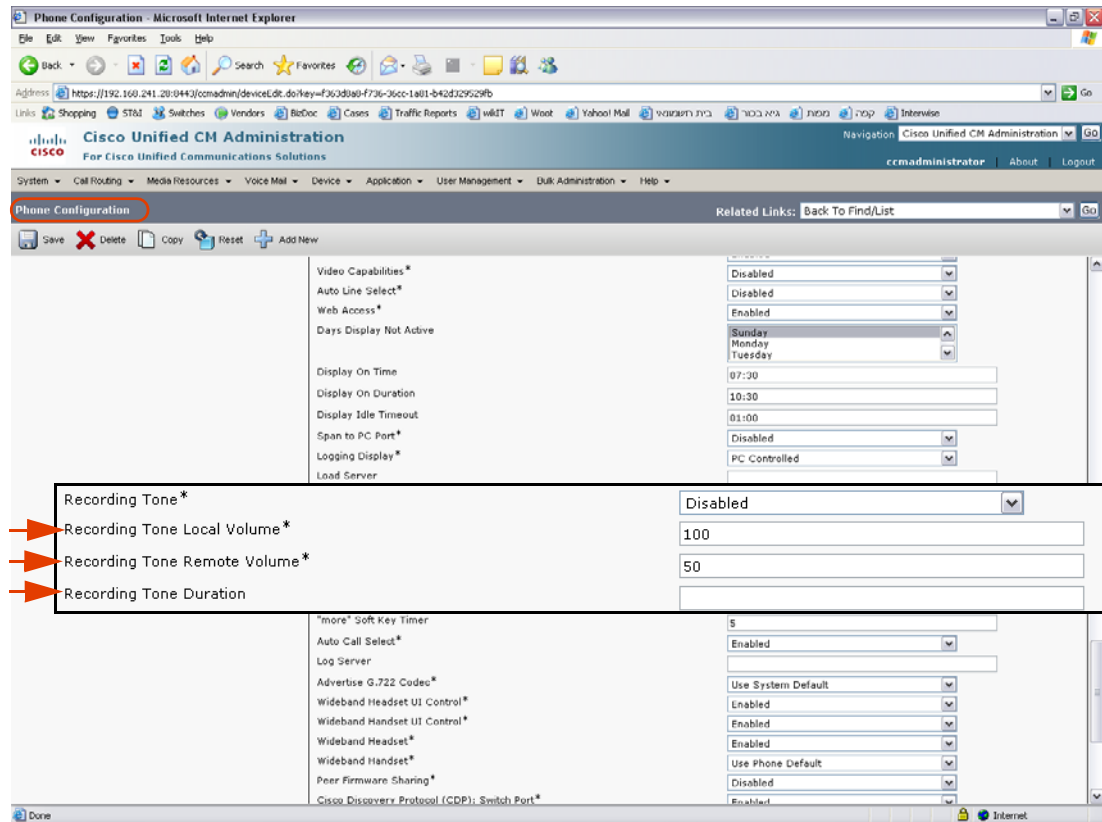
Figure 2-42 Phone Configuration Window



The Phone Configuration window appears.

5. Scroll down the window until you reach **Recording Tone**.

Figure 2-43 Phone Configuration Window - Recording Tone



6. Click the **Recording Tone** drop-down list and choose the desired recording tone.
7. In the **Recording Tone Local Volume** field, type the required local volume.
8. In the **Recording Tone Remote Volume** field, type the required remote volume.
9. In the **Recording Tone Duration** Field, type the required recording tone duration.
10. Click **Save**.

Installing the TSP Client on the NICE Interactions Center

This chapter provides guidelines for the installation and configuration of the Cisco TSP Client on the NICE Interactions Center.

Contents

Installing and Configuring the Telephone Services Provider (TSP) Client	58
Downloading the TSP Client	58
How Many TSP Clients Do I Need?	59
Installing the TSP Client	60
Configuring the TSP Client.....	64
Verifying the TSP Client Configuration.....	67

Installing and Configuring the Telephone Services Provider (TSP) Client

Installation and configuration of the Cisco TSP is comprised of the following procedures:

- **Downloading the TSP Client**
- **Installing the TSP Client:** During the installation procedure, you are prompted to define how many TSPs to install. Install the same number of TSPs as the number of unique TAPI users (nicecti users) previously defined, see **Defining an End User (nicecti User)** on **page 30**.
- **Configuring the TSP Client:** For each TSP instance, define one TAPI User (nicecti user) and the IP address of the CUCM. This configuration is done via the Phone and Modem Options.
- After you install and configure the Cisco TSP, verify that the Cisco TSP is working properly by running the TAPIMonitor.exe.

Downloading the TSP Client

This procedure describes how to download the TSP Client.



IMPORTANT

The Cisco TSP Client version must match the CUCM version. Download and install the Cisco TSP software directly from the CUCM Administration to ensure that you use the latest version and that the versions match.

To download the TSP Client on the NICE Interactions Center:



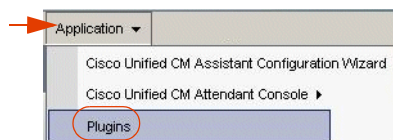
IMPORTANT

A Cisco System Administrator must download the TSP Client!

Download the Cisco TSP as follows:

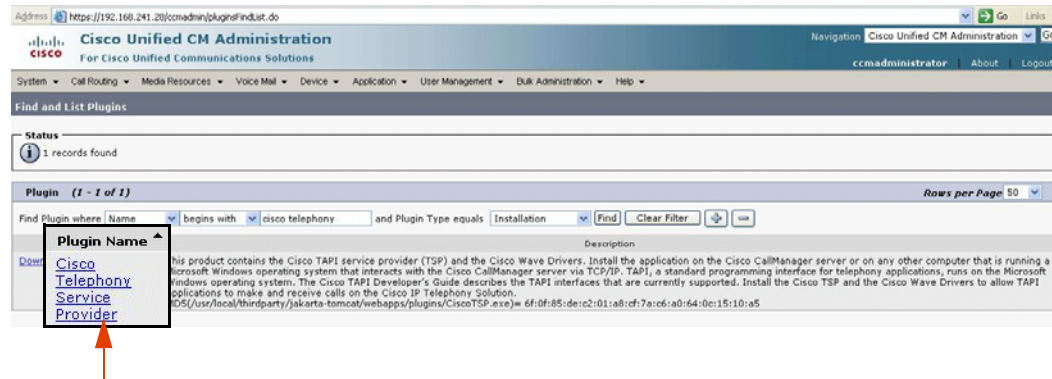
1. On the NICE Interactions Center, log in to the CUCM Administration application.
2. From the **Application** menu, choose **Plugins**. The CUCM Administration appears with a list of Plugins.

Figure 3-1 Choosing Plugins



3. In the **Search Options** area, search for **Cisco Telephony Service Provider**. Click **Find**.

Figure 3-2 Find and List Plugins Window



- From the **Search Results** list, click **Cisco Telephony Service Provider** and click **Download**.

The TSP Client is downloaded and the File Download - Security Warning window appears.

- Continue with **Installing the TSP Client** on [page 60](#).

How Many TSP Clients Do I Need?

The required number of TSP Client instances or installations varies according to the type of installation that you are performing. Follow the recommendations for the relevant site installation:

- Standard Installation (Total or Interaction-based recording)**
 In this installation where either Total or Interaction-based recording is used (but NOT both), one TSP Client instance is installed on the NICE Interactions Center.
- Combined Recording Method Installation (Total and Interaction-based recording)**
 In this installation where BOTH Total or Interaction-based recording are used, two TSP Client instances are installed on the NICE Interactions Center.



IMPORTANT

When working in a mixed environment of Total recording and Interaction-based recording, two TSP Clients instances need to be installed. Each TSP Client is configured with a different TAPI user (nicecti user) in the CUCM.

Each TAPI user (nicecti) is associated with the devices relevant for its type of recording, i.e. the TAPI user (nicecti1) defined for Total recording will have devices using the **Automatic Call Recording Enabled Recording Option**. The TAPI user (nicecti2) defined for Interaction-based recording will have devices using the **Application Invocation Recording Option**. You can view the recording profile for each device using the TAPIMonitor.exe, see [Verifying the TSP Client Configuration](#) on [page 67](#).

Installing the TSP Client

In Cisco IP Phone-based Active Recording solution, the required number of TSP Client instances or installations can vary. In VRSP (FSP) Redundancy installations, two TSP Clients are installed and configured (one on each VRSP machine).

This procedure describes how to install the TSP Client.

To install the TSP Client:

1. In the File Download - Security Warning window, click **Run**.

-or-

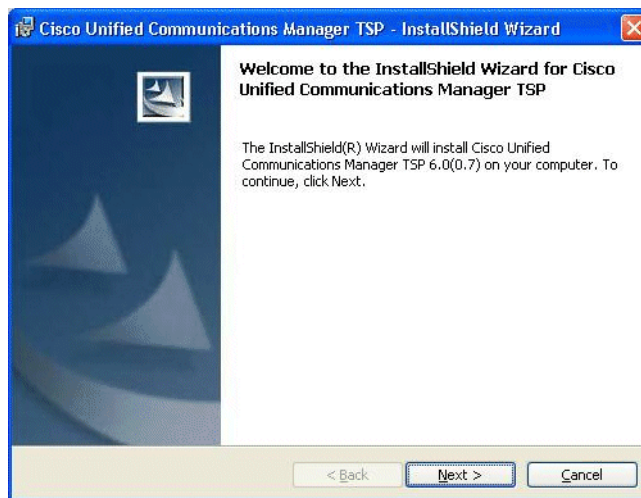
Locate the installation folder and run the **CiscoTSP.exe** file.

Figure 3-3 File Download - Security Warning Window



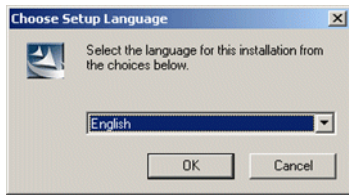
The Cisco Unified Communications Manager TSP Install Wizard starts.

Figure 3-4 Cisco Unified Communications Manager TSP InstallShield Wizard Window



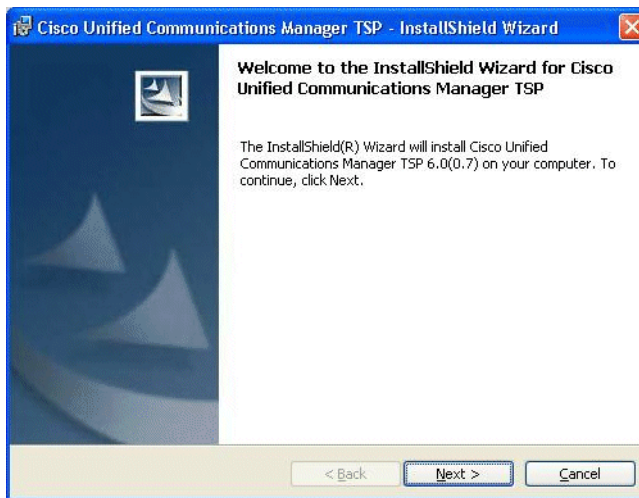
2. Click **Next**. The Choose Setup Language window appears.

Figure 3-5 Choose Setup Language Window



3. Select the appropriate installation language and click **OK**. The Cisco Unified Communications Manager TSP Setup Welcome window appears.

Figure 3-6 Cisco Unified Communications Manager TSP Setup Welcome Window



4. Click **Next**. The Choose Destination Location window appears.

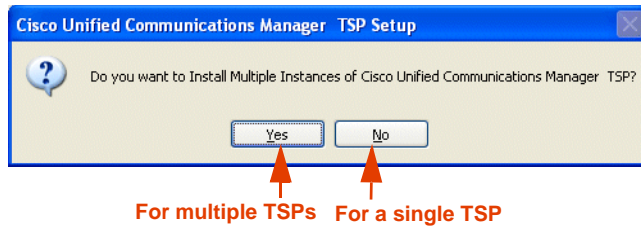
Figure 3-7 Choose Destination Location Window



- a. Install in the default location. To choose an alternate location, click **Browse** and navigate to the preferred location.

- b. Click **Next**. A message appears asking if you want to install multiple instance of Cisco Unified Communications Manager TSP.

Figure 3-8 Do you want to Install Multiple Instances Message Box



- c. In the Message window, click:
 - **No** for only one TSP
 - **Yes** for multiple TSP instances

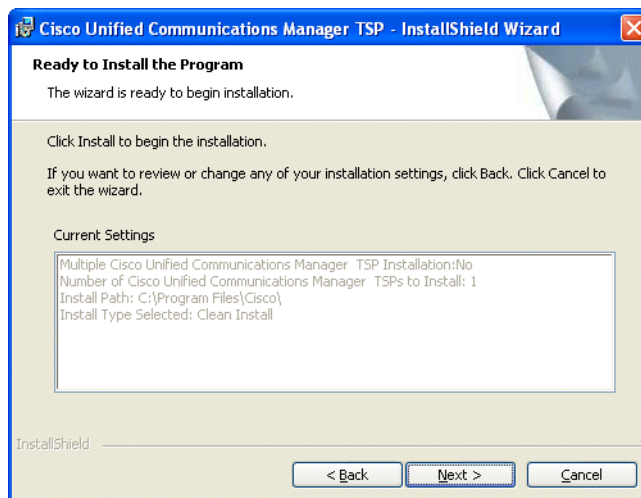


IMPORTANT

For Cisco’s IP Phone-based Active Recording solution, if you are installing for a mixed environment, click **Yes** as you need to install two TSP Clients.

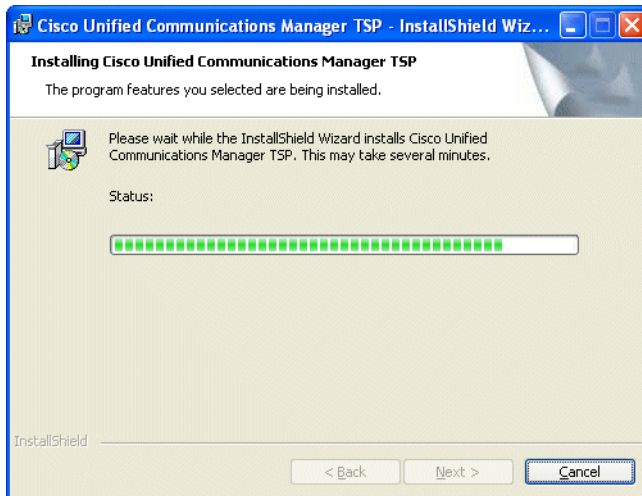
The Start Copying Files window appears.

Figure 3-9 Ready to Install the Program Window



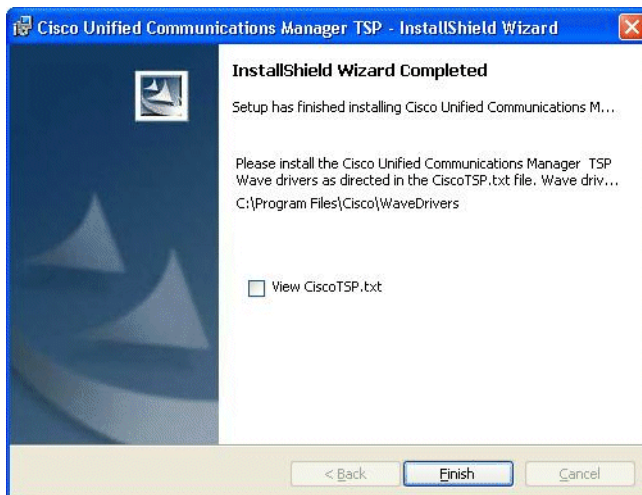
- d. Click **Next**. The Installing Cisco Unified Communications Manager TSP appears.

Figure 3-10 Installing Cisco Unified Communications Manager TSP Windows



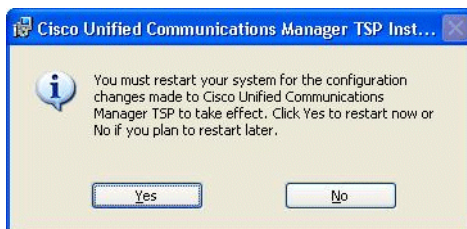
When the installation is complete, the InstallShield Wizard Completed window appears.

Figure 3-11 InstallShield Wizard Completed Wizard



- e. Click **Finish**. A message appears warning that you must restart your system for the configuration of Cisco Unified Communications Manager TSP to take effect.

Figure 3-12 Cisco Unified Communications Manager TSP Install Message



- f. Click **Yes**. The computer is restarted. The installation process is now complete. The TSP Client is now installed.

Configuring the TSP Client

To configure the TSP Client, follow the procedures below. If you need to configure a secure connection, there are a few additional procedures that you need to perform.



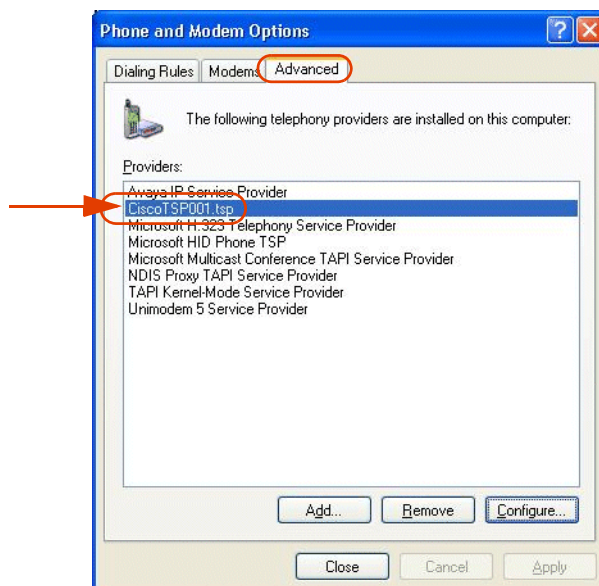
TIP:

It is recommended to configure the TSP Client to support normal recording and to make sure that there is a connection established with the Communications Manager. This will help rule out switch connection issues later on in the integration process.

To configure the TSP Client:

1. Click **Start > Settings > Control Panel > Phone and Modem Options**. The Phone and Modem Options window appears.
2. Click the **Advanced** tab.

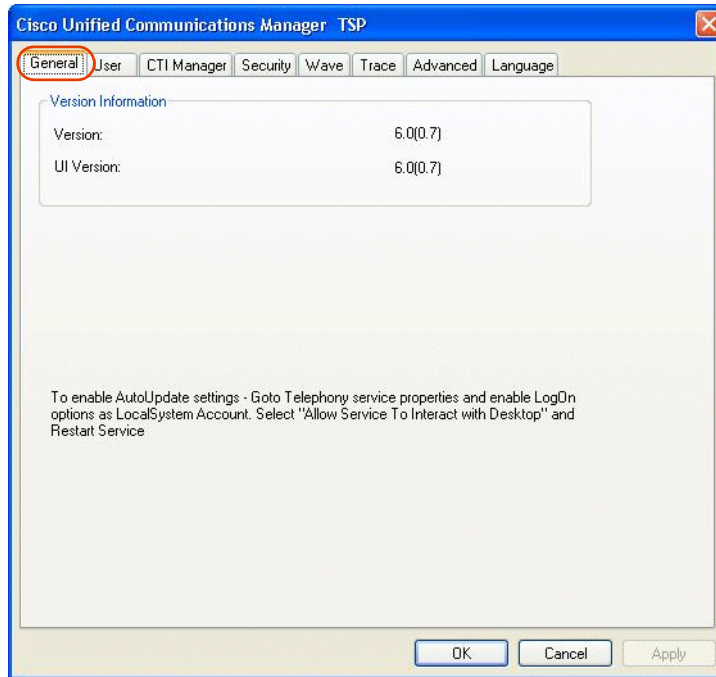
Figure 3-13 Phone and Modem Options - Advanced Tab



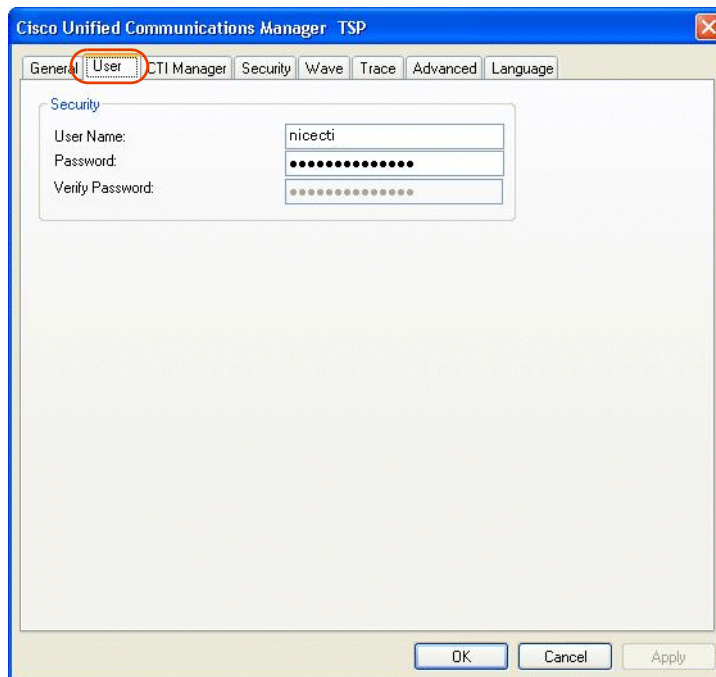
NOTE: If you are using Cisco's IP Phone-based Active Recording solution and you have a mixed environment, there will be two Cisco TSP Clients - **CiscoTSP001.tsp** and **CiscoTSP002.tsp**. Each of these clients has to be configured for its TAPI user, (one for each environment).

3. In the **Providers** list, select **CiscoTSP001.tsp** and click **Configure**.

The Cisco Unified Communications Manager TSP window appears.

Figure 3-14 Cisco Unified Communications Manager TSP - General Tab

4. Click the **User** tab.

Figure 3-15 User Tab

5. In the **Security** area, complete the following:



IMPORTANT

In the **Security** area, use the same user name and password that were used in defining the end user, see **Defining an End User** on page 24. Ask your Cisco switch technician for this information.

- a. In the **User Name** field, type the user name.
 - b. In the **Password** field, type the password.
 - c. In the **Verify Password** field, type the password again.
6. Click the **CTI Manager** tab.

Figure 3-16 CTI Manager Tab

7. In the **Primary CTI Manager Location** area, type the **IP address** of the Cisco Communications Manager.

In the **Backup CTI Manager Location** area, if there is a redundant Communications Manager, type its **IP address** or **Host Name**. Otherwise in the **Backup CTI Manager Location** area, type the same IP Address or Host Name as in the **Primary CTI Manager Location** area.
8. Click **Apply** and then click **OK**.
9. In Cisco's IP Phone-based Active Recording solution, if working with a mixed environment repeat **Step 1** on page 64 to **Step 7** on page 66 and type the second **End User** name (**nicecti2**) that you created.
10. Close the Cisco Unified Communications Manager TSP window.

The TSP Client is configured.

11. Reboot the computer.

**IMPORTANT**

It is critical that you reboot the computer! The configuration will not work if you do not do this!

The TSP Client's configuration is completed.

Verifying the TSP Client Configuration

After you have installed and configured the TSP Client, you need to verify that it is running and properly connected to the CUCM.



NOTE: Extension mobility lines only appear when the agent is logged on. When the agent logs in, a line create appears. When the agent logs out, a line remove appears.

This procedure describes how to verify the connection.



NOTE: You can also use the TAPIMonitor to view the recording modes of each device.

To verify the TSP Client configuration:

1. In the NICE Interactions Center, navigate to the **TAPIMonitor.exe** application (the default location is **D:\NICECT\Integrations\TAPICTILink**).
2. Copy the TAPI monitor application locally.
3. Run the TAPI monitor application. A window appears with the connection details. A successful connection should look similar to **Figure 3-17** on **page 68**.

Figure 3-17 TAPIMonitor.exe Connection Details Window - Successful Connection Example


```

Select D:\NICECTI\9_12\Integration\TAPICITLink\apiMonitor.exe
Nice's TAPI Monitor Application 1.4
API version: 20002

Providers List
-----
unimdn.tsp 5.01.2600.2180
kmdtsp.tsp 5.01.2600.2180
ndptsp.tsp 5.01.2600.2180
ipconf.tsp 5.01.2600.2180
h323.tsp 5.01.2600.2180
hidphone.tsp 5.01.2600.2180
CiscoISP001.tsp 6.00.00.05

Line | Line Address | Line Name
-----
6 | 1550 | Cisco Line: [CtiParkDevice] (1550) <DNs Park number> 1800
7 | 6001 | Cisco Line: [SEP0017E0AE570A1 (6001) <IP Phones> 35020
8 | 6003 | Cisco Line: [SEP0017E0AE570A1 (6003) <IP Phones> 35020
9 | 6004 | Cisco Line: [0019D1253EB4] (6004) <IP Phones> 35020
10 | 6010 | Cisco Line: [SEP0017E0AE570A1 (6010) <IP Phones> 35020
11 | 6020 | Cisco Line: [SEP003094C309C71 (6020) <IP Phones> 35020
12 | 6021 | Cisco Line: [SEP000C85E40AD31 (6021) <IP Phones> 35020
13 | 6021 | Cisco Line: [SEP003094C309C71 (6021) <IP Phones> 35020
14 | 6022 | Cisco Line: [SEP000B5FAAB3AE1 (6022) <IP Phones> 35020
15 | 6033 | Cisco Line: [SEP003094C309C71 (6033) <IP Phones> 35020
16 | 6115 | Cisco Line: [SEP0015F97E28D81 (6115) <IP Phones> 35020
17 | 6115 | Cisco Line: [SEP003094C309C71 (6115) <IP Phones> 35020
18 | 6201 | Cisco Line: [SEP0019569910701 (6201) <IP Phones> 35020

Recording modes of each device:
000000 | eNoRecording
eAutomaticInvocation
eApplicationInvocation
AutomaticInvocation
eApplicationInvocation
eNoRecording
eNoRecording
eNoRecording
eNoRecording
eNoRecording
eNoRecording
eNoRecording
eNoRecording
eNoRecording
eNoRecording
eNoRecording
eNoRecording
eNoRecording
eNoRecording
eNoRecording
eAutomaticInvocation
  
```

4. Verify the connection details that appear in the window and verify in the **Line Address** that all the extensions appear.
5. In the TAPIMonitor.exe window, type one of the lines of the phone devices (in **Figure 3-17**, Line 16 or 17). Press <Enter>.
6. Make a phone call from one device to another.
7. Verify that a padlock icon  appears on the phone's screen.
8. Verify that the TAPIMonitor.exe window displays all of the information for the call coming from the switch, including the keys for this session.
9. Verify that all the monitored devices appear and that their Recording modes also appear. (This was configured in **Step 7** on **page 51**.)



NOTE: You can also see the MAC address for each device which can be useful for future troubleshooting.

The connection is verified. The TSP Client is able to monitor the CUCM and receive the relevant information required to decrypt the call packets and to allow proper recordings.



NOTE: You can view all information regarding the TAPIMonitor results in the TAPIMonitor.txt file.

Installing and Configuring the MPCM (FLM)

This chapter describes the installation and configuration of the Media Provider Control Manager (MPCM (FLM)). The Media Provider Control Manager is an online repository of the forwarding devices installed at your site. The MPCM (FLM) is *installed* on the NICE Interactions Center. However, it is *not defined* in the System Administrator.

Contents

MPCM (FLM) System Requirements	70
Installing the MPCM (FLM).....	71

MPCM (FLM) System Requirements

The MPCM/FLM must be installed on the NICE Interactions Center. Ensure that the following components are installed on this machine:

- The latest version of Microsoft .Net 2.0
See [Microsoft .NET Framework Version 2.0 Redistributable Package \(x86\)](#).
- The remoting serialization hotfix.
See [Microsoft Knowledgebase Article ID 914460](#).

Installing the MPCM (FLM)



IMPORTANT

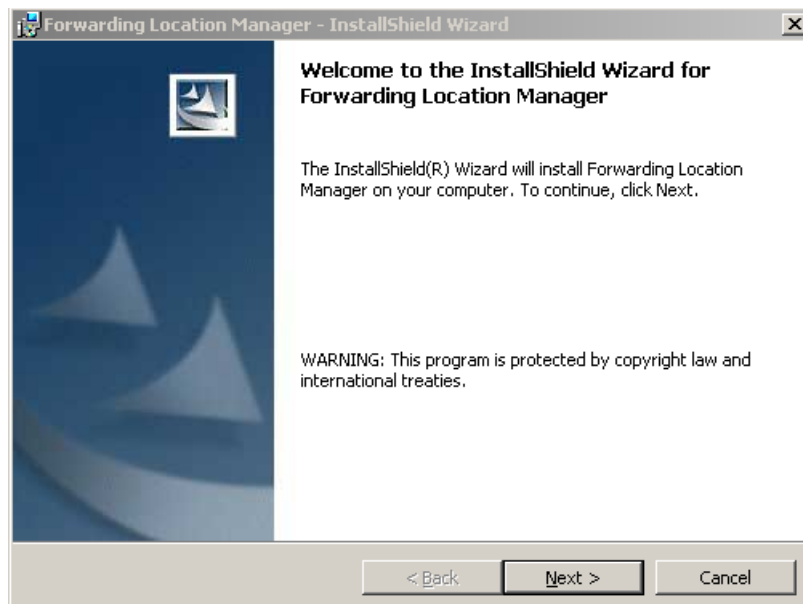
In a standard installation (where redundancy is not used), VRSP (FSP) and MPCM (FLM) are installed on the same machine. In this case, the SIP default port of one of them should be changed as both processes cannot use the same port. (The VRSP (FSP) connects to the CTI and the MPCM (FLM) connects to the logger.) It is recommended that you change the VRSP (FSP) port.

To install the MPCM (FLM):

1. Insert the NICE Interactions Center Installation disk into the drive and double-click *Forwarding Location Manager.msi*.

The Forwarding Location Manager (FLM/MPCM) InstallShield Wizard starts.

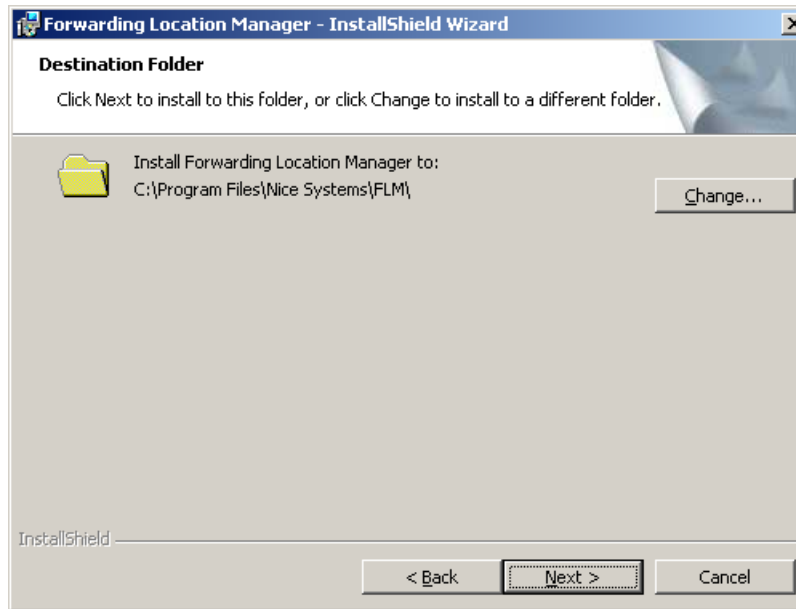
Figure 4-1 Forwarding Location Manager - InstallShield Wizard



2. Click **Next**.

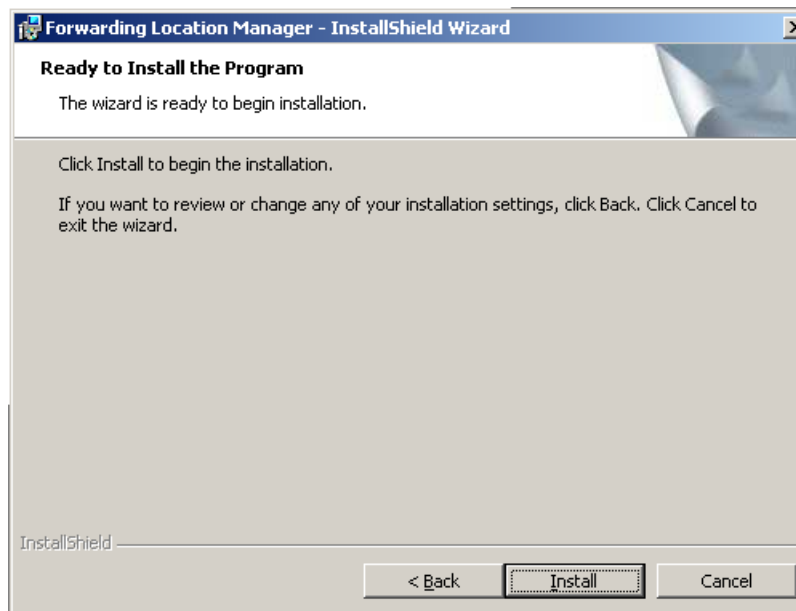
The Destination Folder window appears.

Figure 4-2 Destination Folder Window



3. Keep the default destination folder or click **Change** to choose a new location. Click **Next**. The Ready to Install the Program window appears.

Figure 4-3 Ready to Install the Program Window



4. Click **Install**. A progress bar appears.

Then the FLM (MPCM) Configuration Wizard starts.

Figure 4-4 FLM Configuration Wizard



TIP: If you know that this installation is similar to a previous installation, you may want to use a predefined configuration file.

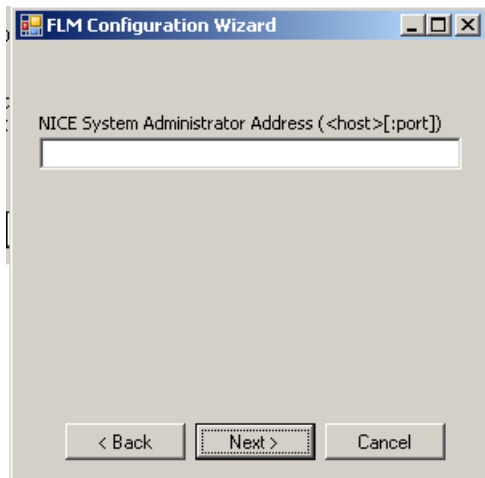
Below is the default path to the FLM (MPCM) configuration file:

C:\Program Files\Nice Systems\FLM\Config\FLMConf.xml

5. Select the file to use for your FLM (MPCM) configuration.
 - To use a predefined configuration file, click **Load** and select the file.
 - or-
 - To create a new configuration file, click **Next**.

The NICE System Administrator Address window appears.

Figure 4-5 NICE System Administrator Address Window



6. Type the IP address or host name of the machine on which System Administrator is installed.

**NOTE:**

- When the MPCM/FLM and System Administrator are installed on separate machines, both machines must be configured on either no domain, the same domain, or on different domains. In the event that each machine is configured on a different domain, during the MPCM installation, you must define the System Administrator's fully qualified host name (FQHN).

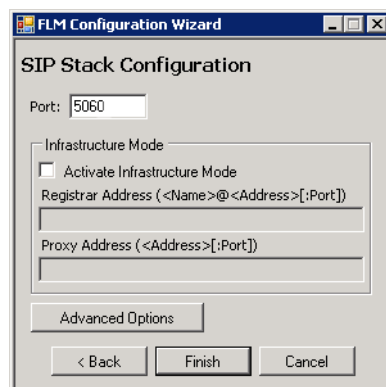
Examples of Fully Qualified Host Names:

- MyMPCM.nice.com - fully qualified host name (FQHN)
- MyMPCM.nice.com:5062 - fully qualified host name (FQHN) + port number
- **Do not install the MPCM and System Administrator on separate machines if one machine is configured on a domain and the other machine is not configured on a domain!**

7. Click **Next**.

The SIP Stack Configuration window appears. The SIP stack configuration determines the way in which the FLM/MPCM handles SIP interactions.

Figure 4-6 SIP Stack Configuration Window



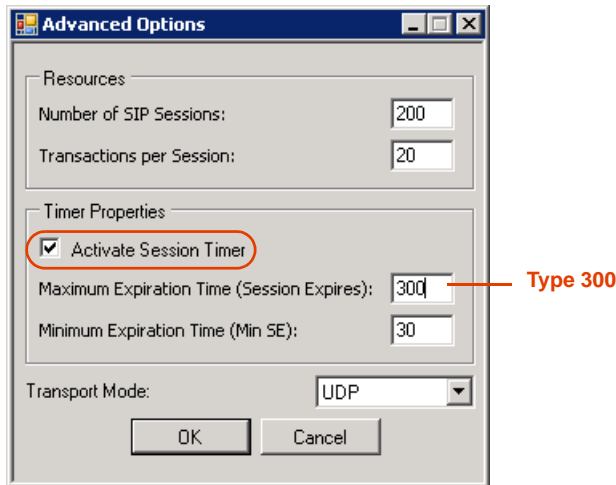
8. For Cisco's IP Phone-based Active Recording solution, leave the **Port** at its default setting - **5060**.

If SIP infrastructure is installed at your site, define the **Registrar** and **Proxy** IP addresses.

9. For Cisco's IP Phone-based Active Recording solution, click **Advanced Options**.

The Advanced Options window appears.

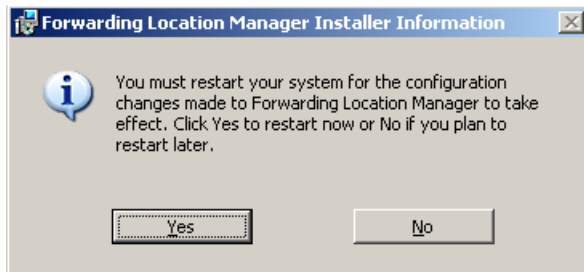
Figure 4-7 Advanced Options Window



- a. In the **Timer Properties** area, verify that the **Activate Session Timer** checkbox is marked.
 - b. In the **Maximum Expiration Time (Session Expires)** field, type **300**.
 - c. Click **OK**.
10. Click **Finish**.

An information message appears.

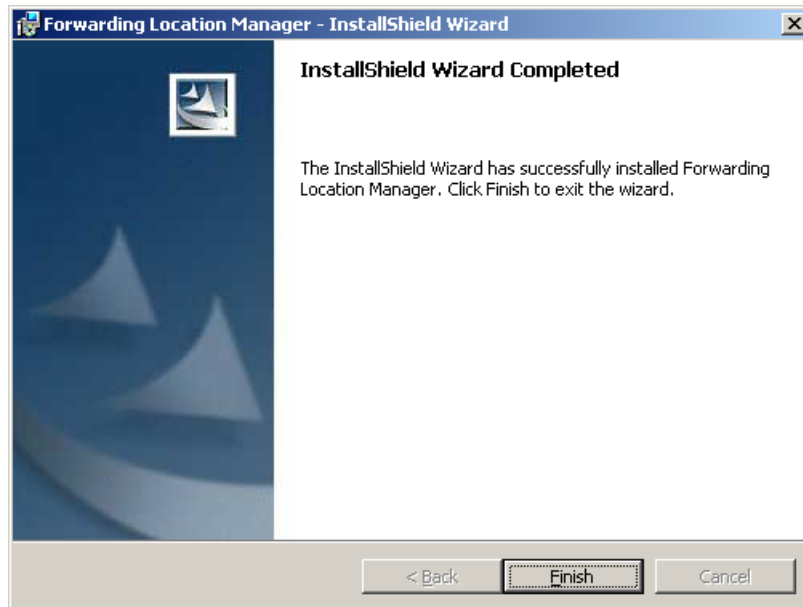
Figure 4-8 Forwarding Location Manager (FLM/MPCM) Installer Information



11. Click **Yes**.

The InstallShield Wizard Completed window appears.

Figure 4-9 InstallShield Wizard Completed Window



12. Click Finish.

The Forwarding Location Manager (FLM/MPCM) installation is complete.

Configuring the Logger

This chapter provides an overview of the installation and configuration of the Active VoIP logger. It also details configuration information regarding the IP Tool - Port and SIP configuration.



IMPORTANT

Verify that the VoIP Logger has been configured for SIP Audio by checking the **Summary.doc** configuration file and look for a SIP Audio type of logger. Another option is to look in the IP Tool window, if the **SIP Configuration** section appears greyed out then the Logger has not been configured for SIP Audio.

In either instance if it is not a SIP Audio type of VoIP logger, contact NICE Customer Support.

For detailed information regarding configuring the Logger, see the *VoIP Logger Installation Guide*.

Contents

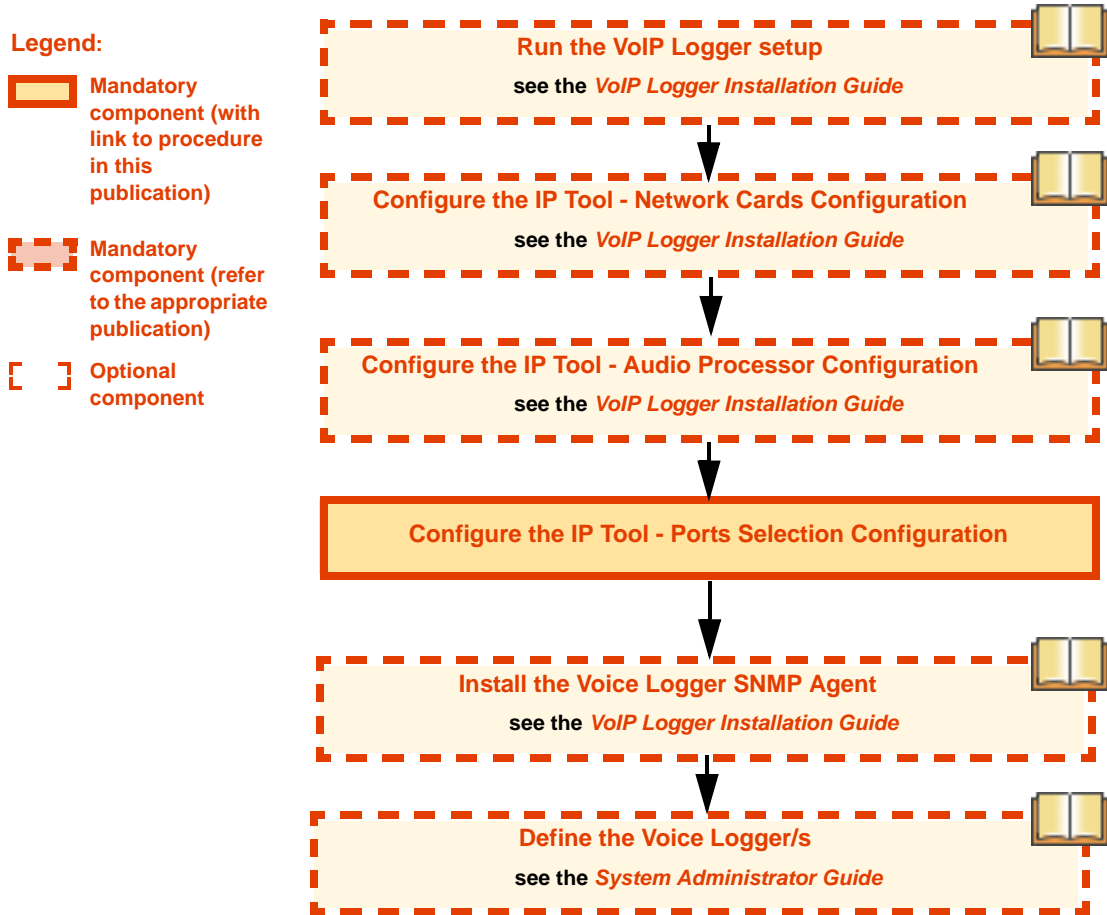
Configuring the Active VoIP Logger	78
Configuring the Ports	79
SIP Configuration	80

Configuring the Active VoIP Logger

Detailed information regarding the **Logger setup** and configuration of the **IP Tool (Network Cards Configuration, Audio Processor Configuration)** (Optional) can be found in the *VoIP Logger Installation Guide*. These procedures will not be repeated in this book.

However, as the IP Tool's **Port Selection Configuration** is an integral part of the Active VoIP Recording solution and has its own specific definitions, this material is included in this guide.

The Active VoIP Logger should be configured following the workflow below.



Configuring the Ports

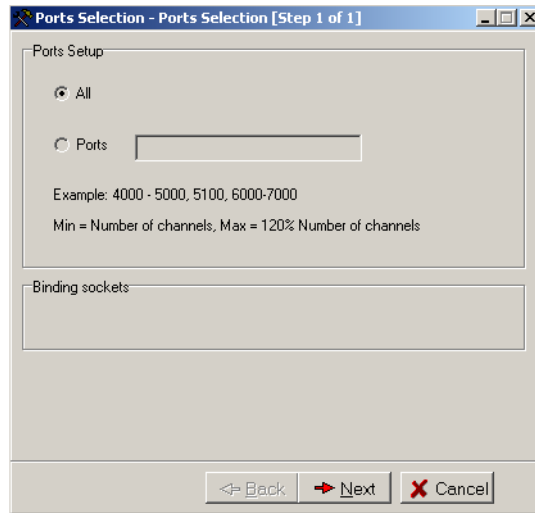
To configure the Logger to use specific ports:

1. In the IP Tool window, click **Ports Selection**.

Figure 5-1 IP Tool Window - Ports Selection

The Ports Selection window appears.

Figure 5-2 Ports Selection Window



2. Define the ports or port range you need to record.



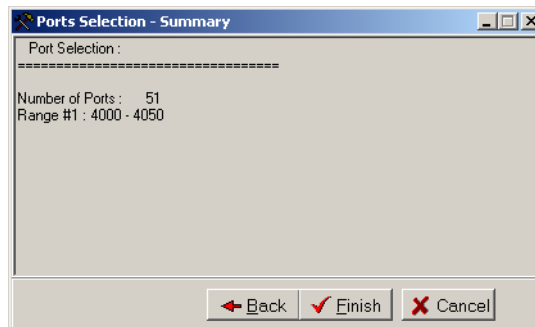
NOTE:

- The port range must be supplied by your system administrator.
- Do not define ports 1-1024, 2000, 2001, 2012, or 5000.

3. Click **Next**.

The Ports Selection Summary window appears.

Figure 5-3 Ports Selection Summary Window (Example)



Network Preparations

If using firewall software, open a pinhole for the RTP stream and the SIP ports by defining the following in the firewall software:

- VoIP Logger IP Address and ports that you just defined in **Configuring the Ports** on **page 79**.

SIP Configuration

Although this is a SIP Audio type of VoIP Logger, you do NOT need to change anything in the SIP Configuration.

Configuring the CTI Integrations for Cisco IP Phone-Based Active Recording Solution

This chapter describes the procedures for integrating Cisco's IP Phone-based Active Recording solution with NICE Perform Release 3.



IMPORTANT

Before configuring the Logger in NICE Perform Release 3, you must configure the **Configuring the Integration Package** on **page 84**, including the Media Provider (Observer). After configuring this, run all the Integration services on the VoIP Logger and the NICE Interactions Center. When all these things are done, **ONLY THEN** should you configure the Logger in NICE Perform Release 3.

Contents

Before you Begin	82
Configuring the Integration Package	84
Configuring the CTI Interface	85
Configuring the Connection Manager	97
Configuring the Driver	101
Configuring a Connection Manager for the VRSP (FSP)	109
Configuring the Media Provider Controller	114
Installing the NICE Integration Software	121

Before you Begin

To configure the NICE Perform CTI Integrations, you run a series of configuration wizards. Each configuration wizard requires you to enter specific information - some of which may have been entered on the switch.

Verify that you have *all* necessary information listed in each of the following sections BEFORE you start your configuration:

- **CTI Interface Configuration**
- **Connection Manager Configuration**
- **Driver Configuration**
- **SNMP Service Installation**
- **Configuring the Integration Package**

CTI Interface Configuration



NOTE: It is important that the Cisco System Administrator is present during the installation to assist with this phase of the installation.

Before proceeding with **Configuring the CTI Interface** on **page 85**, have ready the following information:

- Cisco Unified Communications Manager server IP Address
- If there is a secondary CTI server, the Cisco Unified Communications Manager connection IP Address
- Interface type and its port
- AXL Communications Manager User name and password (see **Terms and Concepts** on **page 13** for an explanation of AXL)
- AXL Communications Manager port, see **TSAPI Ports** on **page 83**
- SIP Trunk port - **5062**
- MPCM (FLM) URI address and port
- VRSP (FSP) address
- A list of all extensions that need to be monitored

Ensure:

The following is monitored:

- Extension - includes extensions used for extensions mobility
- ACD (Hunt group)
- IVR (CTI port)
- PickUp Group

TSAPI Ports

Cisco Communications Manager Server and the NICE Interactions Center Server can be on any subnet, but there has to be IP routing between them. Verify which ports (TCP/UDP) need to have permissions on any existing firewall.

- **For AXL port information**, refer to the section *Web Requests from CCMAAdmin or CCMUser to Cisco Unified CallManager* in the document below. The recommended secure port numbers are **443** or **8443**. The recommended non-secure port number is **80**. See **CTI Interface - Additional Switch Parameters** on **page 188**.
- **For non-secure TSP port information**, refer to the section *Communication between Applications and Cisco Unified Communications Manager* in the document below and see **CTI application server**. The recommended port number is **2748**.

For more information, see the *Cisco Unified Communications Manager 6.1 TCP and UDP Port Usage* white paper:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/6_1/61plrev1.pdf

Connection Manager Configuration

Before proceeding with **Configuring the Connection Manager** on **page 97**, have ready the following information:

- The name, port, and ID number of the Connection Manager
- The IP address or Host Name where the Connection Manager is installed
- Reporting levels for all messages, if different from the defaults
- If any Connection Manager parameters need to be defined, their names and values
- The Interfaces that will be connected to the Connection Manager and any parameters and their values that might need to be customized.

Driver Configuration

Before proceeding with **Configuring the Driver** on **page 101**, have ready the following information:

- The name and ID number of the driver
- The IP address or Host Name where the driver is installed
- The NICE Interactions Center server connected to the driver
- Reporting levels for all messages, if different from the defaults
- If any driver parameters need to be defined, their names and values
- The Interface that will be connected to the driver.

SNMP Service Installation

Before installing the integration software make sure that the SNMP Service is installed on your computer.

Configuring the Integration Package

This section describes the Integration Package configuration procedures.

Perform the following procedures:

- [Configuring the CTI Interface](#)
- [Configuring the Connection Manager](#)
- [Configuring the Driver](#)



NOTE: All system components must also be associated with each other appropriately.



IMPORTANT

For Cisco's IP Phone-based Active Recording solution with *redundancy*, you require two integration installations:

- On the NICE Interactions Center
- On the VRSP (FSP) machine.

For more information, see [Configuring VRSP \(FSP\) for Redundancy](#) on [page 135](#).

Configuring the CTI Interface

The CTI Interface defines the actual CTI Manager with which the system integrates. For every interface, a switch is configured. This is the physical server on which the interface is installed. More than one interface may be installed on the same switch, it is therefore important when configuring the interface that the correct switch is defined.

You begin the NICE Perform CTI integration configurations by configuring the CTI Interface. This procedure describes how to create a CTI interface.

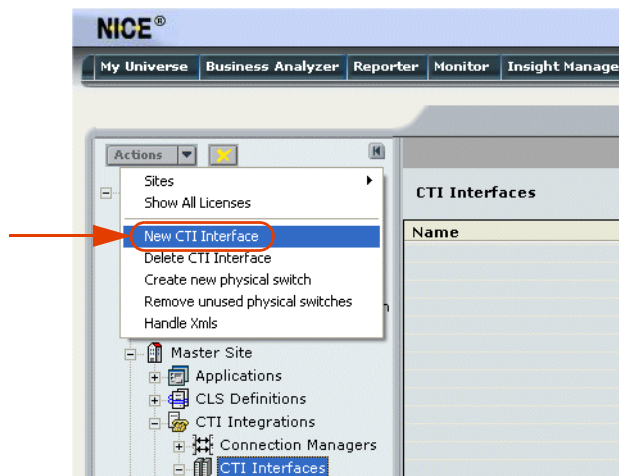


NOTE: For more information regarding defining for hunt groups, CTI ports and Pickup groups, see

To configure the CTI interface:

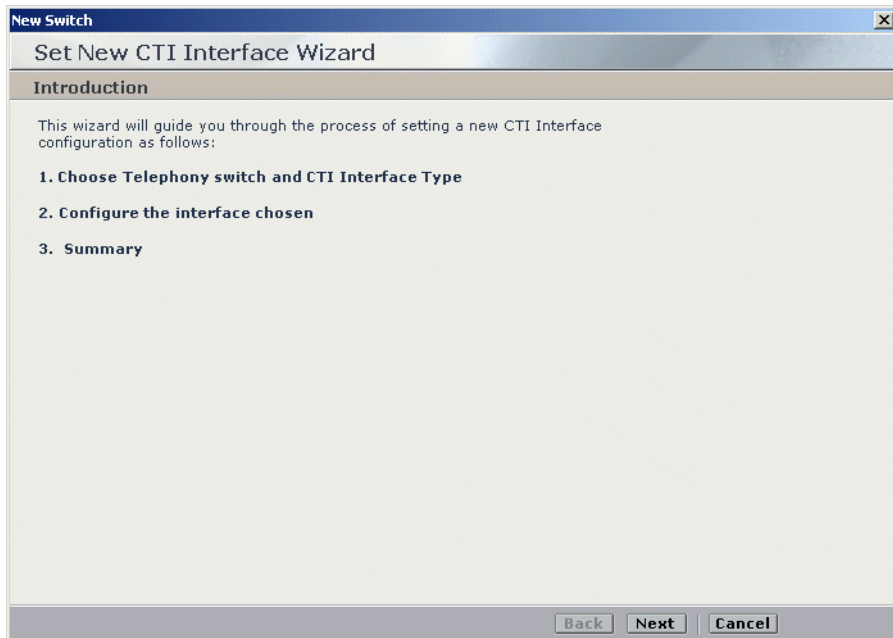
1. Verify that you are working in Technician mode: In the Organization tree, click **Organization**. Then mark the **Technician Mode** checkbox and click **Save** .
2. In the System Administrator, in the **Organization** tree, navigate to **Master Site > CTI Integrations** and select **CTI Interfaces**.
3. From the **Actions** menu, choose **New CTI Interface**.

Figure 6-1 Selecting New CTI Interface



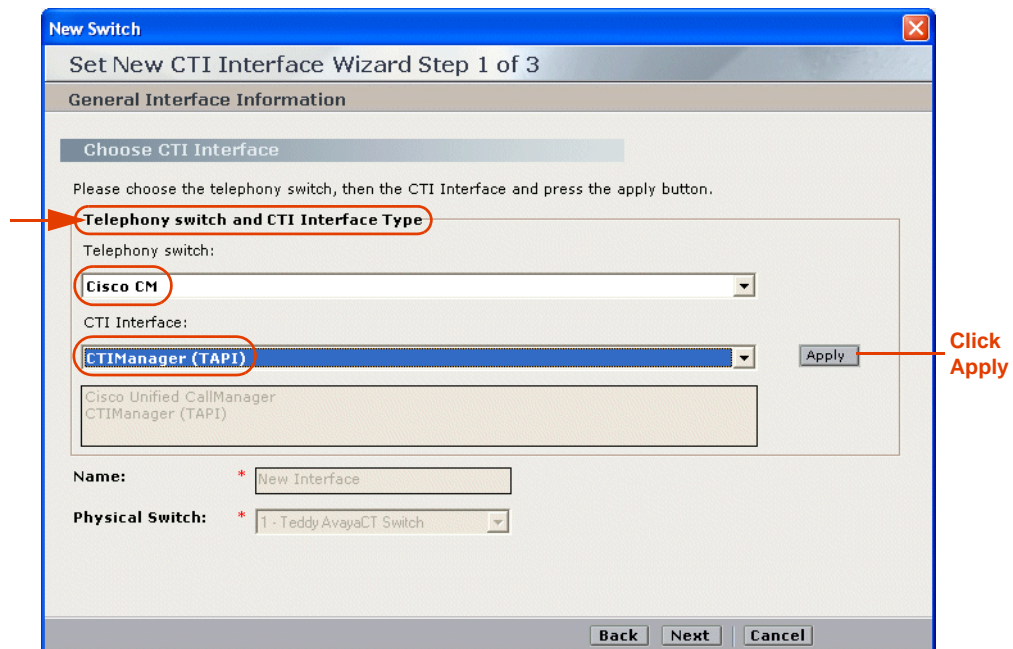
The Set New CTI Interface Wizard starts.

Figure 6-2 Set New CTI Interface Wizard Window



4. Click **Next**. The Set New CTI Wizard Step 1 of 3 window appears displaying the **Choose CTI Interface** section.

Figure 6-3 Choose CTI Interface Section



- a. In the **Telephone switch and CTI Interface Type** area, click the **Telephony switch** drop-down list and choose **Cisco CM**.
- b. Click the **CTI Interface** drop-down list and choose **CTIManager (TAPI)**.

c. Click **Apply**.

The **Name** and **Physical Switch** fields become enabled and the **Create** button appears.

Figure 6-4 Choose CTI Interface Section

d. In the **Name** field, type the new interface name.

e. Select the **Physical Switch**:

- To create a new physical switch, click **Create**. The New Physical Switch window appears. Continue with step numbers **5** and **6**.
- To use an existing switch, continue with step number **6**.

Figure 6-5 New Physical Switch Window

5. To create a New Physical Switch:

- a. In the **Switch Name** field, type a name for the switch.
- b. In the **Physical Switch ID** field, type a switch ID.



NOTE: Give the Physical Switch a unique ID.

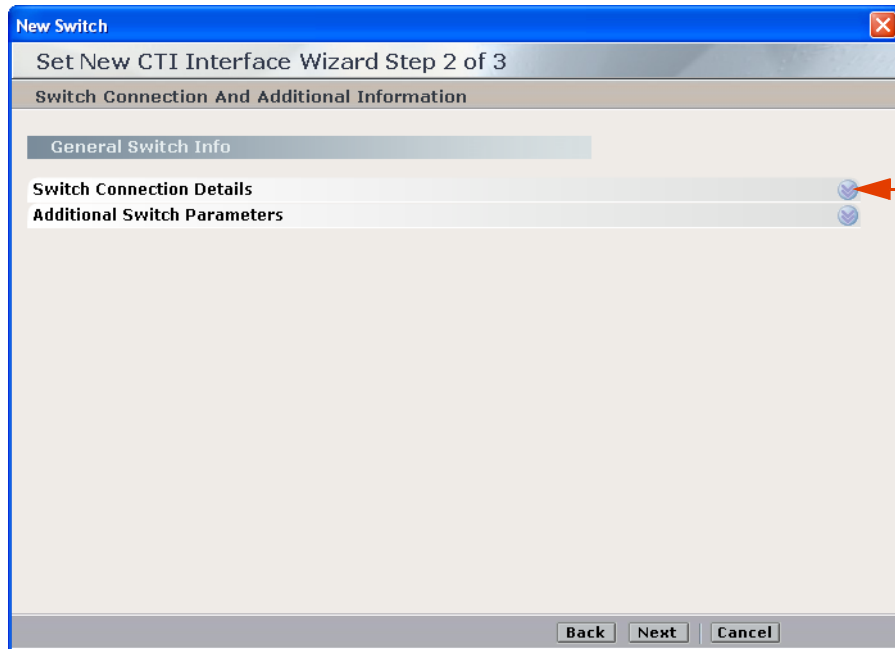
- c. In the **CLS Reporting Type** field, leave **CTI** as the default setting.
- d. **To enable non-standard CLS log-in options**, in the **Agent Logon Mode** area, leave the default checkboxes marked:
 - Marking **To the same station again** - allows agents to log in to the same workstation more than once.
 - Marking **To more than one station** - allows agents to log in to more than one workstation.
 - Marking **To a station another agent is logged into** - allows more than one agent to log in to one workstation.



NOTE: It is recommended that you leave all three **Agent Logon modes** marked.

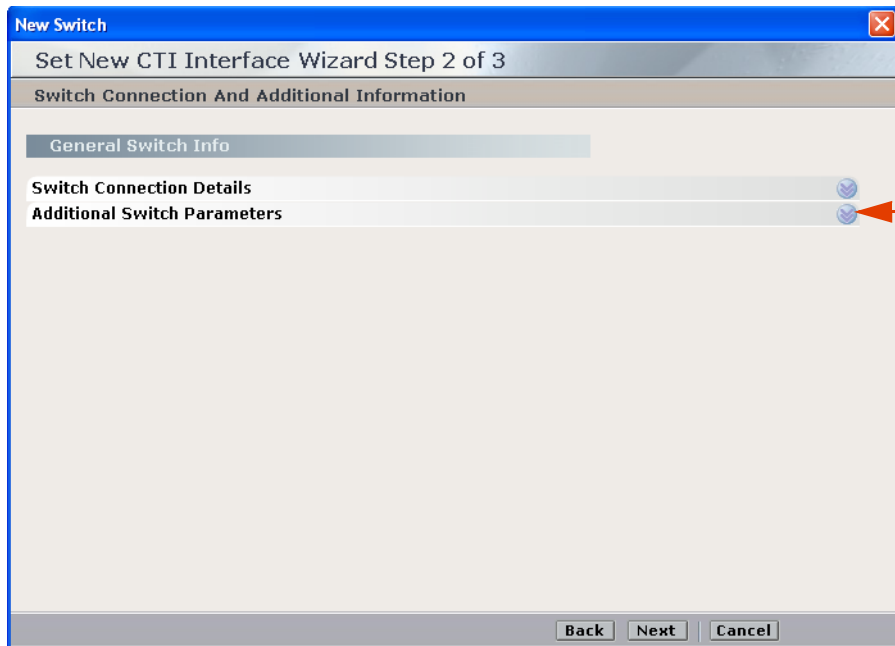
- e. Click **OK**. The newly created physical switch now appears in the Physical Switch list. The General Interface Information window reappears.
6. Click the **Physical Switch** list and choose the relevant physical switch.
 7. Click **Next**. The Set New CTI Wizard Step 2 of 3 window appears displaying the **General Switch Info** section.

Figure 6-6 General Switch Info Section



- Leave the default settings for the **Switch Connection Details**.

Figure 6-7 General Switch Info Section



8. If you need to import devices, expand **Additional Switch Parameters**. The **Additional Switch Parameters** area appears. If you do not need to import devices, continue with **Step 10**.

Figure 6-8 Additional Switch Parameters Area

New Switch
Set New CTI Interface Wizard Step 2 of 3
Switch Connection And Additional Information

General Switch Info

Switch Connection Details

Additional Switch Parameters

Display ReadOnly Information Mandatory fields are marked in red

Name	Value
AxlIpAddress	192.168.241.27
AxlPortId	8443
AxlUserId	CiscoActive
AxlPassword	*****
AxlSecured	True

Description: Password for the AKL

Back Next Cancel

9. To define the existing parameters or to create new ones, see **CTI Interface - Additional Switch Parameters** on **page 188**.
10. Click **Next**. The Set New CTI Wizard Step 2 of 3 window appears displaying the **Set Devices** section. Continue with the relevant procedure:
 - If you need to add devices, continue with **Step 11**.
 - If you do not need to add devices, continue with **Step 15**.

Figure 6-9 Set Devices Section

New Switch
Set New CTI Interface Wizard Step 2 of 3
Switch Devices Configuration

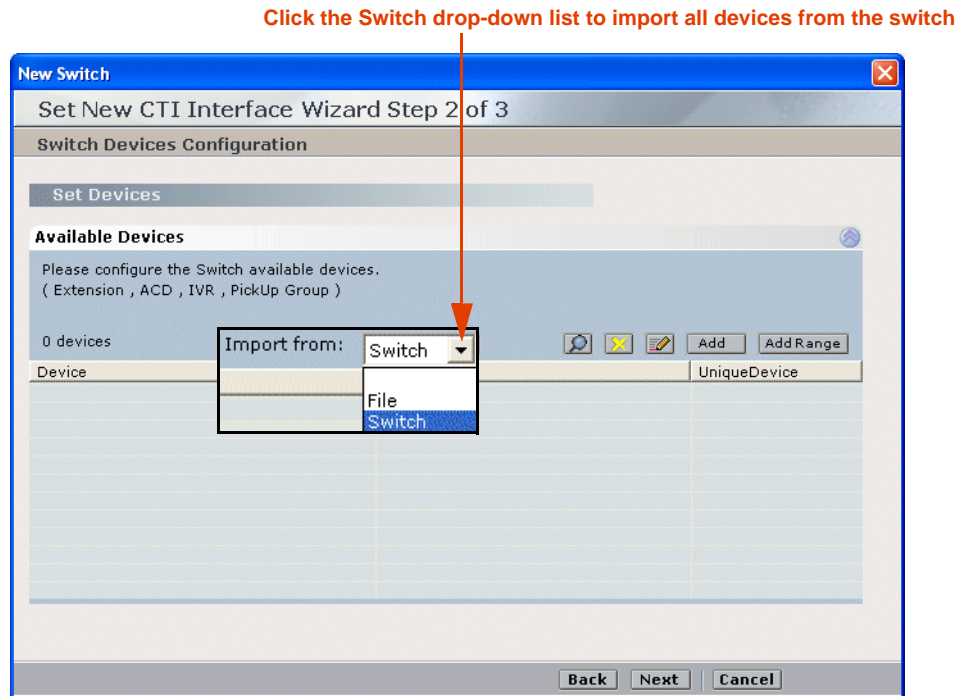
Set Devices

Available Devices

Back Next Cancel

11. Expand **Available Devices**. The **Available Devices** area appears.

Figure 6-10 Available Devices Area



Set devices by following the relevant procedure/s below.

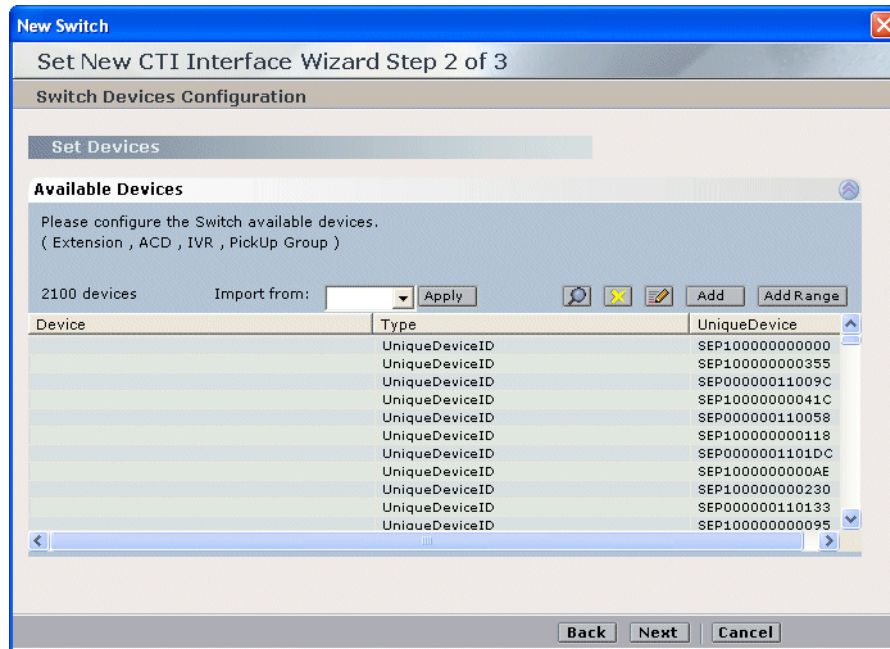
- a. **For Channel Mapping purposes**, you need to import a list of UniqueDeviceIDs (host names) from the switch using the AXL interface. Continue with **Importing Available Devices from the Switch** on [page 190](#). This enables you to import *all* available UniqueDeviceIDs directly from the switch.

The devices imported from the switch are imported with their UniqueDeviceIDs. They do not display in the Driver's **Monitor Devices** area, see [Figure 6-31](#) on [page 106](#). You perform this import from the switch only to enable the configuration of Channel Mapping. It does not take the place of defining the extensions, etc. You still need to either import devices from a text file or add the devices manually, see below.



NOTE: The same device can be listed with both a UniqueDeviceID (host name) and with a Device ID (extension number).

Figure 6-11 Available Devices Area



- b. To import a list of devices from an existing text file, continue with **Importing Text Files** on page 191.
- c. To add a single device, continue with step number 12.
- d. To add a range of devices, continue with step number 13 below.

12. To add a single device:

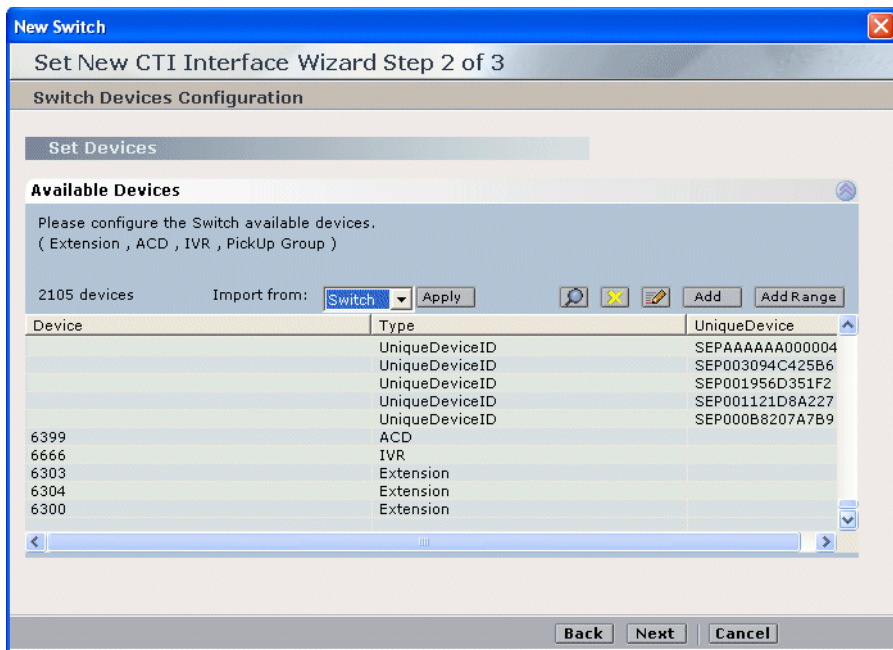
- a. Click **Add**. The Available Device window appears.

Figure 6-12 Available Device Window



- b. In the **Device Number** field, type the number you want to assign to the device. For:
 - Extension - add the device number
 - ACD (a hunt group) - add the device number of the hunt group.
 - IVR (a CTI Port used for call routing) - add the device number of the CTI port.
 - Pickup Group - add the number of the Pickup group.
- c. From the **Device Type** drop-down list, choose a device. The devices supported by the Cisco Unified Communications Manager switch are:
 - Extension
 - ACD (a hunt group)
 - IVR (a CTI Port used for call routing).
 - Pickup Group
- d. Click **OK**. The **Available Devices** area reappears displaying the added devices.

Figure 6-13 Available Devices Area



13. To add a range of devices:

- a. Click **Add Range**. The Available Devices Add Range window appears.

Figure 6-14 Available Device Add Range Window

- b. Type the starting number in the **Start at device number** field. For:
 - Extension - add the first device number
 - ACD (a hunt group) - add the first device number of the hunt group.
 - IVR (a CTI Port used for call routing) - add the first device number of the CTI port.
 - Pickup Group - add the first number of the Pickup group.
- c. Type the number of devices you want to add in the **Number of devices to add field**.
- d. From the **Device Type** drop-down list, choose a device. The devices supported by the Cisco Communications Manager switch are:
 - Extension
 - ACD (a hunt group)
 - IVR (a CTI Port used for call routing). Add the device number of the CTI port.
 - Pickup Group

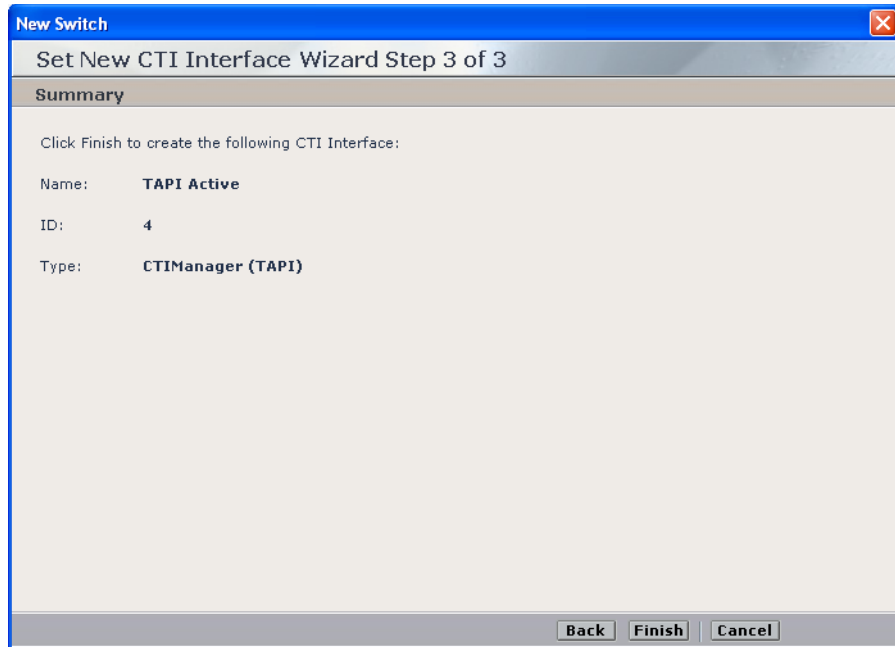


NOTE: ACD and Pickup Group are not recorded. They are added here so that accurate analysis can be made regarding events. There is also no need to configure channeling for them.

14. Click **OK**. The Set New CTI Wizard Step 2 of 3 window reappears displaying all the devices that you have added.

- Click **Next**. The Summary window appears.

Figure 6-15 Summary Window

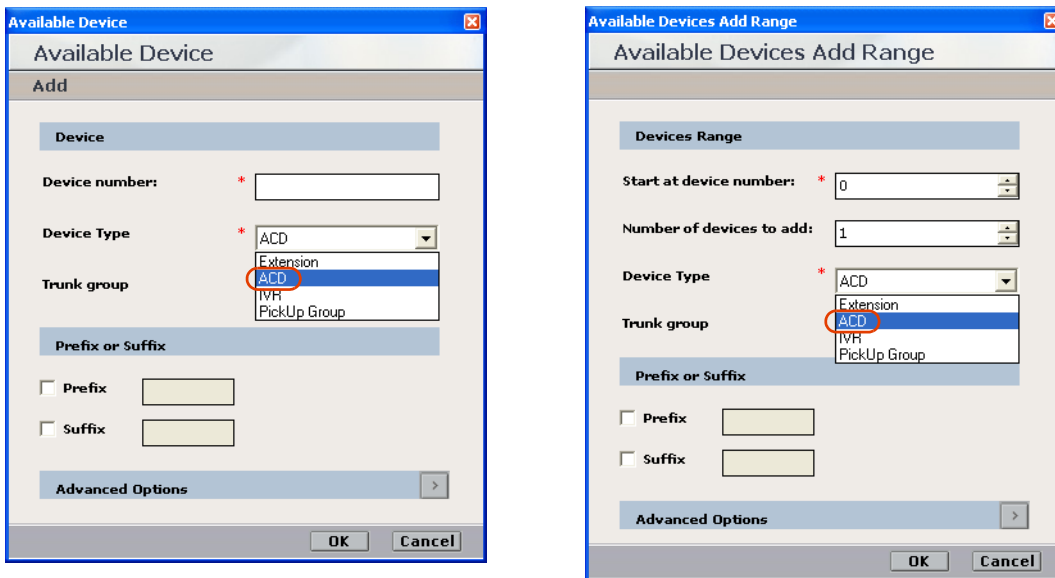


- Click **Finish**. The CTI interface is created.

Monitoring ACDs (Hunt Groups)

You can add monitoring for Hunt Groups by adding ACD devices, see [Step 12 on page 92](#) and [Step 13 on page 93](#).

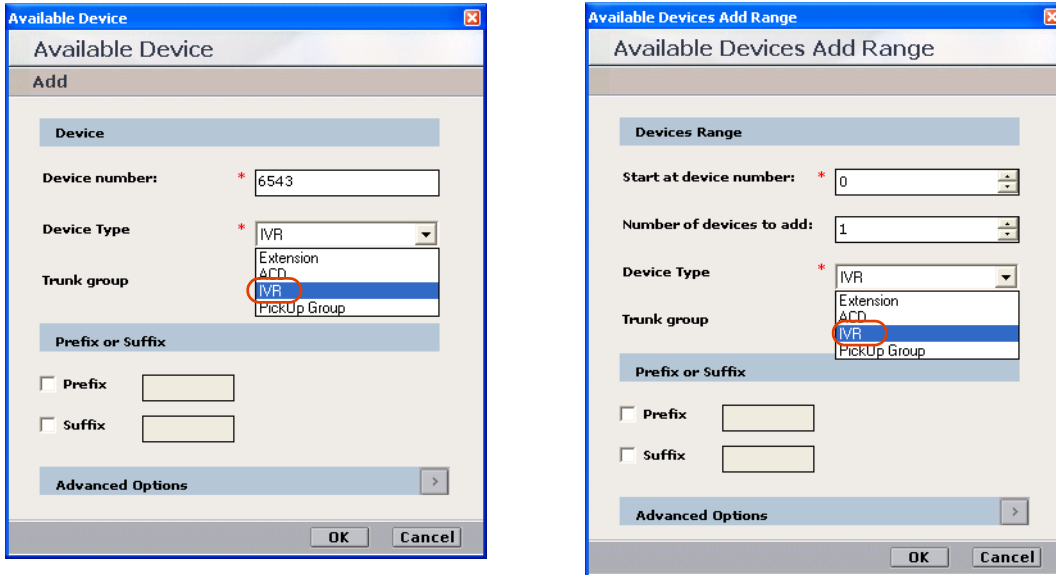
Figure 6-16 Available Device Window - ACD (Hunt Group)



Monitoring IVRs (CTI Ports)

You can add monitoring for CTI ports by adding **IVR** devices, see **Step 12** on **page 92** and **Step 13** on **page 93**.

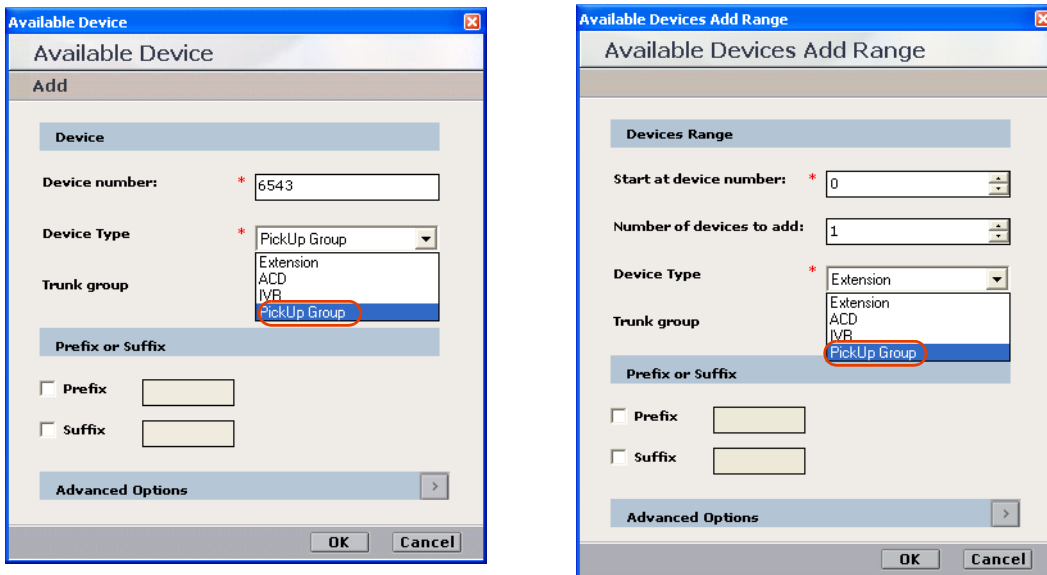
Figure 6-17 Available Device Window - IVR (CTI Port)



Monitoring Pickup Groups

You can add monitoring for Pickup groups by adding **PickUp Group** devices, see **Step 12** on **page 92** and **Step 13** on **page 93**.

Figure 6-18 Available Device Window - Pickup Group



Configuring the Connection Manager

The Connection Manager is used for creating and maintaining the CTI link. It functions as a pipeline for transferring information between the interface and the driver/s once the link is established. One Connection Manager can be used to connect to several Interfaces and can have several Drivers.

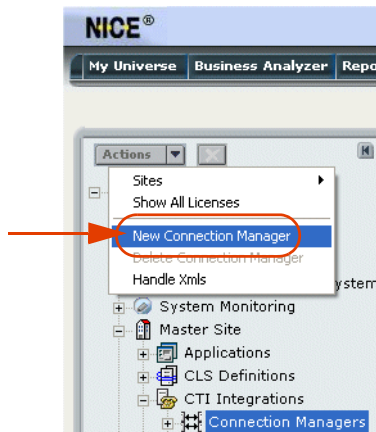
After configuring the CTI Interface, you must configure the Connection Manager to the TAPI Active link that you created in the CTI Interface.

The Connection Manager module will interface with the switch to receive all of the relevant CTI events and information.

To configure the Connection Manager:

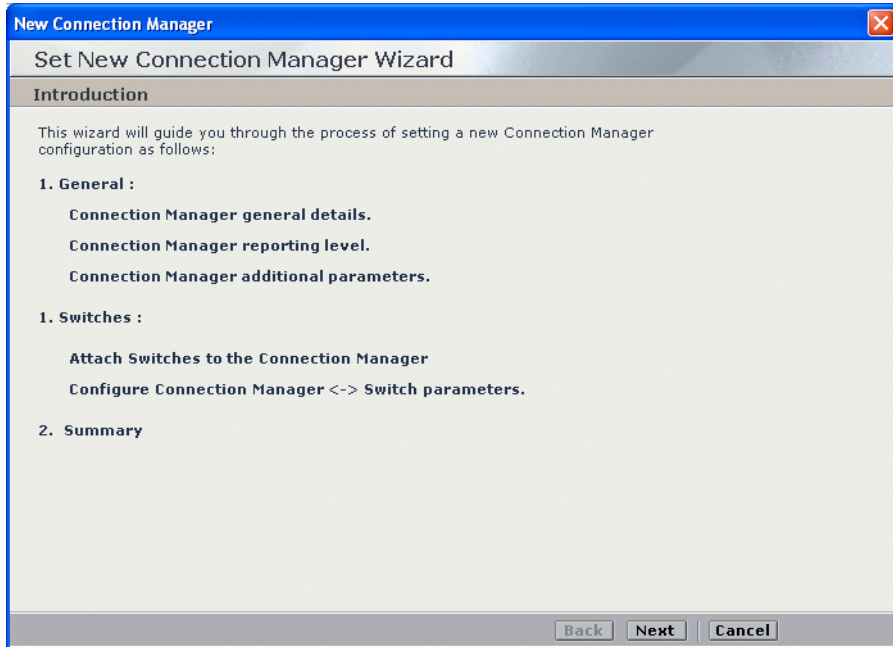
1. In the **Organization** tree, under **Master Site > CTI Integrations**, choose **Connection Managers**.
2. From the **Actions** menu, choose **New Connection Manager**.

Figure 6-19 Actions Menu



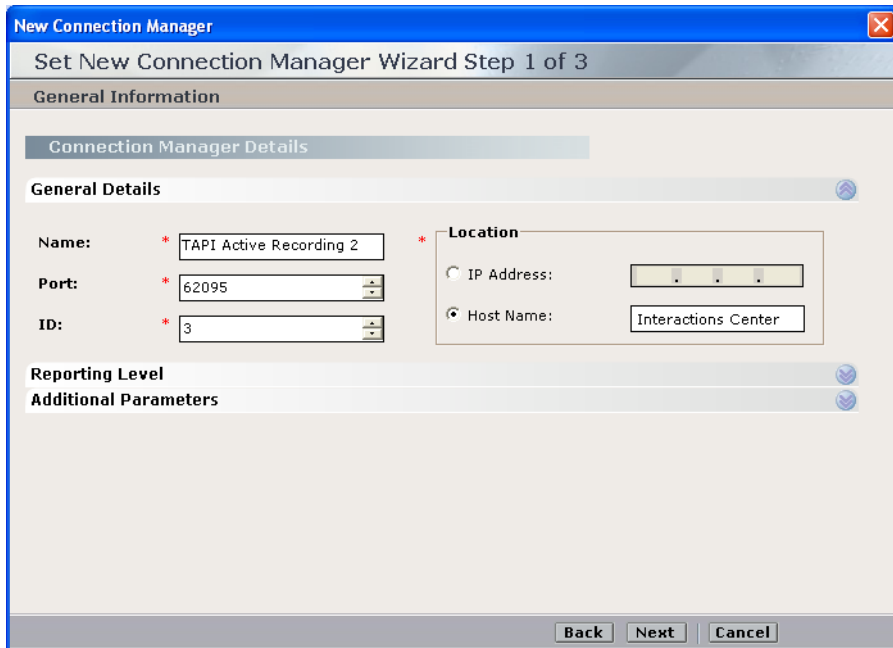
The Set New Connection Manager Wizard starts.

Figure 6-20 Set New Connection Manager Wizard - Introduction Window



3. Click **Next**. The Set New Connection Manager Wizard Step 1 of 3 window appears displaying the **General Details** area.

Figure 6-21 General Details Area



- a. In the **Name** field, type the name you want to give to the Connection Manager.

- b. Accept the default port number.



NOTE: Do not change the default port number.

- c. In the **ID** field, type the ID number you want to give to the Connection Manager.
 - d. In the **Location** area, select either the **IP Address** or the **Host Name** of the computer on which the Connection Manager is located. This is usually the Interactions Center.
4. It is recommended to accept the existing defaults for the Connection Manager's **Reporting Levels**.

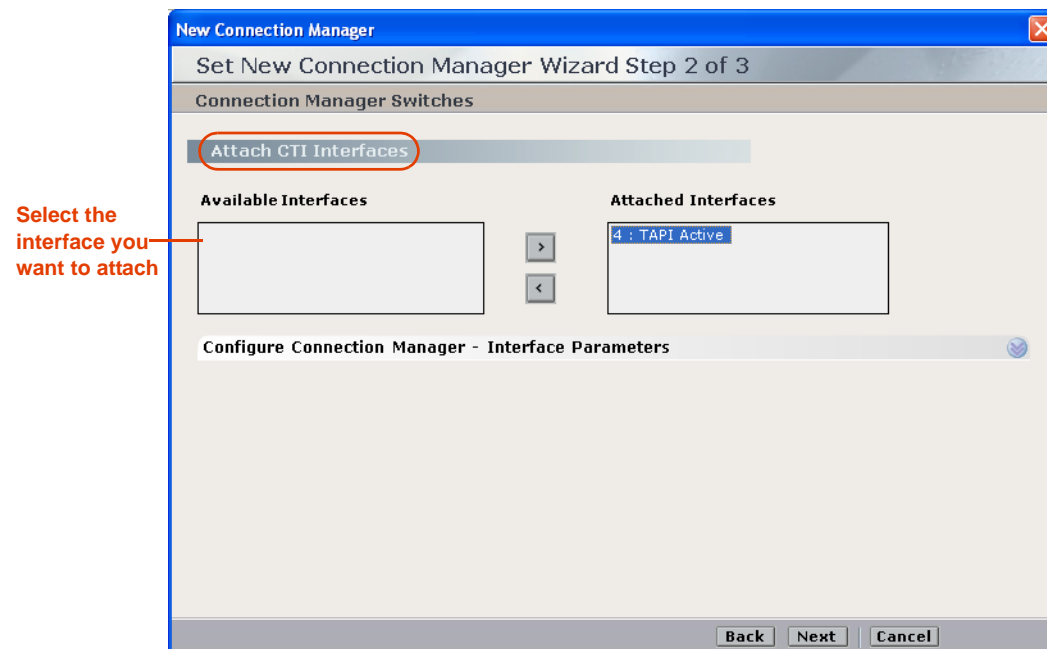
If it should be necessary to make changes, see **Reporting Levels** on **page 193**.

5. It is recommended to accept the existing defaults for the Connection Manager's **Additional Parameters**.

If it should be necessary to define existing parameters or to create new ones, see **Connection Manager - Additional Parameters** on **page 195**.

6. Click **Next**. The Set New Connection Manager Wizard Step 2 of 3 window appears displaying the **Attach CTI Interfaces** section.

Figure 6-22 Attach CTI Interfaces Section



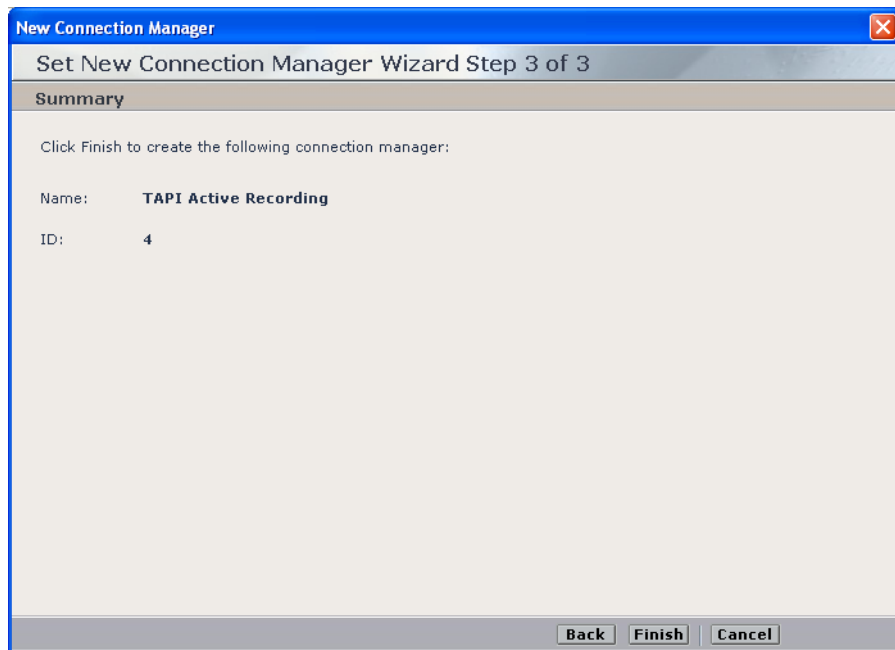
All available CTI Interfaces are listed in the **Available Interfaces** list.

- a. Select the interface(s) you want to attach and click the arrow to transfer the interface(s) to the **Attached Interfaces** list.
- b. It is recommended to accept the existing defaults for the **Connection Manager - Interface Parameters**.

If you need to define existing parameters or to create new ones, see [Connection Manager - Interface Parameters](#) on [page 197](#).

7. Click **Next**. The Summary window appears.

Figure 6-23 Summary Window



The Summary window displays the Connection Manager name and ID.

8. Click **Finish** to create the Connection Manager.

Upon completion, the System Administrator page reappears and the new Connection Manager appears in the list of Connection Managers.



NOTE: For details pertaining to maintaining or changing the Connection Manager or any of its definitions, refer to the *NICE Perform System Administrator's Guide*.

Configuring the Driver

You now need to define the driver. The driver is used to get the actual events from the Interface via the Connection Manager. When the driver receives these events, they are filtered and translated into CAPI commands (start call, end call) or discarded according to the system configuration (recording rules, CTI analysis installed, and so on).

Extension Mobility Guidelines

It is very important for extension mobility to define *all* devices in the **Monitor Devices** area, see step **11** on **page 106**. After you define the devices there, the TAPIMonitor will monitor them. See **Verifying the TSP Client Configuration** on **page 67**.

Creating the Driver

After configuring the Connection Manager, you create the driver and connect it to the Connection Manager.

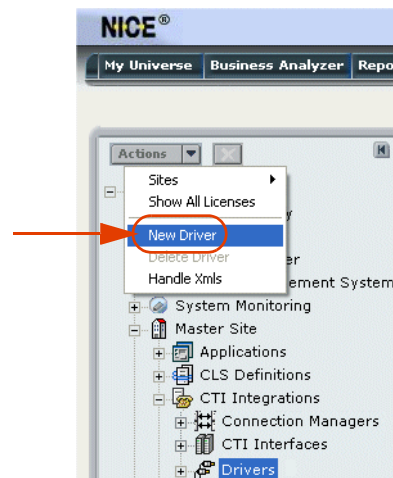


NOTE: The driver needs to be associated with a Connection Manager. This is only possible after you have defined the Connection Manager, see **Step 10** on **page 105**.

To create the driver:

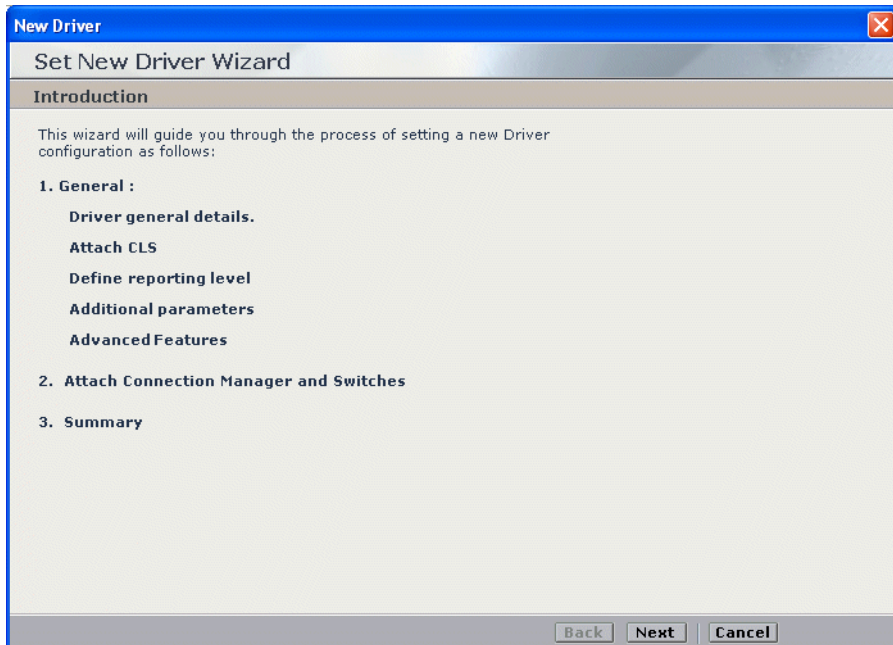
1. In the System Administrator, in the **Organization** tree, navigate to **Master Site > CTI Integrations** and select **Drivers**.
2. From the **Actions** menu, choose **New Driver**.

Figure 6-24 Actions Menu



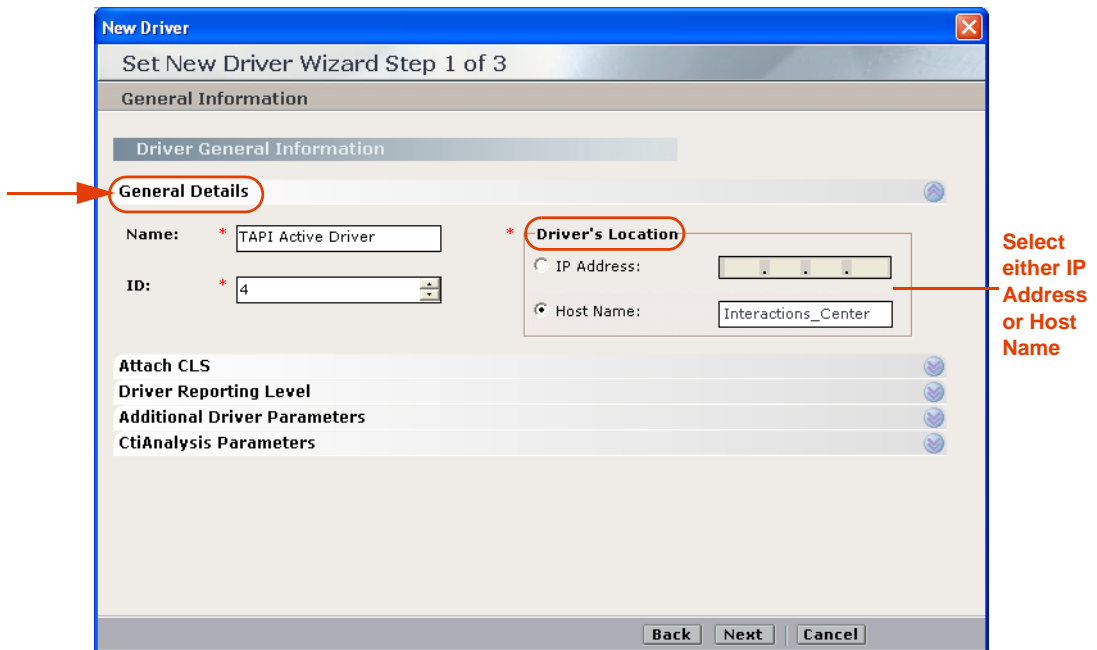
The Set New Driver Wizard starts.

Figure 6-25 Set New Driver Wizard - Introduction Window



3. Click **Next**. The Set New Driver Wizard Step 1 of 3 window appears displaying the **General Details** area.

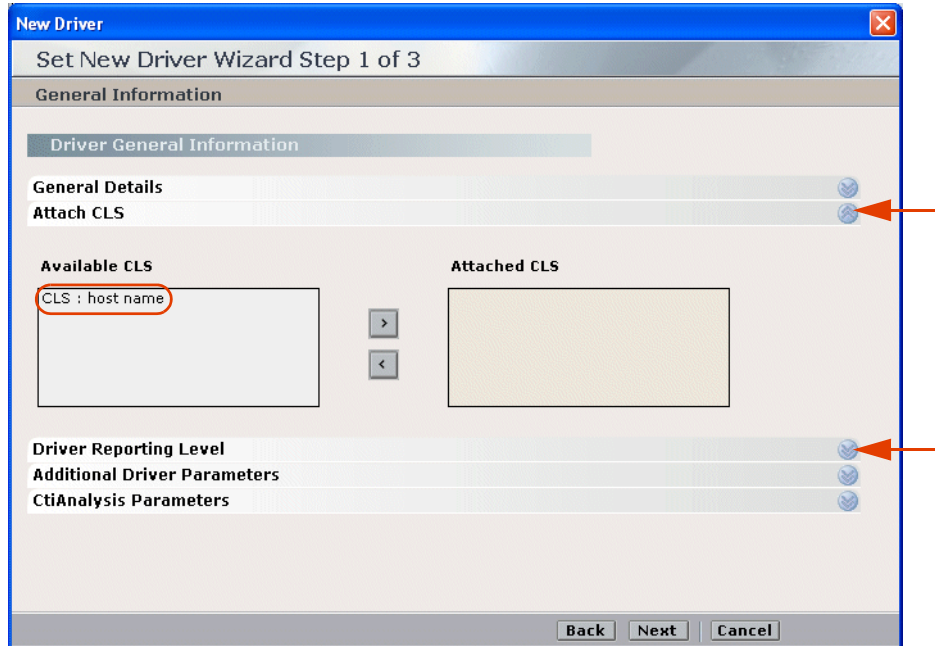
Figure 6-26 General Details Area



- a. In the **Name** field, type the name you want to give to the driver.
- b. In the **ID** field, type the ID number you want to give to the driver.

- c. In the **Driver's Location** area, type either **IP Address** or **Host Name** for the computer on which the NICE Integrations are installed. This is usually the Interactions Center.
4. Expand **Attach CLS**. The **Attach CLS** area appears.

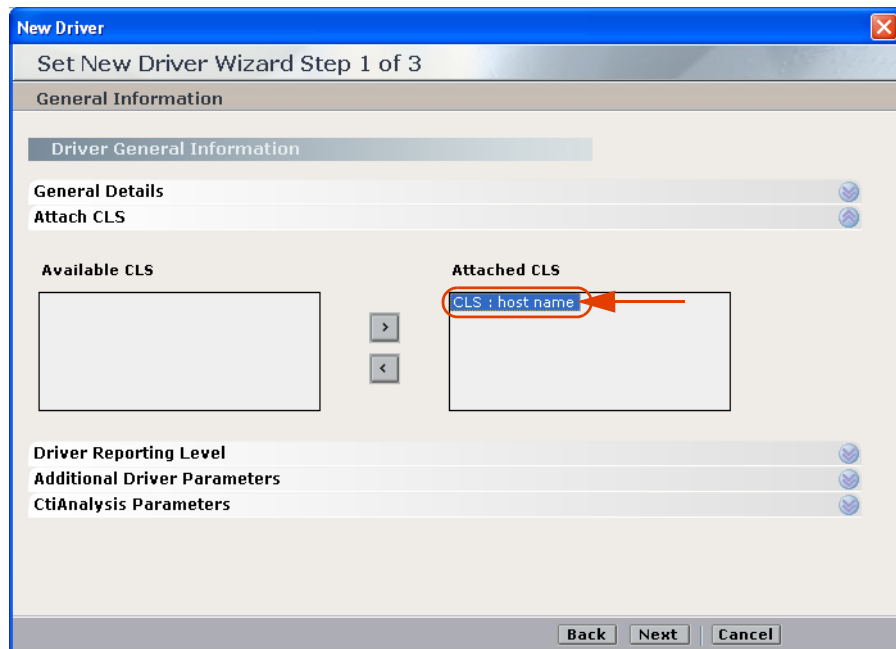
Figure 6-27 Attach CLS Area



All available CLS servers are listed in the **Available CLS** list.

5. Select the CLS server(s) you want to attach and click the arrow to transfer the CLS server to the **Attached CLS** list.

Figure 6-28 Attach CLS Area



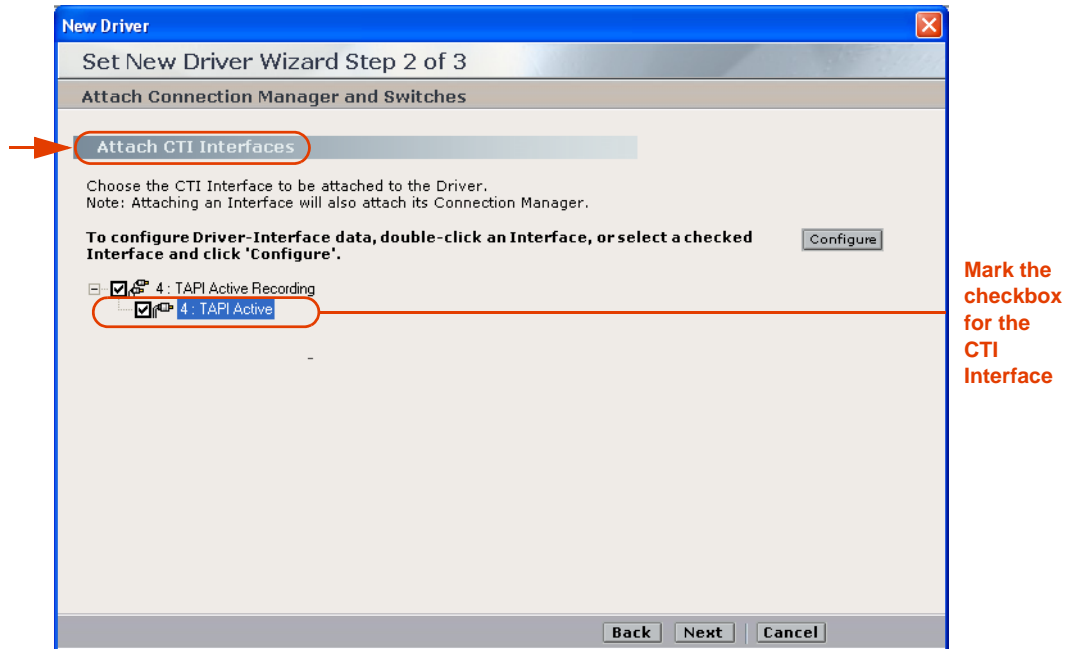
6. It is recommended to accept the existing defaults for the new **Driver Reporting Level** parameters.



NOTE: Setting up the reporting level is similar for all the different Integration components.

7. It is recommended to accept the existing defaults for the New Driver's **Additional Driver Parameters**.
If it should be necessary to define existing parameters or to create new ones, see **Driver - Additional Driver Parameters** on [page 199](#).
8. It is recommended to accept the existing defaults for the New Driver's **CtiAnalysis Parameters**.
9. Click **Next**. The Set New Driver Wizard Step 2 of 3 window appears displaying the **Attach CTI Interfaces** section.

Figure 6-29 Attach CTI Interfaces Section



NOTE: After creating the Connection Manager and the driver, you must specify the switch (CTI Server) with which this Connection Manager will be associated. In this case the Connection Manager will be associated with the Cisco TAPI Active CTI interface created previously, see [Configuring the CTI Interface](#) on [page 85](#).

10. To attach the CTI interface:

- a. In the **Attach CTI Interfaces** area, mark the checkbox for the CTI Interface you want to attach to this driver.



NOTE: When you mark the checkbox for the CTI Interface, the checkbox for the corresponding Connection Manager automatically becomes marked as well. You cannot mark the checkbox of the Connection Manager by itself.

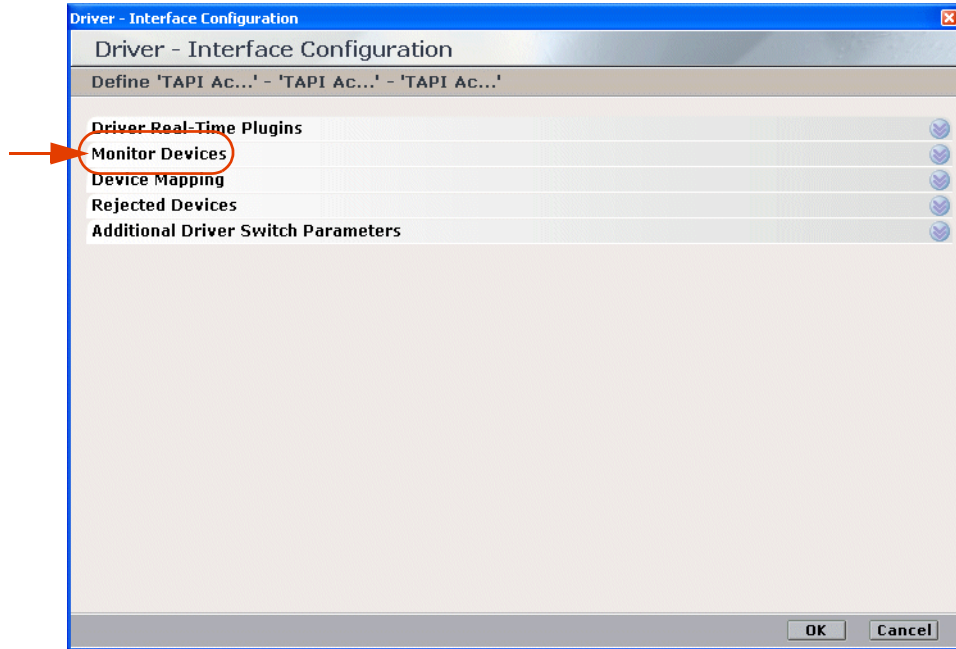
- b. Double-click the relevant interface.

-or-

Select the relevant interface and click **Configure**.

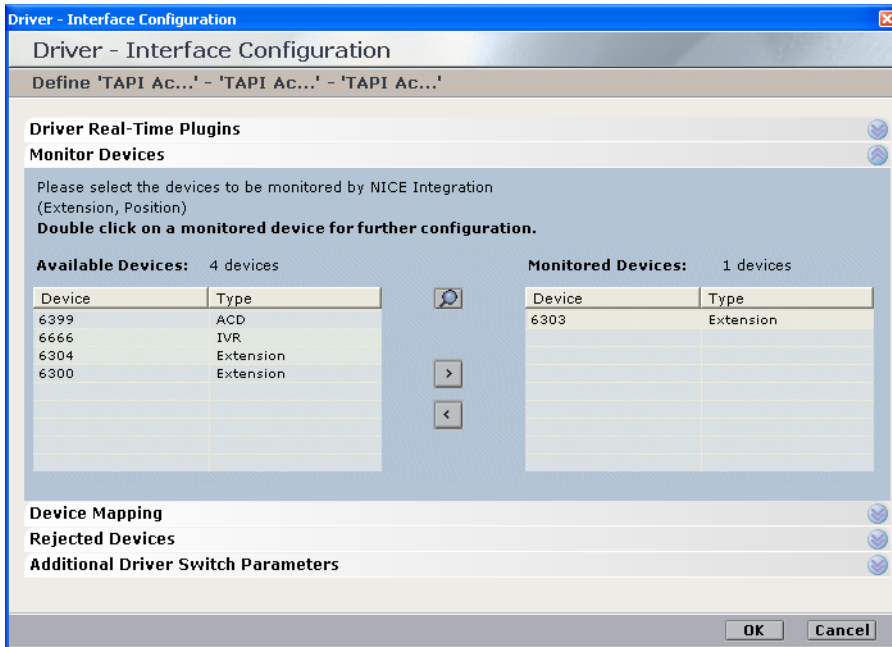
The Driver - Interface Configuration Window appears.

Figure 6-30 Driver - Interface Configuration Window



11. Expand **Monitor Devices**. The **Monitor Devices** area displays.

Figure 6-31 Monitor Devices Area



All available devices are listed in the **Available Devices** list.



NOTE: The UniqueDeviceID devices do not display in the **Available Devices** area.

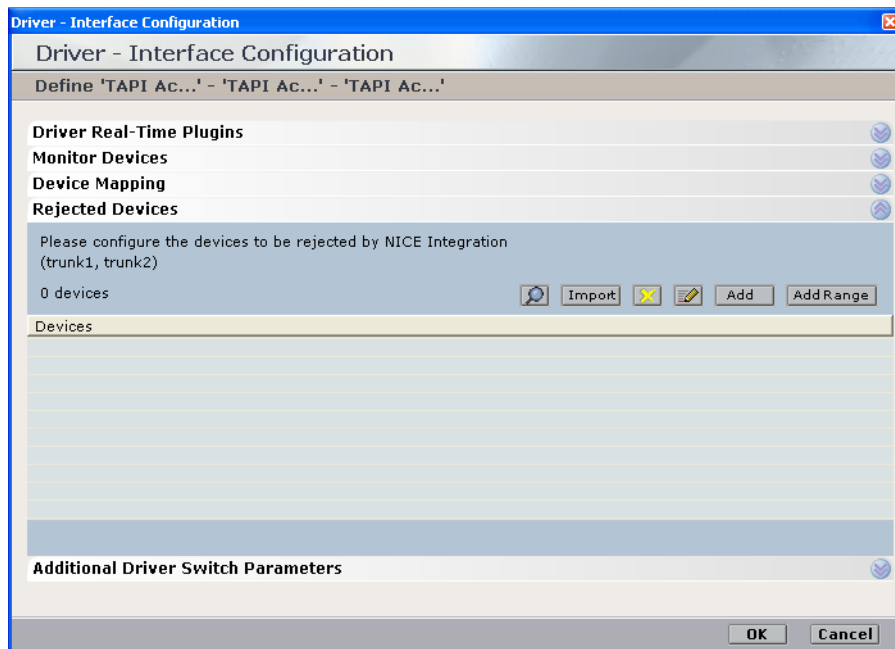
- Select the device(s) you want to monitor and click the arrow to transfer the device(s) to the **Monitored Devices** area. Include in this:
 - All ACD (hunt group) devices
 - All IVR (CTI port) devices
 - All Pickup group devices
 - All Extension Mobility numbers.



NOTE: It is highly recommended to monitor all available devices.

12. It is recommended to accept the existing defaults for the **Rejected Devices**.

Figure 6-32 Rejected Devices Area

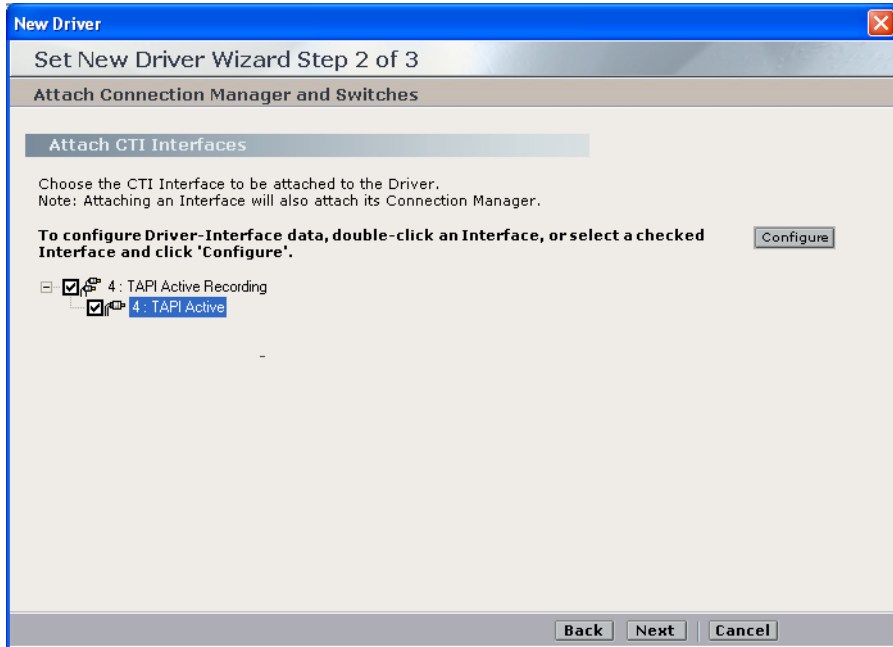


- a. If it should be necessary to define the devices that you do NOT want to record, expand **Rejected Devices**.
 - b. Use the **Import**, **Add**, or **Add Range** buttons to define the devices you do not want to record. For details, see [page 92](#).
13. It is recommended to accept the existing defaults for the **Additional Driver Switch Parameters**.

If it should be necessary to define existing parameters or to create new ones, see [Driver Interface - Additional Driver Switch Parameters](#) on [page 203](#).

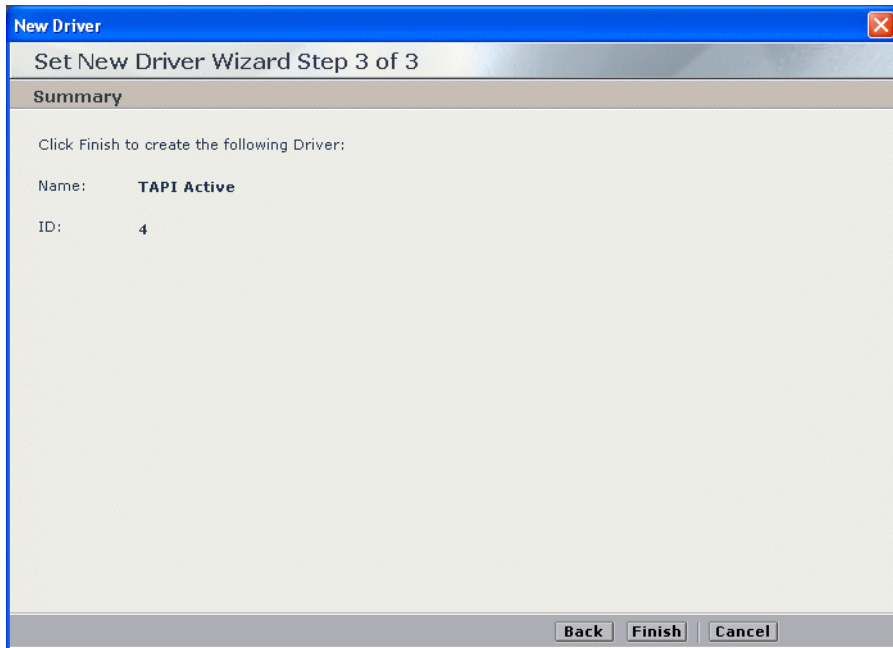
14. Click **OK**. The Set New Driver Wizard Step 2 of 3 window reappears displaying the **Attach CTI Interfaces** section again.

Figure 6-33 Attach CTI Interfaces Section



15. Click **Next**. The Summary window appears.

Figure 6-34 Summary Window



16. The Summary window displays the driver name and ID. Click **Finish** to create the new driver. The System Administrator page reappears and the new driver appears in the list of drivers.

NOTE: For details pertaining to maintaining or changing the driver or any of its definitions, refer to the *NICE Perform System Administrator's Guide*.

Configuring for Cisco IP Phone-based Active Recording

If you are configuring for a Cisco IP Phone-based Active Recording configuration, perform the following procedures:

- **Configuring a Connection Manager for the VRSP (FSP)**
- **Configuring the Media Provider Controller**
- **Verifying the CTI Integration**

Configuring a Connection Manager for the VRSP (FSP)

The VRSP (FSP) is configured according to your site installation. Choose the relevant location for the VRSP (FSP) accordingly:

- **Standard VRSP (FSP) installation** - install on the NICE Interactions Center
- **VRSP (FSP) redundancy** - install VRSP (FSP) twice:
 - Primary VRSP (FSP) on a separate machine NOT the NICE Interactions Center or a VoIP Logger
 - Redundant VRSP (FSP) is installed on the NICE Interactions Center



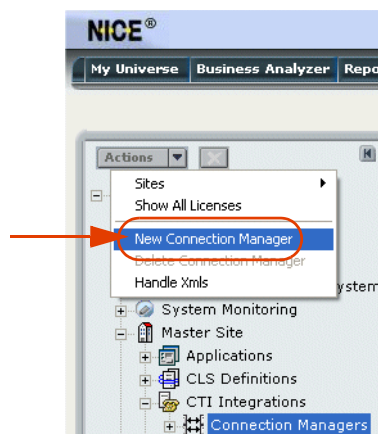
NOTE: Before you configure the Media Provider Controller, you must have the following:

- VRSP (FSP) IP address or Host name

To define a Connection Manager for the VRSP (FSP):

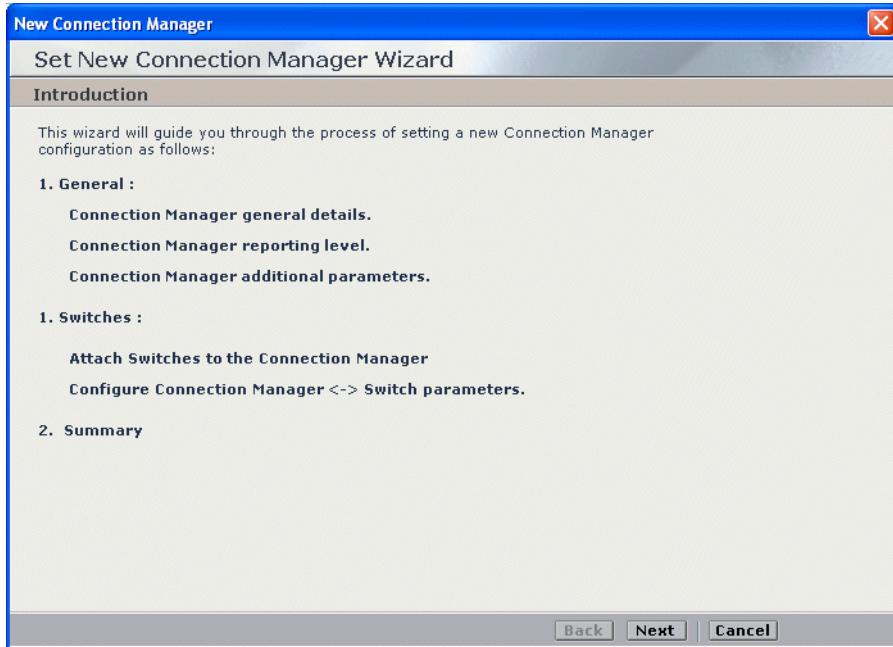
1. In the **Organization** tree, under **Master Site > CTI Integrations**, choose **Connection Managers**.
2. From the **Actions** menu, choose **New Connection Manager**.

Figure 6-35 Actions Menu



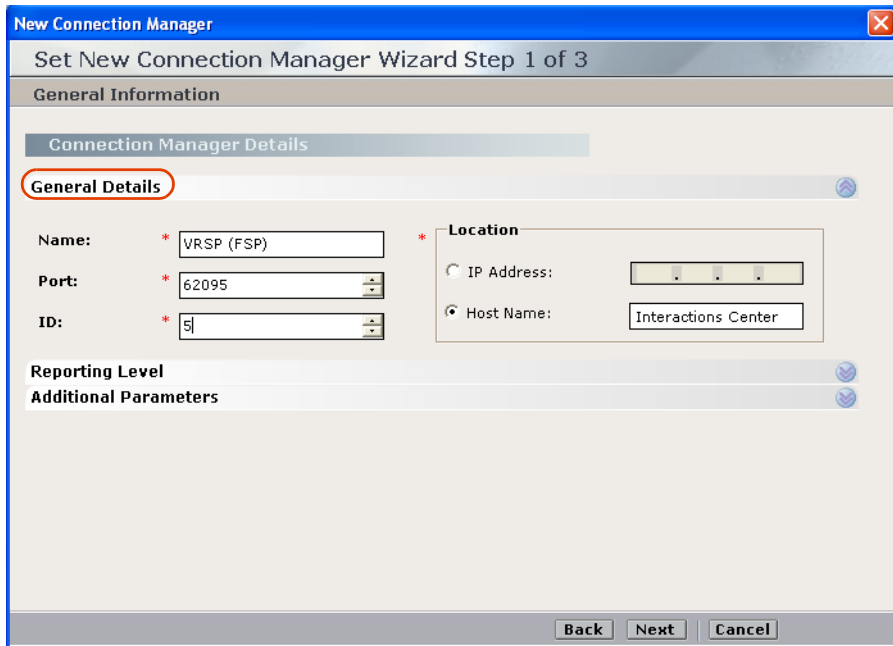
The Set New Connection Manager Wizard starts.

Figure 6-36 Set New Connection Manager Wizard - Introduction Window



3. Click **Next**. The Set New Connection Manager Wizard Step 1 of 3 window appears displaying the **General Details** area.

Figure 6-37 General Details Area



- a. In the **Name** field, type a meaningful name for this Connection Manager.

- b. Accept the default port number.



NOTE: Do not change the default port number.

- c. In the **ID** field, type the ID number you want to give to the Connection Manager.



NOTE: Assign an unique ID.

Figure 6-38 Location Area

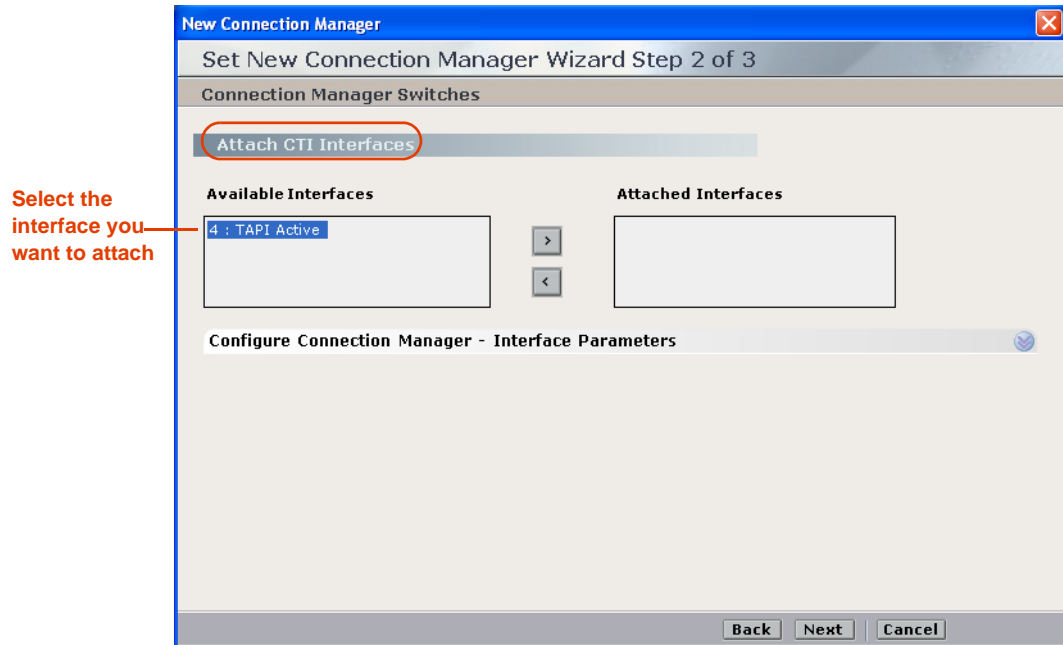
The screenshot shows a window titled "New Connection Manager" with a subtitle "Set New Connection Manager Wizard Step 1 of 3". The "General Information" section is expanded to show "Connection Manager Details". Under "General Details", there are three input fields: "Name:" with the value "VRSP (FSP)", "Port:" with the value "62094", and "ID:" with the value "5". To the right of these fields is a "Location" section, which is circled in red. It contains two radio buttons: "IP Address:" (unselected) and "Host Name:" (selected). The "Host Name:" field contains the text "Interactions Center". A red arrow points from the text "Type the IP address or Host Name of the VRSP (FSP)" to the "Host Name:" field. At the bottom of the window are "Back", "Next", and "Cancel" buttons.



NOTE: The IP address shown in the figure is only an example of the VRSP (FSP) address.

4. In the **Connection Manager's Location** area, select either **IP Address** or **Host Name** and type the computer on which the VRSP (FSP) is installed.
 - a. It is recommended to accept the existing defaults for the Connection Manager's **Reporting Levels**.
If it should be necessary to make changes, see **Reporting Levels** on **page 193**.
 - b. It is recommended to accept the existing defaults for the Connection Manager's **Additional Parameters**.
If it should be necessary to define existing parameters or to create new ones, see **Connection Manager - Additional Parameters** on **page 195**.
5. Click **Next**. The Set New Connection Manager Wizard Step 2 of 3 window appears displaying the **Attach CTI Interfaces** section.

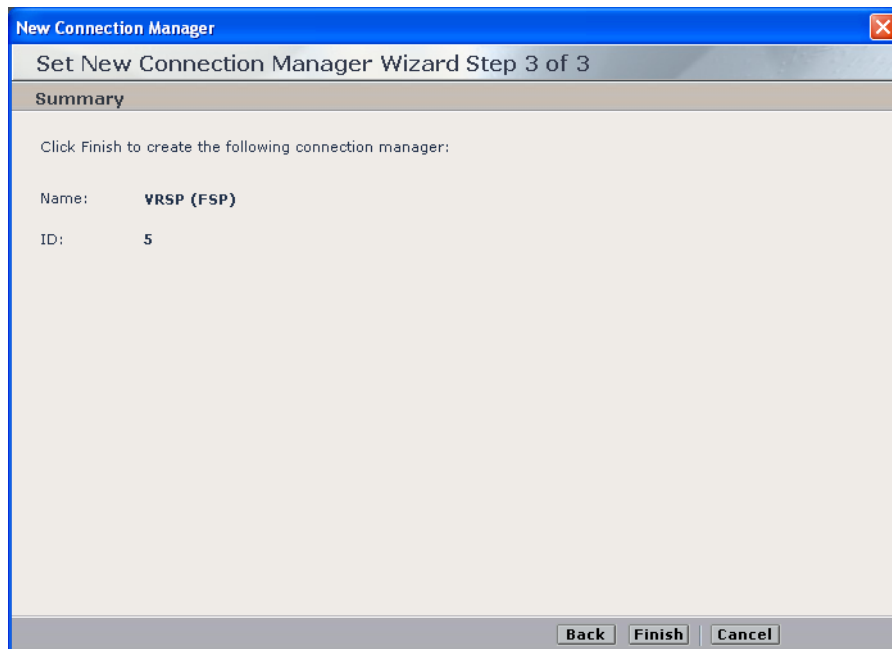
Figure 6-39 Attach CTI Interfaces Section



All available CTI Interfaces are listed in the **Available Interfaces** list.

- a. Select the interface(s) you want to attach and click the arrow to transfer the interface(s) to the **Attached Interfaces** list.
 - b. It is recommended to accept the existing defaults for the **Connection Manager - Interface Parameters**.
If you need to define existing parameters or to create new ones, see **Connection Manager - Interface Parameters** on [page 197](#).
6. Click **Next**. The Summary window appears.

Figure 6-40 Summary Window



The Summary window displays the Connection Manager name and ID.

7. Click **Finish** to create the Connection Manager.
8. Upon completion the System Administrator page reappears and the new Connection Manager appears in the list of Connection Managers.



NOTE: For details pertaining to maintaining or changing the Connection Manager or any of its definitions, refer to the *NICE Perform System Administrator's Guide*.

Configuring the Media Provider Controller

You now need to configure the Media Provider Controller for the VRSP (FSP).



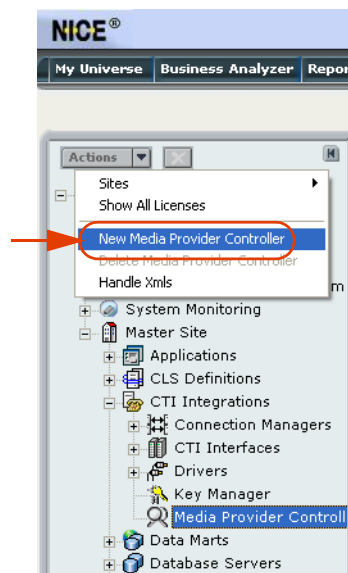
NOTE: Before you configure the Media Provider Controller, you must have the following:

- VRSP (FSP) Host name
- Connection Manager for VRSP (FSP)

To configure the Media Provider Controller:

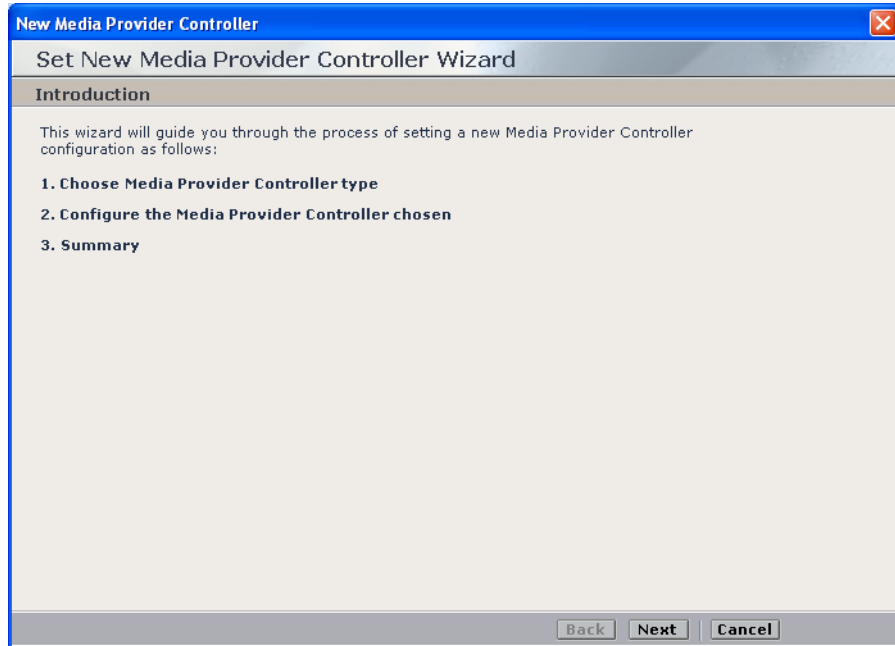
1. In the System Administrator, in the **Organization** tree, navigate to **Master Site > CTI Integrations** and select **Media Provider Controller**.
2. From the **Actions** menu, choose **New Media Provider Controller**.

Figure 6-41 Actions Menu



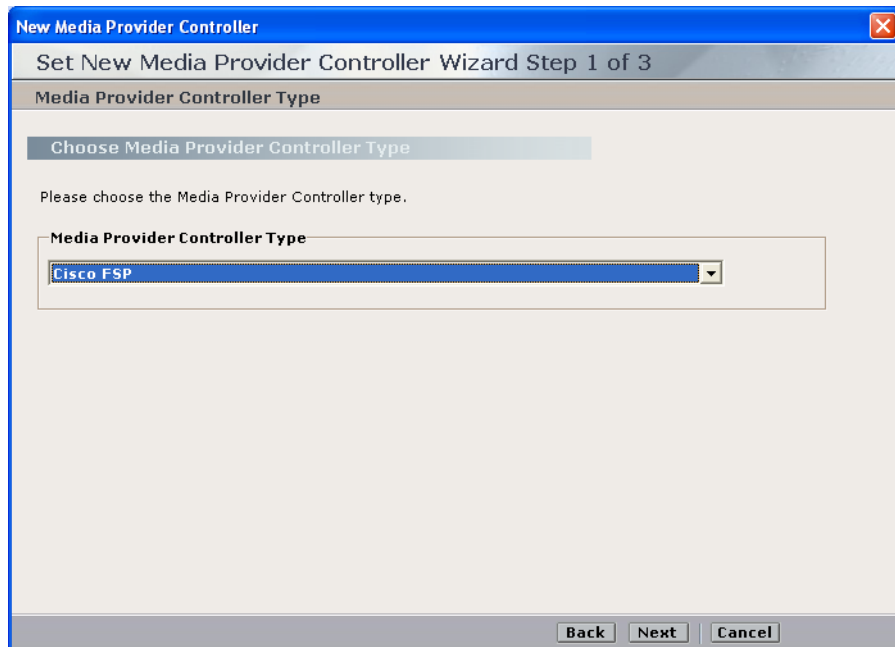
The Set New Media Provider Controller Wizard starts.

Figure 6-42 Set New Media Provider Controller Wizard - Introduction Window



3. Click **Next**. The Set New Media Provider Controller Wizard Step 1 of 3 window appears displaying the **Choose Media Provider Controller Type** section.

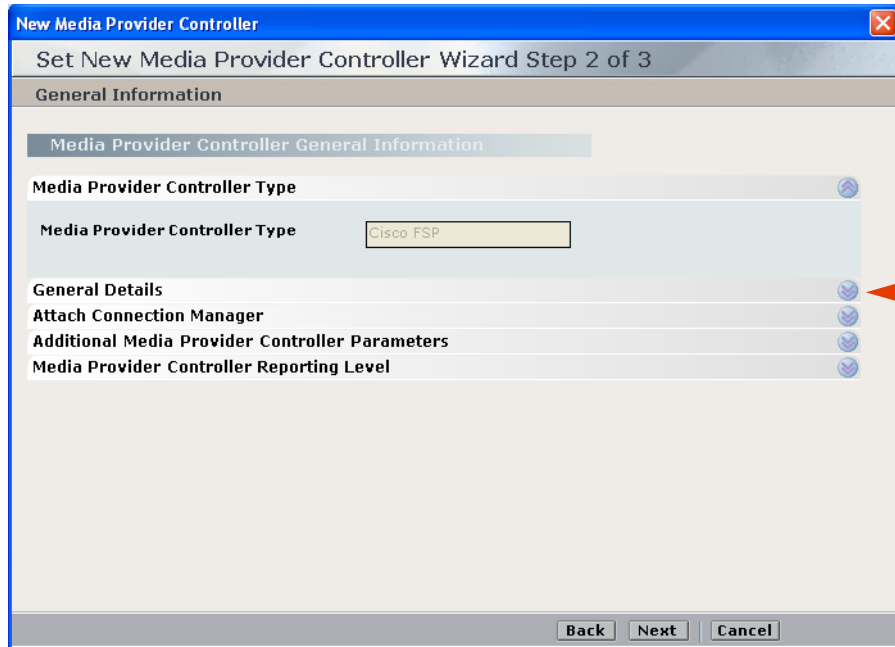
Figure 6-43 Choose Media Provider Controller Type Section



4. In the **Media Provider Controller Type** drop-down list, choose **Cisco FSP**.

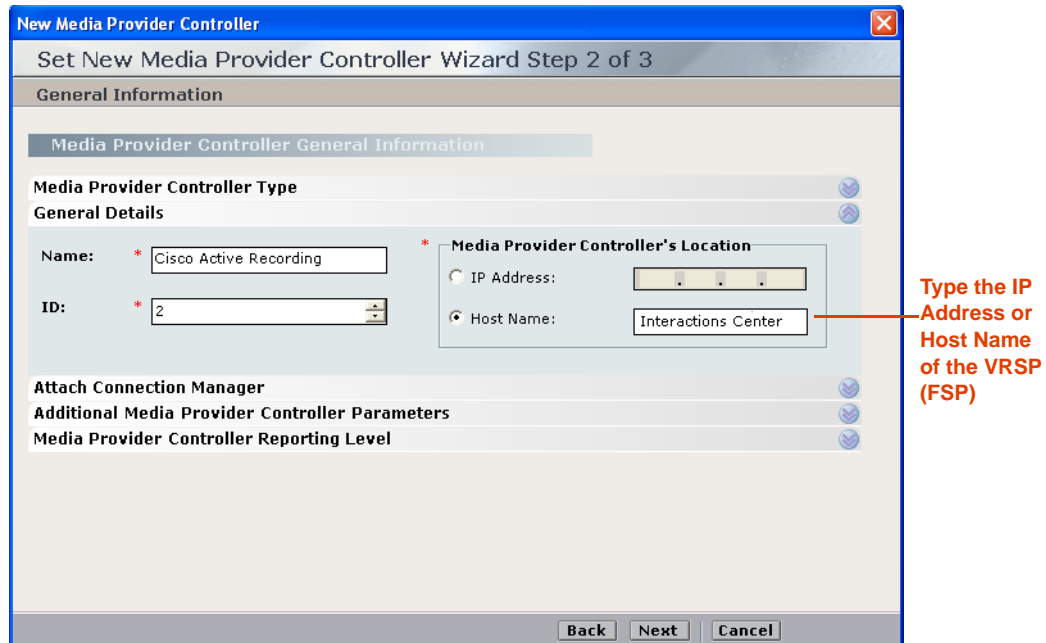
5. Click **Next**. The Set New Media Provider Controller Wizard Step 2 of 3 window appears displaying the **Media Provider Controller Type** area.

Figure 6-44 Media Provider Controller Type Area



6. Expand **General Details**. The **General Details** area appears.

Figure 6-45 General Details Area



- a. In the **ID** field, type a unique number.

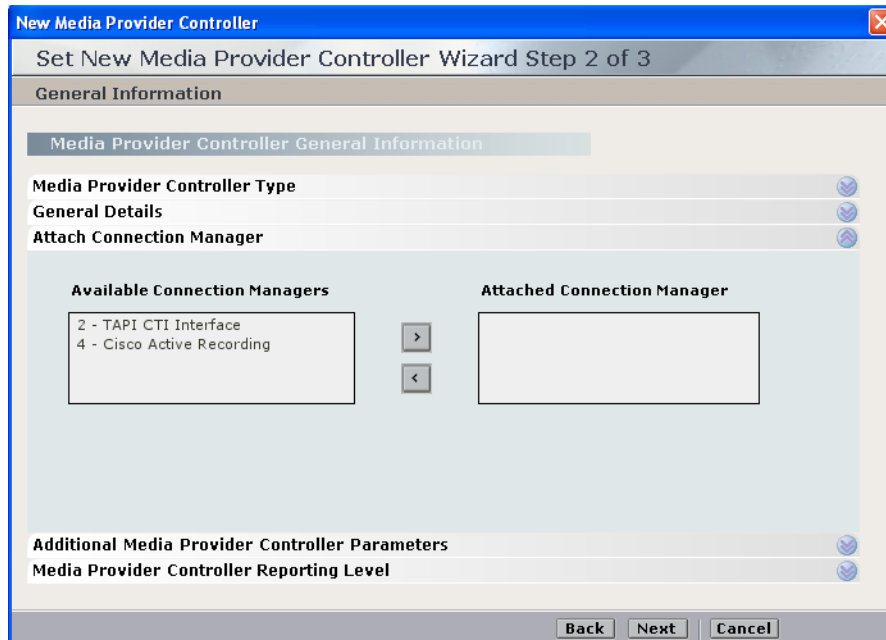
- b. Under **Media Provider Controller's Location**, select **Host Name** and type the IP address of the VRSP (FSP).



NOTE: The IP address shown in the figure is only an example of the VRSP (FSP) IP address.

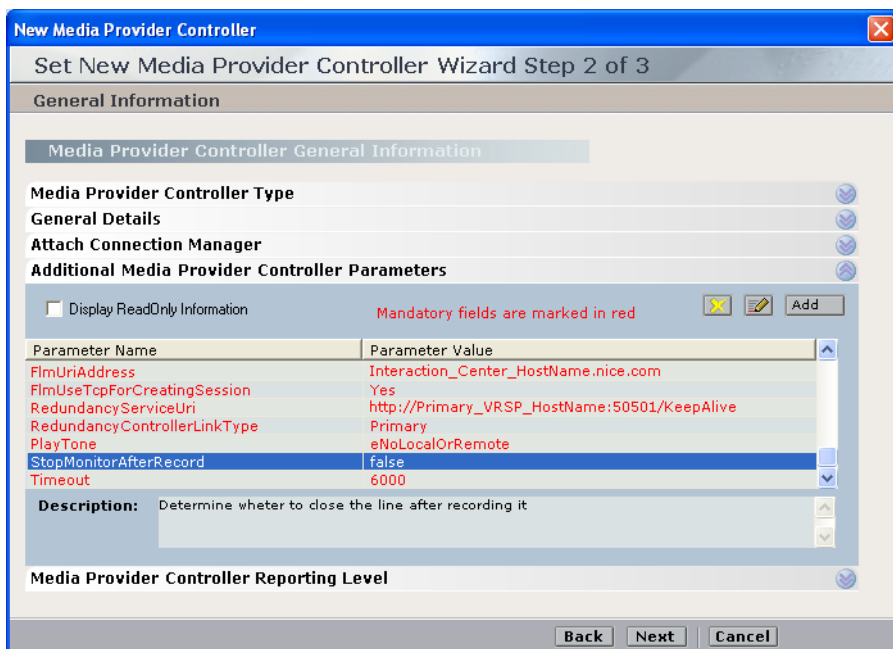
- 7. Expand **Attach Connection Manager**. The **Attach Connection Manager** area appears.

Figure 6-46 Attach Connection Manager Area



- a. Select the second Connection Manager that you created in **Configuring a Connection Manager for the VRSP (FSP)** on **page 109** and move it from the **Available Connection Managers** list to the **Attached Connection Managers** list by clicking the right arrow.
- b. Expand the **Additional Media Provider Controller Parameters**.

Figure 6-47 Additional Media Provider Controller Parameters Area

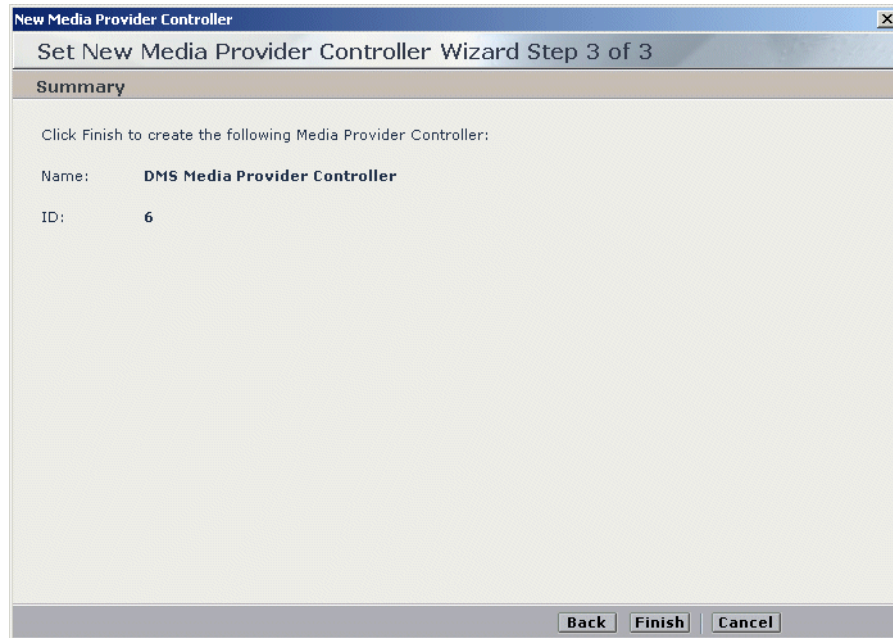


c. Define the following parameters:

Parameter Name	Parameter Value
SipStackUdpPort	Set the port number to 5062 to match the SIP Trunk port that was defined in the CUCM.
SipStackTcpPort	Set the port number to 5062 to match the SIP Trunk port that was defined in the CUCM.
FlmPort	Set the port number to 5060 .
FlmUriAddress	MPCM (FLM) URI Address: If in a domain: Hostname.Domain If the MPCM (FLM) is not in the domain, use an IP Address.
FlmUseTcpForCreatingSession	Yes.
PlayTone	eNoLocalOrRemote* *Beep tones in Interaction-based recording
StopMonitorAfterRecord	false

- d. To define VRSP (FSP) for redundancy, see **VRSP (FSP) Redundancy** on [page 134](#).
- e. Click **Next**. The Set New Media Provider Controller Wizard Step 3 of 3 window appears displaying the Summary section.

Figure 6-48 Summary Section



8. Click **Finish**.

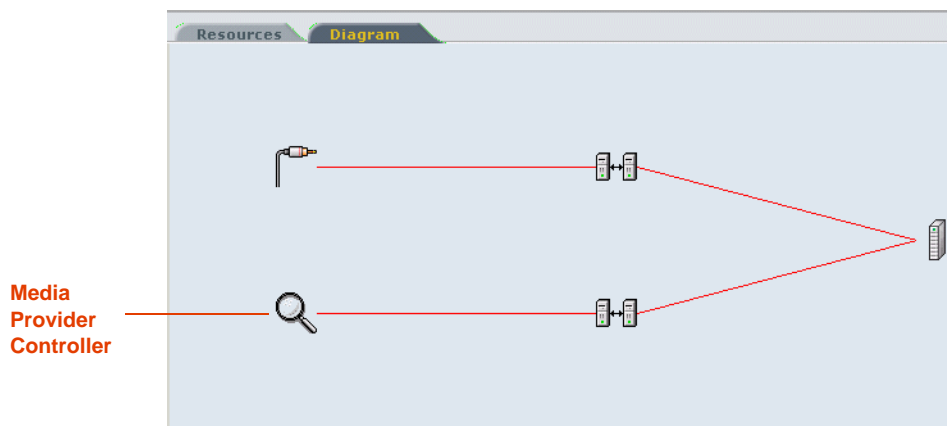
Verifying the CTI Integration

This procedure describes how to verify that all the relevant system components have been attached.

To verify the CTI integration:

- In the System Administrator, in the **Organization** tree, navigate to **CTI Integrations**.
 - a. Select **CTI Integrations**.
 - b. Click the **Diagram** tab.
 - c. Verify that the diagram appears as in **Figure 6-49**.

Figure 6-49 CTI Integrations - Diagram Tab



Installing the NICE Integration Software

After performing all the above configurations, you now install the integration software on the NICE Interactions Center server.



NOTE: It is preferable to install the integration software after performing the configuration.



IMPORTANT

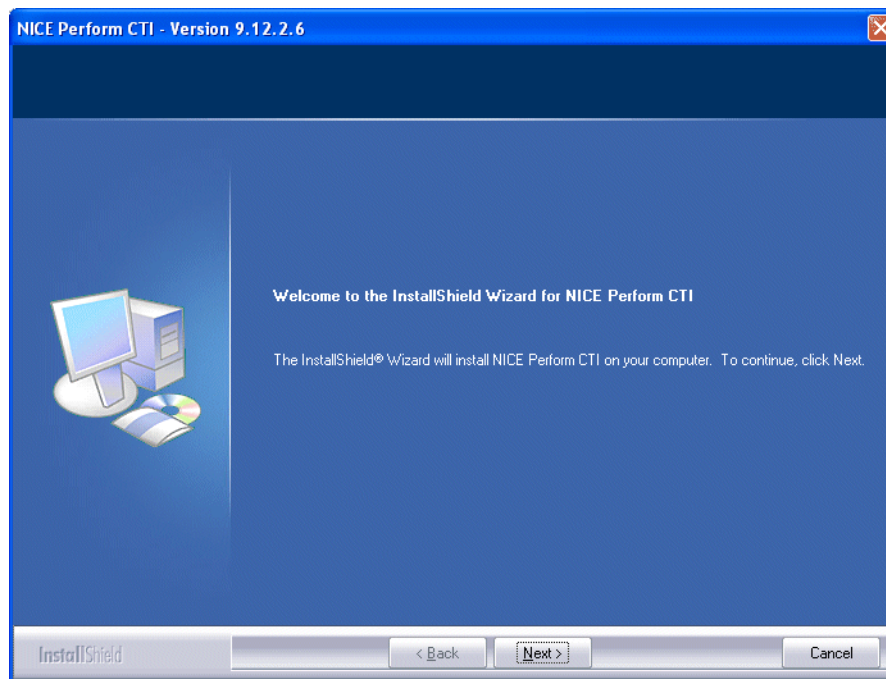
When selecting CTIManager (TAPI) in this installation, you are automatically choosing to install the VRSP (FSP).

To install the integration software:

1. Insert the **NICE Perform CTI Integration Suite Installation** CD in the CD-ROM drive.
2. Navigate to the Integration installation program and double-click **Setup.exe**.

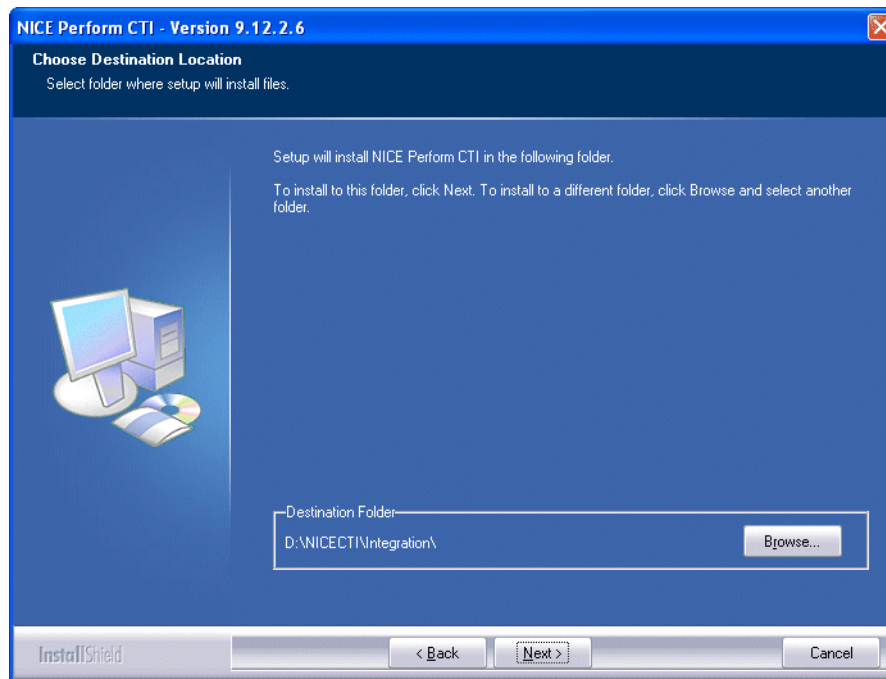
The NICE Perform CTI Wizard starts.

Figure 6-50 NICE Perform CTI - InstallShield Welcome Window



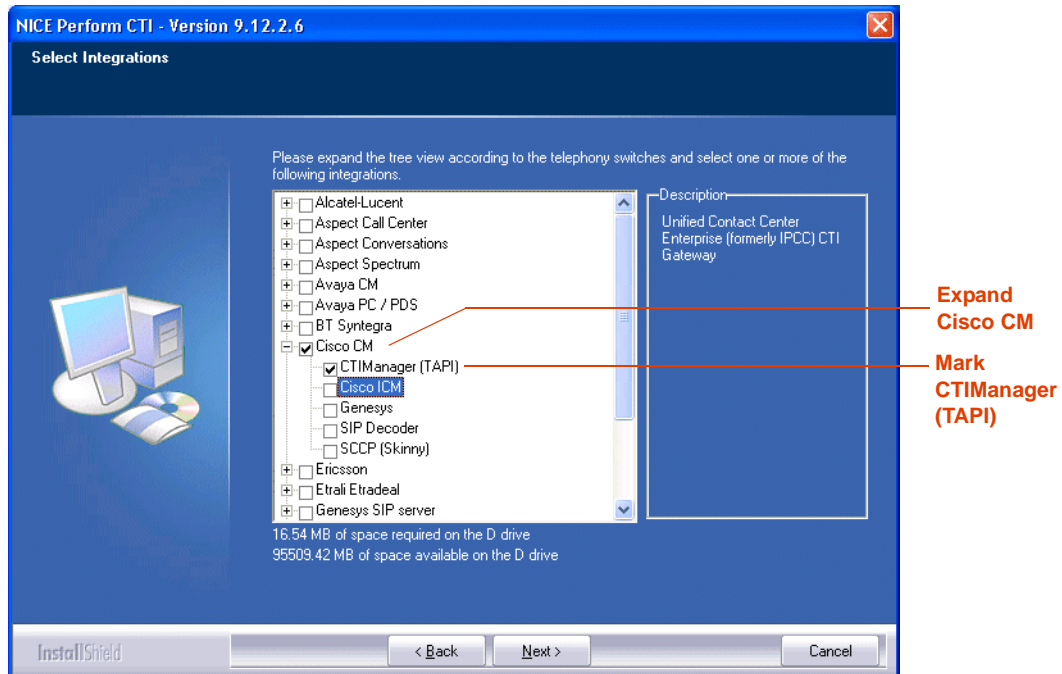
3. Click **Next**. The Choose Destination Location window appears.

Figure 6-51 Choose Destination Location Window



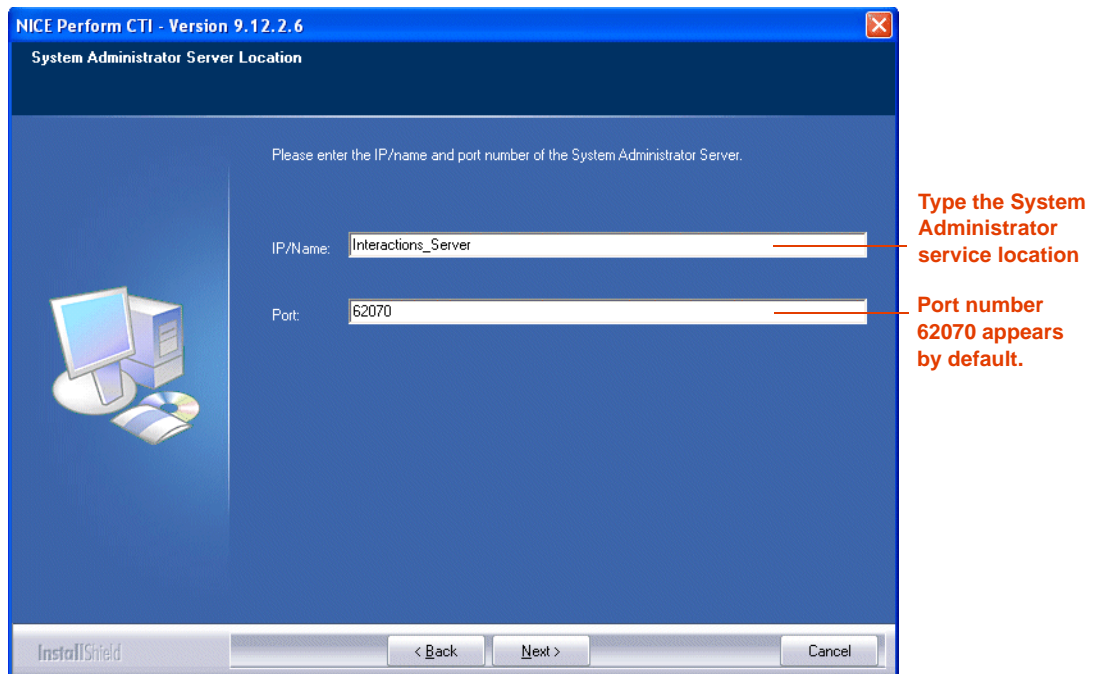
4. To change the default installation path, click **Browse** and select the required path. In the Choose Folder window, click **OK**.
5. Click **Next**. The Select Integrations window appears.
6. Select the relevant integration:
 - Expand **Cisco CM** and mark **CTIManager (TAPI)**.

Figure 6-52 Select Integrations Window



The System Administrator Server Location window appears.

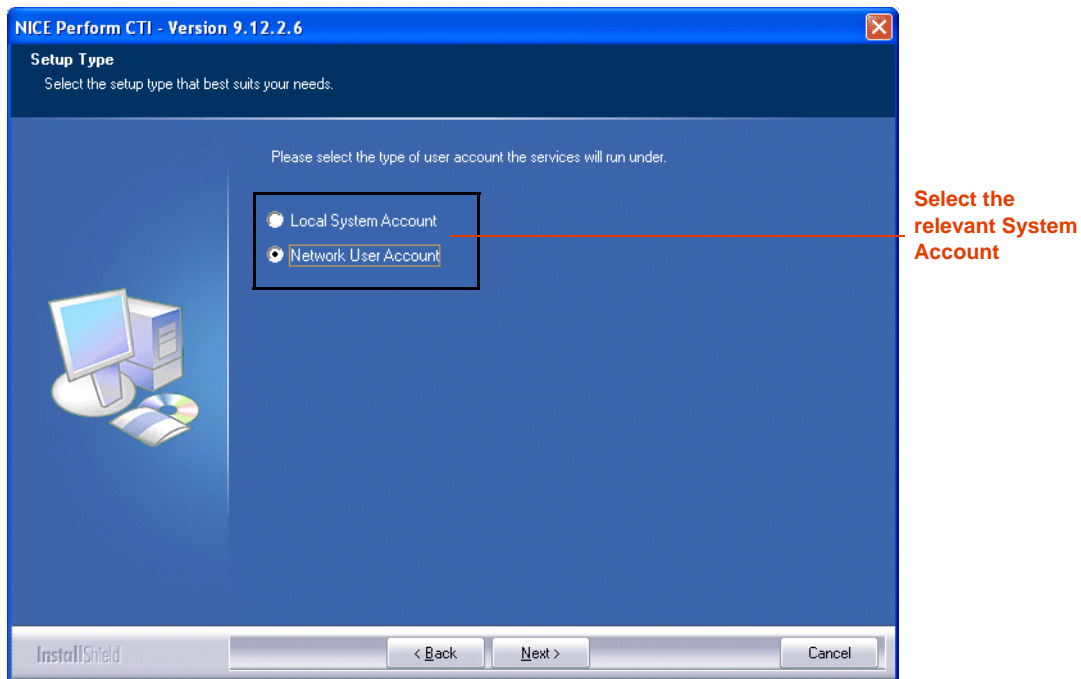
Figure 6-53 System Administrator Server Location Window



The associated **Port** number (**62070**) appears by default.

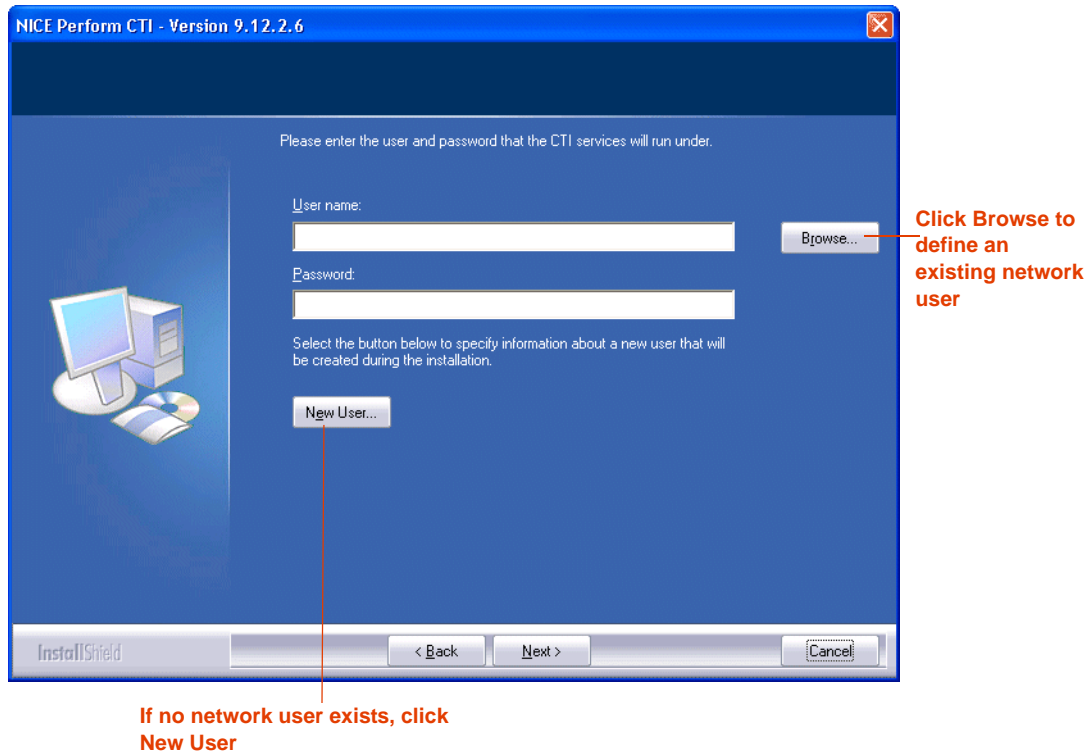
7. Type the location of the System Administrator service.
8. Click **Next**. The Setup Type window appears.

Figure 6-54 Setup Type Window



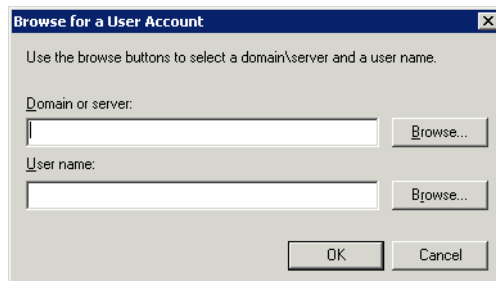
- a. *If your site is configured for a network user account, leave the default setting.*
-or-
*If you need to configure for a local system account, select **Local System Account**.*
Continue with **Step 11**.
- b. Click **Next**. The Network User Account Setup window appears.

Figure 6-55 Network User Account Setup Window



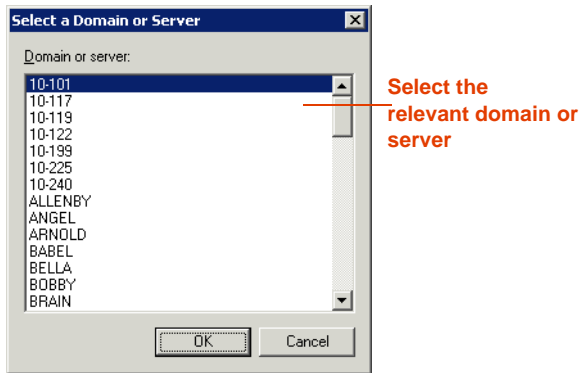
- To define an existing network user, continue with **Step 9**.
 - If no user exists or to add an additional new user, continue with **Step 10**.
9. To define an existing network user, in the **User name** area, click **Browse**. The Browse for a User Account window appears.

Figure 6-56 Browse for a User Account Window



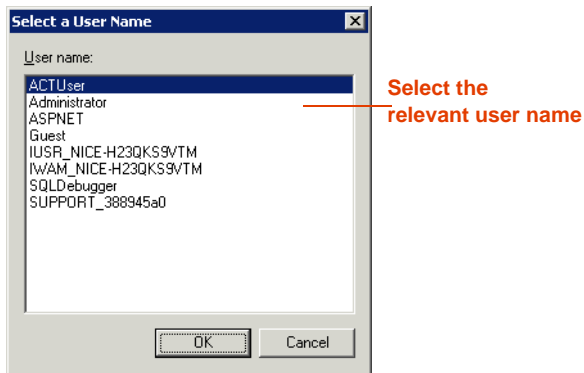
- a. In the **Domain or server** area, click **Browse**. The Select a Domain or Server window appears.

Figure 6-57 Select a Domain or Server Window



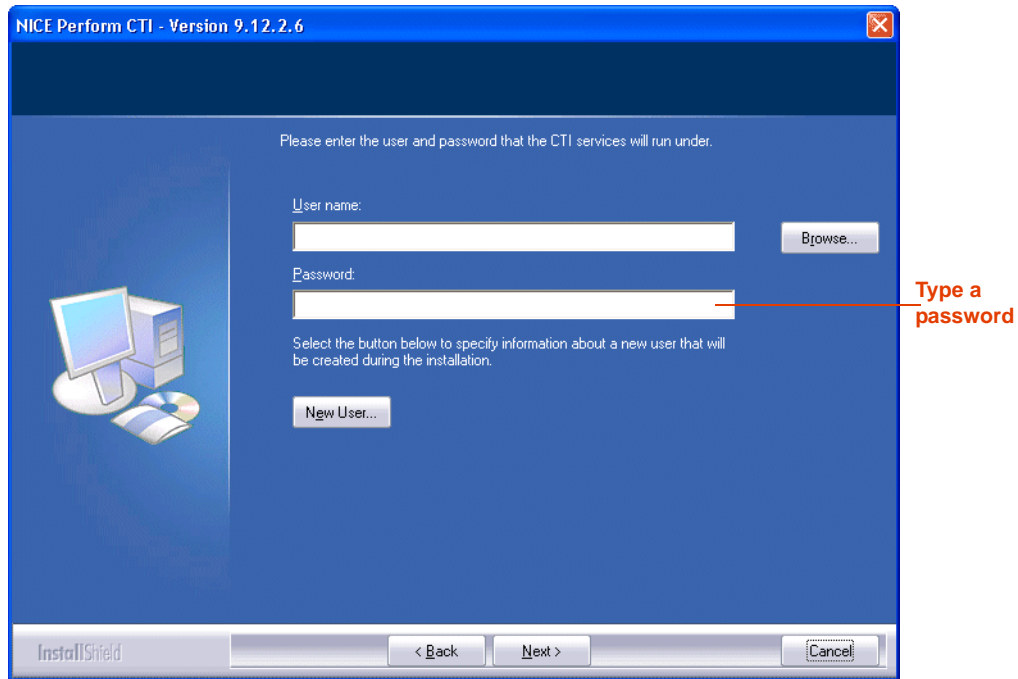
- b. Select a domain or server and click **OK**.
- c. In the Browse for a User Account window, in the **User name** area, click **Browse**. The Select a User Name window appears.

Figure 6-58 Select a User Name Window



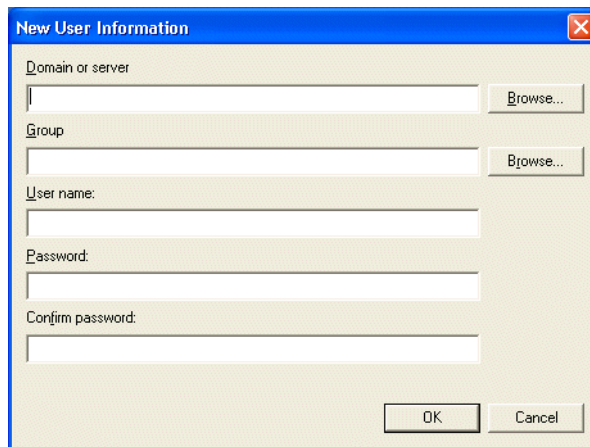
- d. Select a user name, and click **OK**. The Network User Account setup window reappears.

Figure 6-59 Network User Account Setup Window



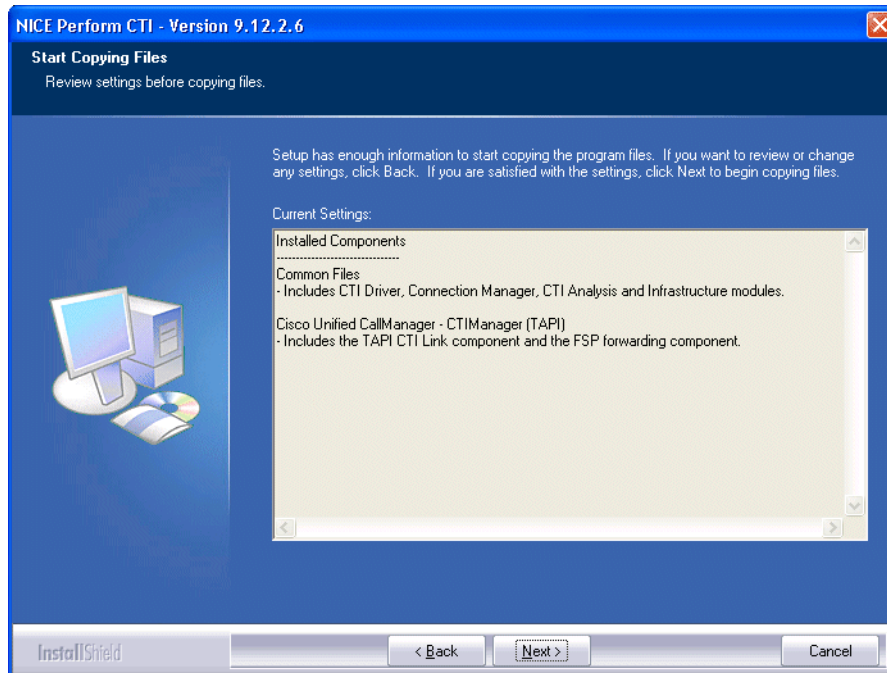
- e. In the Network User Account setup window, in the **Password** field, type the password provided by the site administrator.
- 10. If no user exists or to add an additional new user, click **New User**. The New User Information window appears.

Figure 6-60 New User Information Window



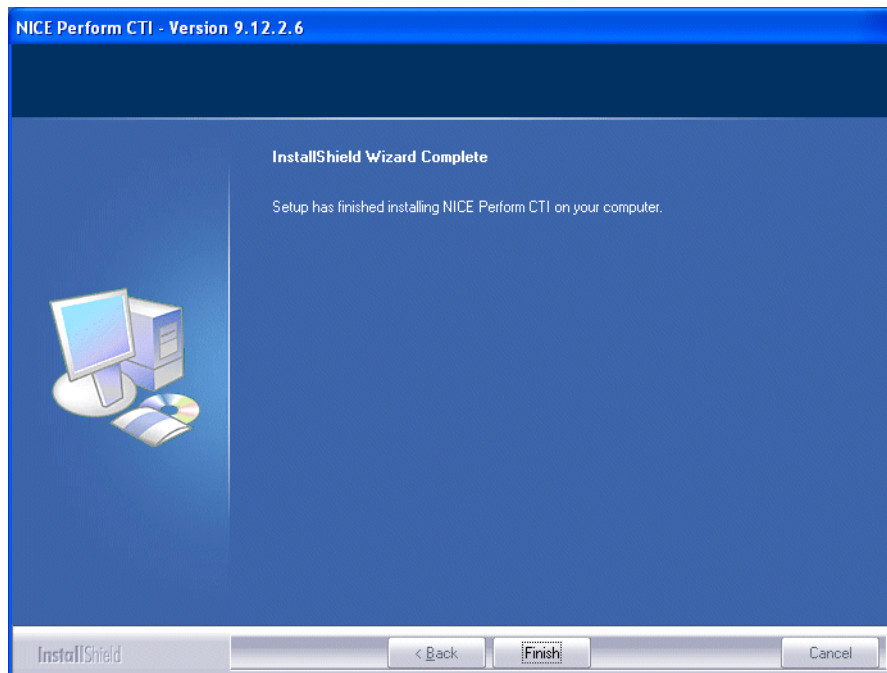
- Complete all fields and click **OK**.
- 11. Click **Next**. The Start Copying Files window appears.

Figure 6-61 Start Copying Files Window



12. Click **Next**. The InstallShield Wizard Complete window appears.

Figure 6-62 InstallShield Wizard Complete Window



13. Click **Finish**. The Integration package is installed.

Blank page for double-sided printing.

Using Redundancy

Cisco's IP Phone-based Active Recording solution can employ both N+1 and VRSP (FSP) redundancy.

Contents

Overview	132
Redundancy Workflow	133
VRSP (FSP) Redundancy	134
VRSP (FSP) Requirements.....	134
Configuring VRSP (FSP) for Redundancy	135

Overview

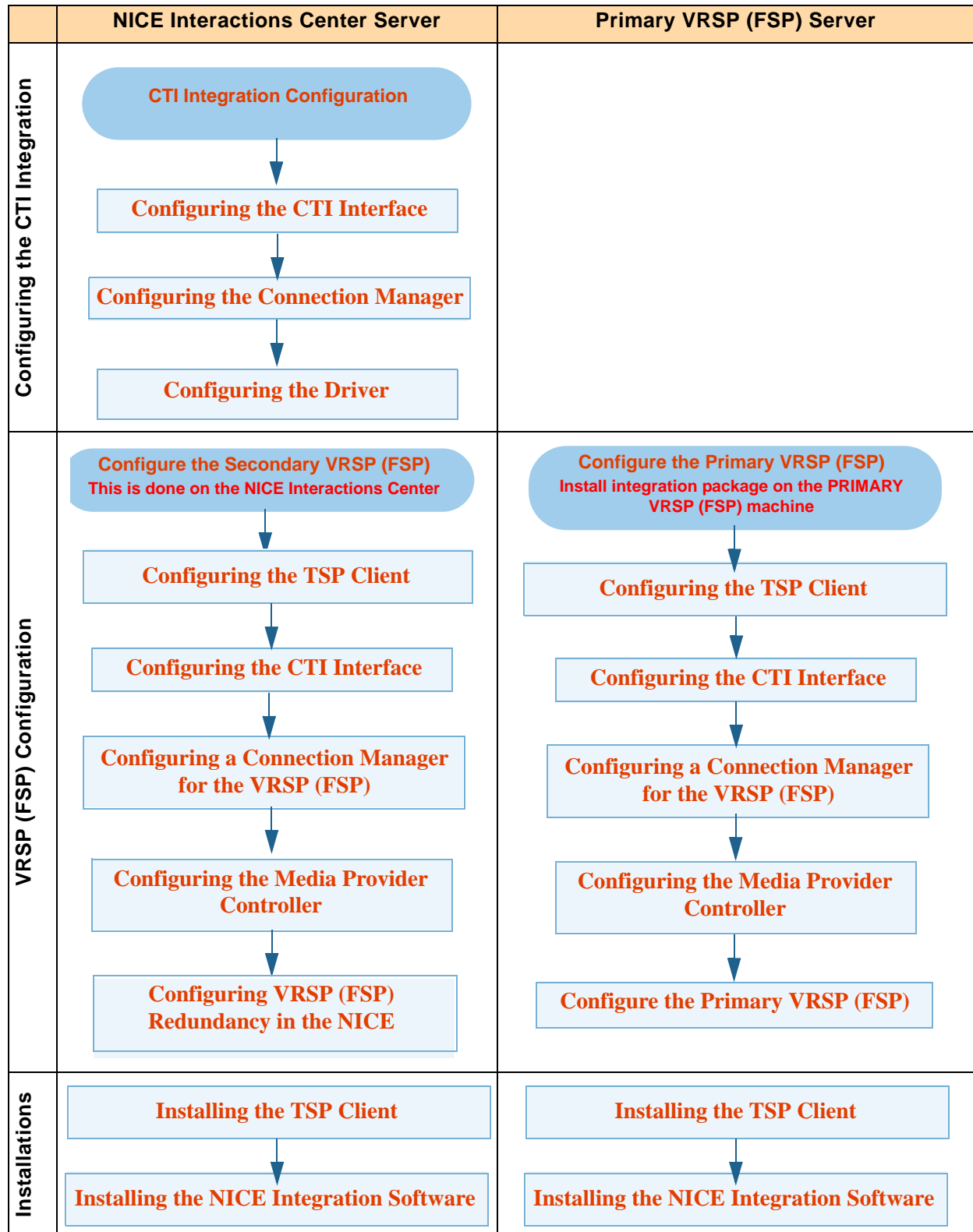
N+1 and VRSP Redundancy is only relevant for Total recording solutions. For detailed information, regarding the:

- VoIP Logger N+1, see the *NICE Perform Release 3 System Administrator's Guide*
- VRSP redundancy, see **VRSP (FSP) Redundancy** on **page 134**



NOTE: There is no redundancy for the MPCM (FLM).

Redundancy Workflow



VRSP (FSP) Redundancy

Figure 7-1 VRSP (FSP) Redundancy



The VRSP (FSP) is crucial for recording purposes. It is vital that it continues to function even when the NICE Interactions Center and/or the MPCM (FLM) have crashed as the CUCM establishes a call with NICE at the beginning of each and every phone call via the VRSP (FSP).

Why Is It Designed With the Primary on a Separate Machine?

The design for VRSP (FSP) redundancy ensures that *real* redundancy occurs in a Total recording environment: in the event that the dedicated server with the primary VRSP (FSP) crashes, the redundant VRSP on the Interactions Center takes its place. In the event that the Interactions Center crashes completely, the primary VRSP (FSP) stays alive and continues recording together with the VoIP Logger.

How does it function?

The VRSP (FSP) functions in the following way:

1. During system startup, both VRSPs (FSPs) acquire the TAPI extensions. The redundant VRSP (FSP) is always on but not active.
2. KeepAlive messages (in HTTP format) are sent between the primary and redundant VRSPs (FSPs) to inform the redundant VRSP (FSP) when the primary VRSP (FSP) has crashed or gone down. This is very important as the redundancy VRSP (FSP) needs to report its media sources to the MPCM.
3. When the primary VRSP (FSP) fails, the CUCM establishes the phone calls with the redundant VRSP (FSP).

VRSP (FSP) Requirements

VRSP (FSP) redundancy requires the following:

- The Primary VRSP (FSP) is installed on a separate machine.



NOTE: It should not be installed on the NICE Interactions Center or on any of the VoIP Loggers.

- The redundant VRSP (FSP) is installed on the NICE Interactions Center.
- A VRSP (FSP) (both primary and redundant) are defined in the NICE Perform System Administrator.
- Two (and no more than two) VRSP (FSP) servers are installed in the site

Configuring VRSP (FSP) for Redundancy

Configure the VRSP (FSP) for redundancy by following the procedures below:

- [Configuring VRSP \(FSP\) Redundancy in the Cisco Environment](#)
- [Configuring VRSP \(FSP\) Redundancy in the NICE Environment](#)

Configuring VRSP (FSP) Redundancy in the Cisco Environment

To configure VRSP (FSP) redundancy:

1. In the CUCM, perform the following steps:
 - a. Configure an additional SIP Trunk to the Route Group, see [Defining a Route Group](#) on [page 40](#).
 - b. In the **SIP Information** area, in the **Destination Address** field type the IP Address of the redundant VRSP.

Figure 7-2 SIP Information Area

SIP Information	
Destination Address*	192.168.241.100
<input type="checkbox"/> Destination Address is an SRV	
Destination Port*	5062
MTP Preferred Originating Codec*	711ulaw
Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
DTMF Signaling Method*	No Preference

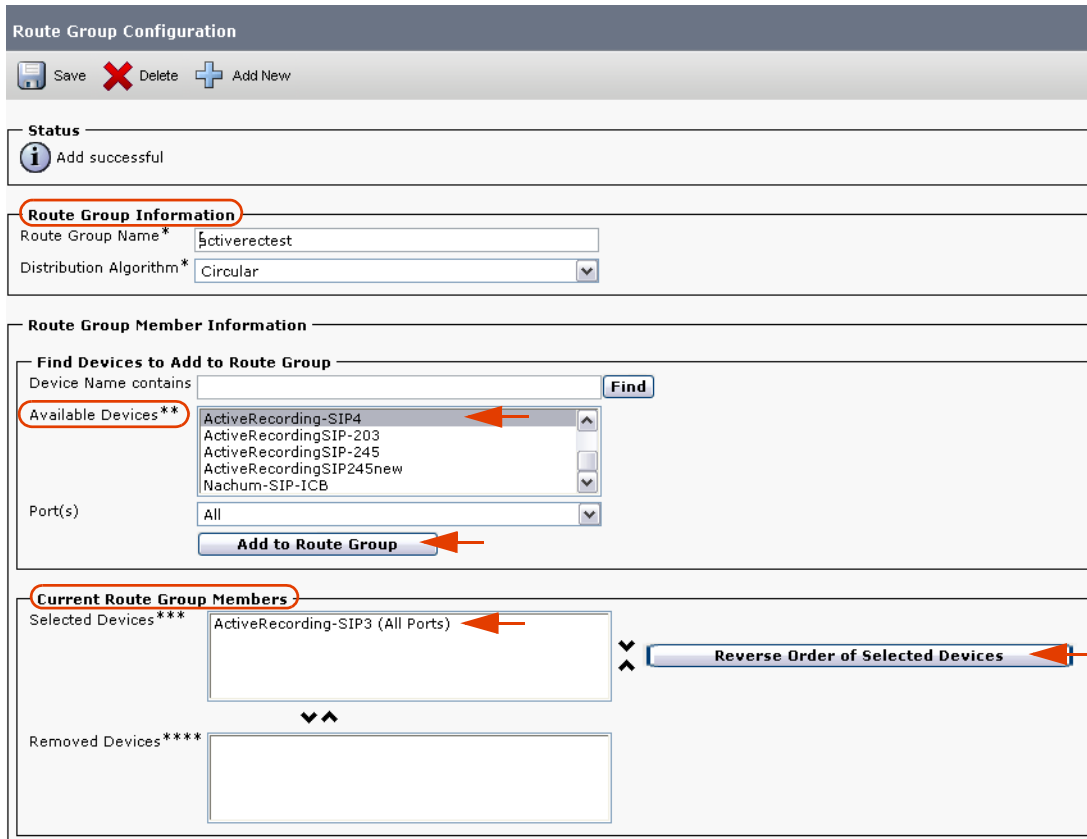
Save

Redundant VRSP IP Address

Use this number to configure the SIP Port

- c. Add this SIP Trunk to the Route Group.

Figure 7-3 Route Group Configuration Window



- d. In the **Find Devices to Add to Route Group** area, in the **Available Devices** list, choose the SIP trunk that you created in **Defining a SIP Trunk** on page 35.



NOTE: If using VRSP (FSP) redundancy, you need to select the two SIP Trunks that point to the primary VRSP (FSP) and redundant VRSP (FSP), see **Defining a SIP Trunk** on page 35.

- e. Click **Add to Route Group**. The selected IP trunk appears in the **Selected Devices** area.



NOTE: In VRSP (FSP) redundancy, both IP trunks appear in the **Selected Devices** area.

- f. In the **Current Route Group Members** area, in the **Selected Devices** list, you can change the order of the SIP trunks. Make sure that the SIP Trunk that points to the primary VRSP (FSP) will appear first in the list.

Configuring VRSP (FSP) Redundancy in the NICE Environment

Installing the NICE Integration Software on the Primary VRSP (FSP)

After performing all the above configurations, you now install the integration software on the primary VRSP (FSP).



NOTE: It is preferable to install the integration software now and NOT before the configuration.

Configure the Primary VRSP (FSP)

Perform the following procedure to configure the primary

To configure the primary VRSP (FSP):

1. See **Configuring the Media Provider Controller** on **page 114**.
2. In the **Media Provider Controller** branch, click the **Primary VRSP**:
3. Expand the **Additional Media Provider Controller Parameters**. The Additional Media Provider Controller Parameters area appears.

Figure 7-4 Additional Media Provider Controller Parameters Area - Primary VRSP

Parameter Name	Parameter Value
FilmUriAddress	Interaction_Center_HostName.nice.com
FilmUseTopForCreatingSession	Yes
RedundancyServiceUri	http://Primary_VRSP_HostName:50501/KeepAlive
RedundancyControllerLinkType	Primary
PlayTone	eNoLocalOrRemote
StopMonitorAfterRecord	false
Timeout	6000

Description: Determine wheter to close the line after recording it

- Verify that the following parameters have been defined:

Parameter Name	Parameter Value
RedundancyServiceUri	VRSP (FSP) address e.g. http://Primary VRSP IP Address:50501/KeepAlive
RedundancyControllerLinkType	Primary

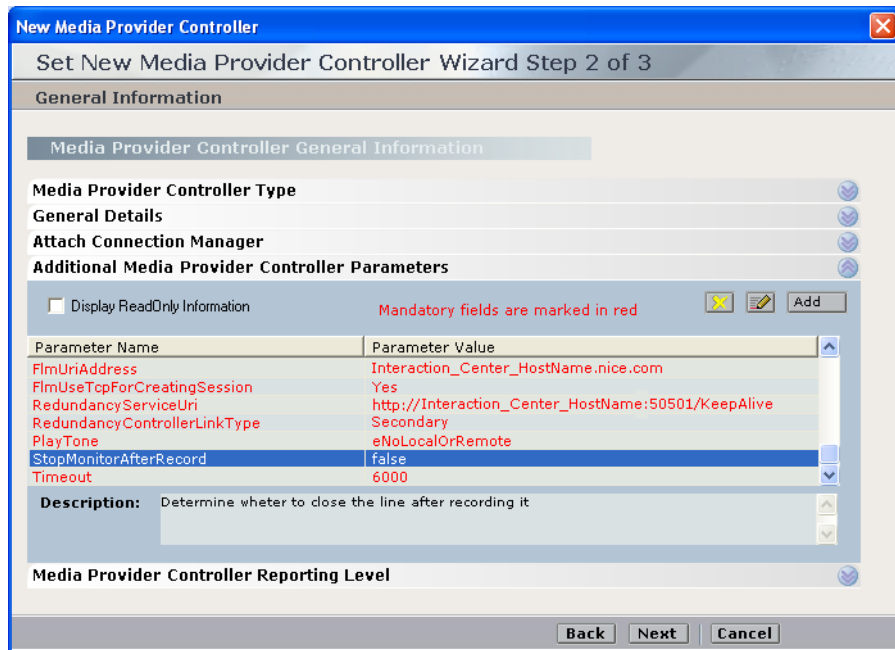
- Click **Next**.
- Click **Finish**.

Configure the Redundant VRSP (FSP) on the NICE Integrations Center

In the NICE System Administrator:

- a. In the **Media Provider Controller** branch, click the **Redundant VRSP**.
- b. Expand the **Additional Media Provider Controller Parameters**. The Additional Media Provider Controller Parameters area appears.

Figure 7-5 Additional Media Provider Controller Parameters Area - Redundant VRSP



- c. Verify that the following parameters have been defined:

Parameter Name	Parameter Value
RedundancyServiceUri	Primary VRSP (FSP) address e.g. http://Primary VRSP IP Address:50501/KeepAlive
RedundancyControllerLinkType	Secondary

- d. Click **Next**.
- e. Click **Finish**.

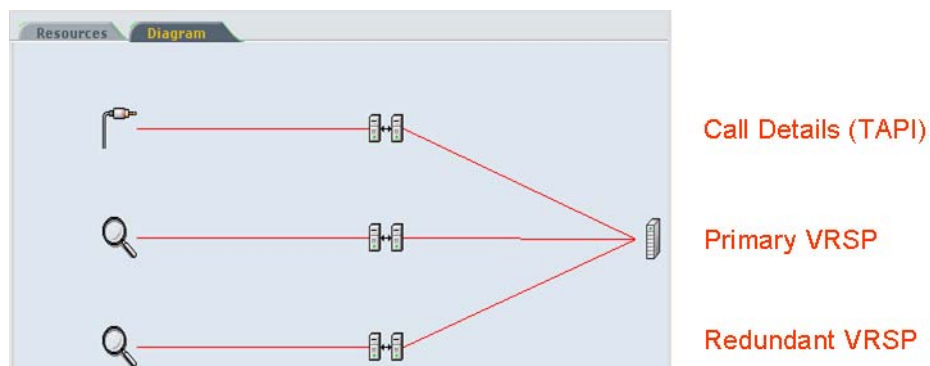
Verifying the Redundancy Integration

This procedure describes how to verify that all the relevant system components have been attached.

To verify the Redundancy integration:

- In the System Administrator, in the **Organization** tree, navigate to **CTI Integrations**.
 - a. Select **CTI Integrations**.
 - b. Click the **Diagram** tab.
 - c. Verify that the diagram appears as in **Figure 7-6**.

Figure 7-6 Redundancy Integration - Diagram Tab



NICE Testing and Debugging Tools

This chapter describes several NICE testing and debugging tools which enable you to troubleshoot your site. Use the different tools to help you isolate problems.



NOTE: All these tools should *only* be used by authorized personnel and in conjunction with NICE Customer Support.

Contents

NICE Events Spy	142
NICE Debug Service	147
Connection Manager Monitor	153
Log Manager System	159
CAPI Spy.....	166
TAPIMonitor.....	171

NICE Events Spy

NICE Events Spy enables you to trace events after they were transferred from the PABX to the Connection Manager, enabling you to detect bugs or malfunctions.

WARNING

Using the NICE Events Spy can greatly increase the load on your system. The **UseSpy** parameter default is therefore **No**. Using the NICE Events Spy and changing the parameters should be performed only by authorized personnel and in conjunction with NICE Customer Support.

This section includes:

- [Setting Up the Events Spy](#)
- [Receiving Events](#)
- [Saving Events](#)
- [Setting up the SimCTILink Tool](#)

Setting Up the Events Spy

The NICE Events Spy tool is part of the NICE Perform Applications Suite.

To set up the NICE Events Spy Tool:

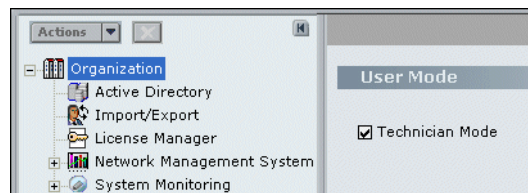
1. Open the System Administrator, as follows:
 - a. Log in to the NICE Perform Applications Suite.
 - b. From the **Accessories** menu, choose **System Administrator**.



The System Administrator appears with a list of NICE components under the **Site** branch in the **Organization** tree.

To add components in the System Administrator, you must work in Technician Mode.

2. Set the System Administrator to Technician Mode:
 - a. In the Organization Tree, select the **Organization** branch.




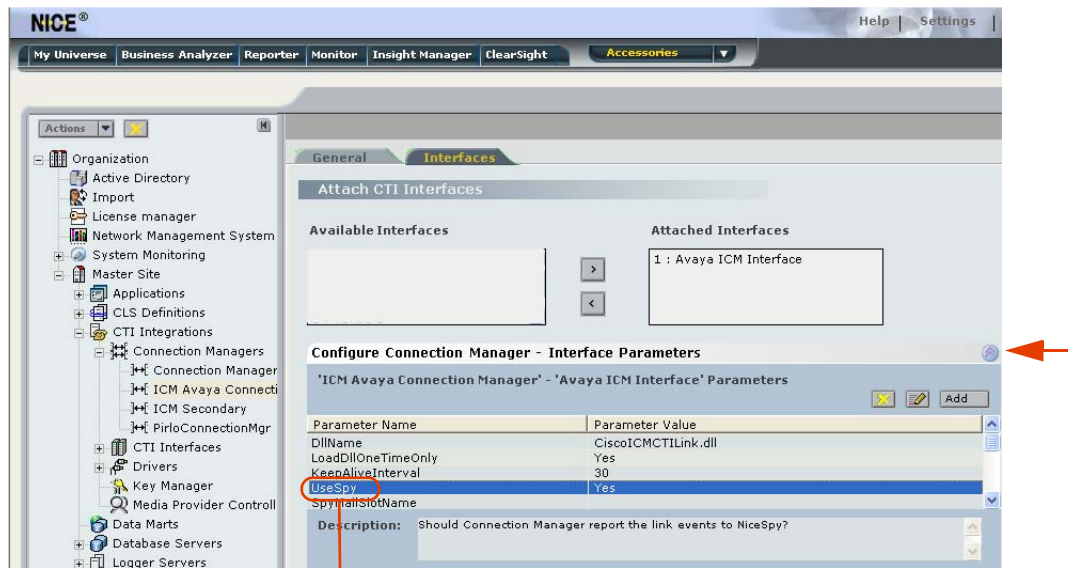
- b. Mark the **Technician Mode** checkbox and click **Save** .
3. In the **Organization** tree, navigate to **Master Site > CTI Integrations > Connection Managers**. Choose the Connection Manager for which you want to set up the NICE Events Spy tool.
4. Click the **Interfaces** tab and expand **Configure Connection Manager - Interface Parameters**.

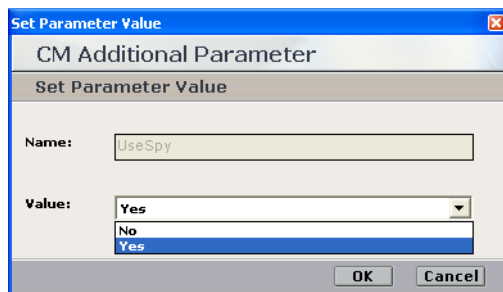
Figure 8-1 Interfaces Tab



Double-click UseSpy

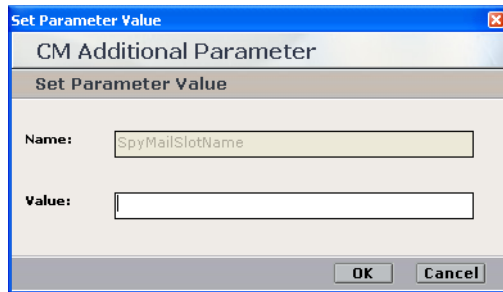
5. Double-click the **UseSpy** parameter. The Set Parameter Value window appears.

Figure 8-2 Set Parameter Value Window



6. From the **Value** drop-down list, choose **Yes** and click **OK**.
7. Double-click the **SpyMailSlot Name** parameter. The Set Parameter Value window appears.

Figure 8-3 Set Parameter Value Window



- In the **Value** field, type the name of the mailslot that you want to use in conjunction with NICE Events Spy.



TIP: It is recommended to use a short name.

- Click **OK**.



NOTE: If the Connection Manager is running, you should restart it after setting these definitions.

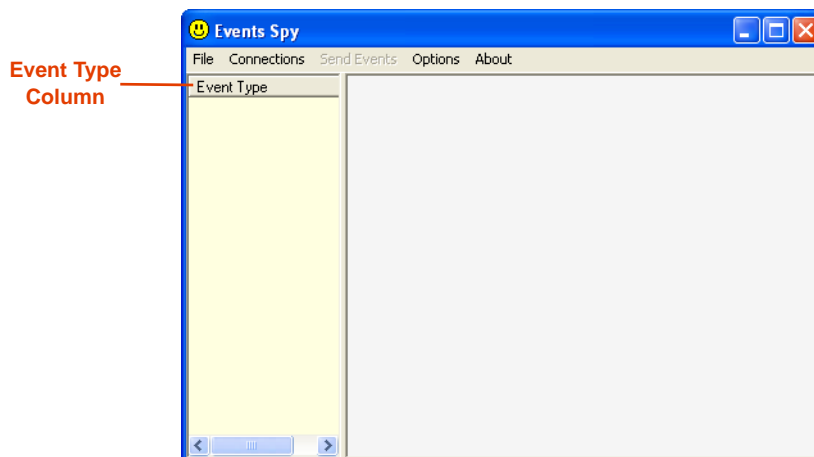
Receiving Events

You should set up the Events Spy so that you can receive events.

To use NICE Events Spy:

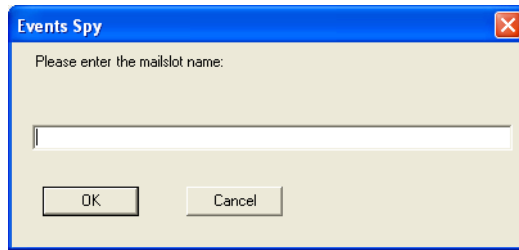
- On the Interaction Center server, navigate to the **Integrations** folder (the default location is **D:\NICECT\Integrations**). Double-click **EventSpy.exe**. The Events Spy window appears.

Figure 8-4 Events Spy Window



- From the **Connections** menu, choose **Mailslot Connections for Receiving Events > Open Mailslot**. The Events Spy - Mailslot Name window appears.

Figure 8-5 Events Spy - Mailslot Name Window



3. Type the name of the mailslot you defined in setting up the NICE Events Spy tool. Click **OK**. The Events Spy begins to receive events from the switch. The events are listed in the **Event Type** column of the Events Spy window, see **Figure 8-4**.

Saving Events

NICE Events Spy enables you to:

- Create and save events in an active log file.
- Save all current events.
- Save selected current events.

You can save the files in either **.xml** or **.bin** formats.

Saving Events in a Log File

This option enables you to create a log file that saves all events from the time you create the file until you close it.

To save events in a log file:

1. From the **File** menu, choose **Log to File**.
2. To create a log file using the **.xml** format, click **Log to XML File**. To create a log file using the **.bin** format, click **Log to Binary File**. The Save as window appears.
3. Save the file in any convenient location.



NOTE: To view the contents of any of the log files you created, from the **File** menu click **Open Log File**.

Saving Current Events

This option enables you to create a file in which you can save all events that currently appear in the **Event Type** column.

To save current events:

1. From the **File** menu, choose **Save Current Events to File**.

2. To create a file using the **.bin** format, click **Save all Events to Binary File**. To create a file using the **.xml** format, click **Save all Events to XML File**. The Save as window appears.
3. Save the file in any convenient location.

Saving Selected Current Events

This option enables you to create a file in which you can save selected events from the list that currently appears in the **Event Type** column.

To save selected current events:

1. Select the events you want to save, clicking the events while holding down the **<Ctrl>** key.
2. From the **File** menu, choose **Log to File**.
3. To create a file using the **.bin** format, click **Save Only Selected Events to Binary File**. To create a file using the **.xml** format, click **Save Only Selected Events to XML File**. The Save as window appears.
4. Save the file in any convenient location.

Setting up the SimCTILink Tool

The SimCTILink tool simulates the transfer of events to the Connection Manager as if they originated in the PABX. This enables you to save and analyze them without having to actually use the PABX itself.

WARNING

Use of the SimCTILink tool must be coordinated in advance with NICE Systems and must be performed only by authorized personnel. **DO NOT** attempt to use this tool on your own.

You must therefore leave the parameter default value as **No** unless specifically instructed to do so by NICE Customer Support.

Sending Events

WARNING

You can send events to NICE Systems using the Events Spy window. Sending events is only done when using the SimCTILink tool, and must be coordinated in advance with NICE Customer Support.

NICE Debug Service

The Debug Service enables you to gather data critical for solving problems stemming from the transfer of events between the switch and the Connection Manager.



IMPORTANT

Do not attempt to solve bugs or other problems yourself. Use the Debug Service in coordination with NICE Systems to gather the data as described below, and then send it to NICE Customer Support for assistance.

This section includes the following topics:

- Setting Up the NICE Debug Service
- Accessing the NICE Debug Service

Setting Up the NICE Debug Service

The Debug Service enables developers and customer support personnel to reproduce problematic scenarios.

WARNING

Using the Debug Service can greatly increase the load on your system. The `DebugServiceMode` parameter default is therefore **Idle**. Using the Debug Service and changing the parameters should be performed only by authorized personnel and in conjunction with NICE Customer Support.

To set up the Debug Service:

1. Open the System Administrator, as follows:
 - a. Log in to the NICE Perform Applications Suite.
 - b. From the **Accessories** menu, choose **System Administrator**.

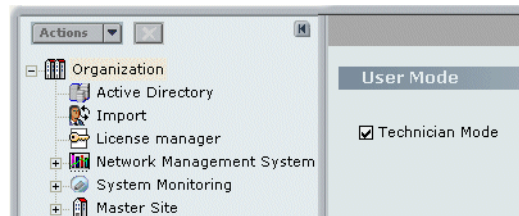


The System Administrator appears with a list of NICE components under the **Site** branch in the **Organization** tree.

To add components in the System Administrator, you must work in Technician Mode.

2. Set the System Administrator to Technician Mode:

- a. In the Organization Tree, select the **Organization** branch.




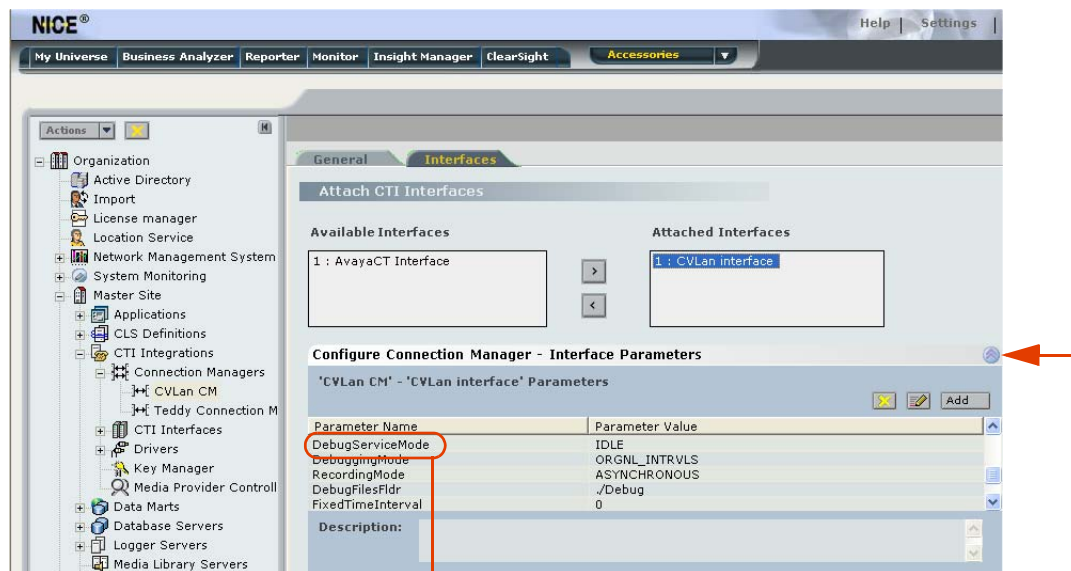
- b. Mark the **Technician Mode** checkbox and click **Save** .
3. In the **Organization** tree, navigate to **Master Site > CTI Integrations > Connection Managers**. Choose the Connection Manager for which you want to set up the Debug Service.
4. Click the **Interfaces** tab and expand **Configure Connection Manager - Interface Parameters**.

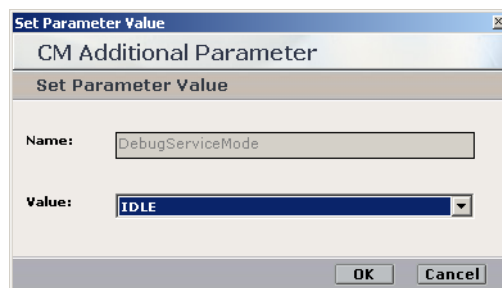
Figure 8-6 Interfaces Tab



Double-click DebugServiceMode

5. Double-click the **DebugServiceMode** parameter. The Set Parameter Value window appears.

Figure 8-7 Set Parameter Value Window



6. From the **Value** drop-down list, choose either **Record** or **Debug** (see following table) and click **OK**.
7. Define the Debug Service parameters according to the following table:



NOTE: You can also create and add additional parameters by clicking **Add**.

Table 8-1: Debug Service Parameters

Parameter Name	Description	Default Value
DebugServiceMode	<ul style="list-style-type: none"> • Idle - the Debug Service is disabled. • Record - the CTI Interface records every event, request, and response. • Debug - the CTI Interface receives events, requests, and responses directly from the Debug Service (to be used only by NICE System personnel in lab environments). 	Idle
DebuggingMode	<ul style="list-style-type: none"> • Orignl_Intrvl - retains the original intervals between events that were used by the switch. • Fixed_Intrvl - events are transferred to the link at fixed intervals, which are defined in the FixedTimeInterval parameter. • Single_Step - events are transferred upon user input. <p>NOTE: This parameter is activated only when you activate the DebugServiceMode.</p>	Single_step
RecordingMode	<ul style="list-style-type: none"> • Asynchronous - synchronization of the requests and responses by the InvokeID is defined by the switch. <i>Not applicable to TAPI.</i> • Semi_Synchronous - synchronization of the requests and responses by the InvokeID is defined by the Debug Service. <i>Not applicable to TAPI.</i> • Simple - No synchronization is performedFor TAPI, set Simple. <p>NOTE: This parameter is activated only when you activate the DebugServiceMode.</p>	Asynchronous

Table 8-1: Debug Service Parameters (Continued)

Parameter Name	Description	Default Value
DebugFilesFldr	<p>Defines the folder in which the files created by the Debug Service are saved.</p> <p>NOTE:</p> <ul style="list-style-type: none"> It is highly recommended to delete the contents of the Debug folder before activating the Debug Service. This parameter is activated only when you activate the DebugServiceMode. The files are saved in binary format. 	Debug
FixedTimeInterval	<p>Defines the value when you define Fixed_Intrvls as the value for the DebuggingMode parameter above.</p> <p>NOTE:</p> <ul style="list-style-type: none"> The value is defined in seconds. This parameter is activated only when you activate the DebugServiceMode. 	0
AvailableDiskQuota	<p>Defines the maximum size allowed on the hard disk for the Debug file you defined in the DebugFilesFldr above.</p> <ul style="list-style-type: none"> The value is defined in MB. This parameter is activated only when you activate the DebugServiceMode. 	300

- To activate the Debug Service after you have defined the above parameters, close the Connection Manager process in the Interaction Center server. The Debug Service is activated when the Dispatch Service automatically restarts the Connection Manager process.

9. The Debug Service transfers the event data to the file you defined in the **DebugFilesFldr** above.

For each debug session, the Debug Service automatically creates four debug files:

e_XXXXXXXXXX.dbg

e_XXXXXXXXXX.ndx

r_XXXXXXXXXX.dbg

r_XXXXXXXXXX.ndx

in which “XXXXXXXXXX” is the unique debug session identifier. The folder to which the above files are transferred is located in **D:\NICECTI\Integrations\Debug** (default), or in the location you defined in the **DebugFilesFldr** parameter above.



IMPORTANT

You must send all four Debug files to NICE Customer Support. If any one of the Debug files is missing, the scenario cannot be reconstructed.



NOTE: To avoid confusion with any Debug files from previous sessions, it is highly recommended to delete all existing Debug file(s) before activating the Debug Service.

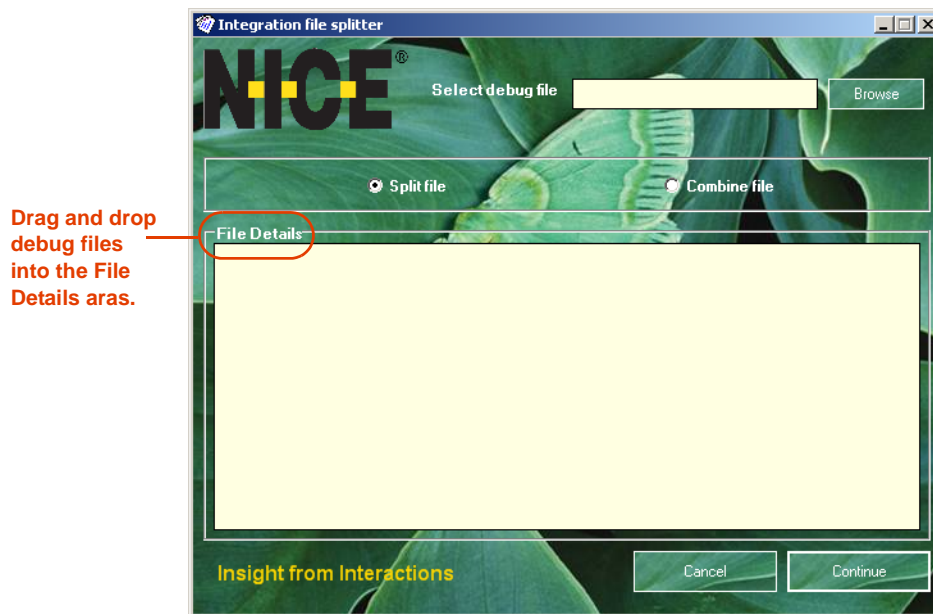
Accessing the NICE Debug Service

NICE Systems provides a utility for viewing the Debug files. You then send the four Debug files to NICE Customer Support.

To access the Debug files:

1. In the Interaction Center, navigate to the **Integrations** folder (the default location is **D:\NICECTI\Integrations**).
2. In the **Tools** folder, double-click **IntegrationFileSplitter.exe**. The Integration File Splitter window appears.

Figure 8-8 Integration File Splitter Window



3. Drag and drop the Debug files into the **File Details** area. The Debug files and the debug session identifier numbers appear in the **File Details** area.
4. When necessary, you can open and view the contents of the .dbg files.



IMPORTANT

Make sure that you send to NICE Customer Support the four debug files that correspond to the debug session ID number.

Connection Manager Monitor

The NICE Connection Manager Monitor tool enables you to view the contents of the Connection Manager's tables. It also enables you to verify if:

- Devices are monitored
- Monitored devices are filtered
and
- Displays the loaded CTI links
- Displays connected clients.

Your next step is to connect the Connection Manager Monitor tool to the Connection Manager as a client. It then receives events in addition to monitoring devices, enabling you to conduct simple tests without running a driver.

This section includes:

- [Setting Up the Connection Manager Monitor](#)
- [Managing the Connection Manager Monitor](#)

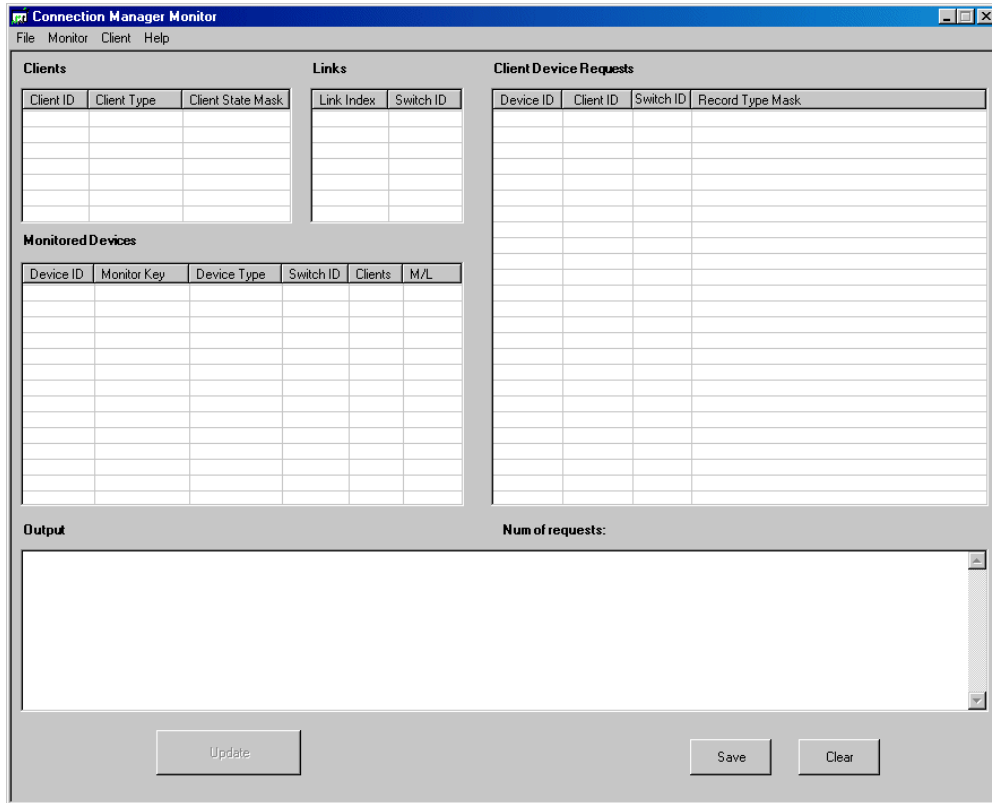
Setting Up the Connection Manager Monitor

To set up the Connection Manager Monitor, follow the procedures below.

To set up Connection Manager Monitor:

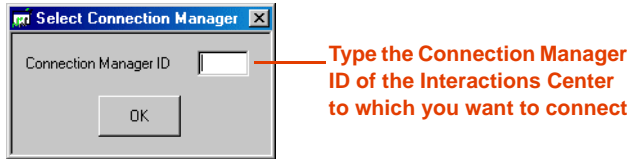
1. In the Interactions Center, navigate to the **Integrations** folder (the default location is **D:\NICECTI\Integrations**). Double-click **ConnectionManagerMonitor.exe**. The Connection Manager Monitor window appears.

Figure 8-9 Connection Manager Monitor Window



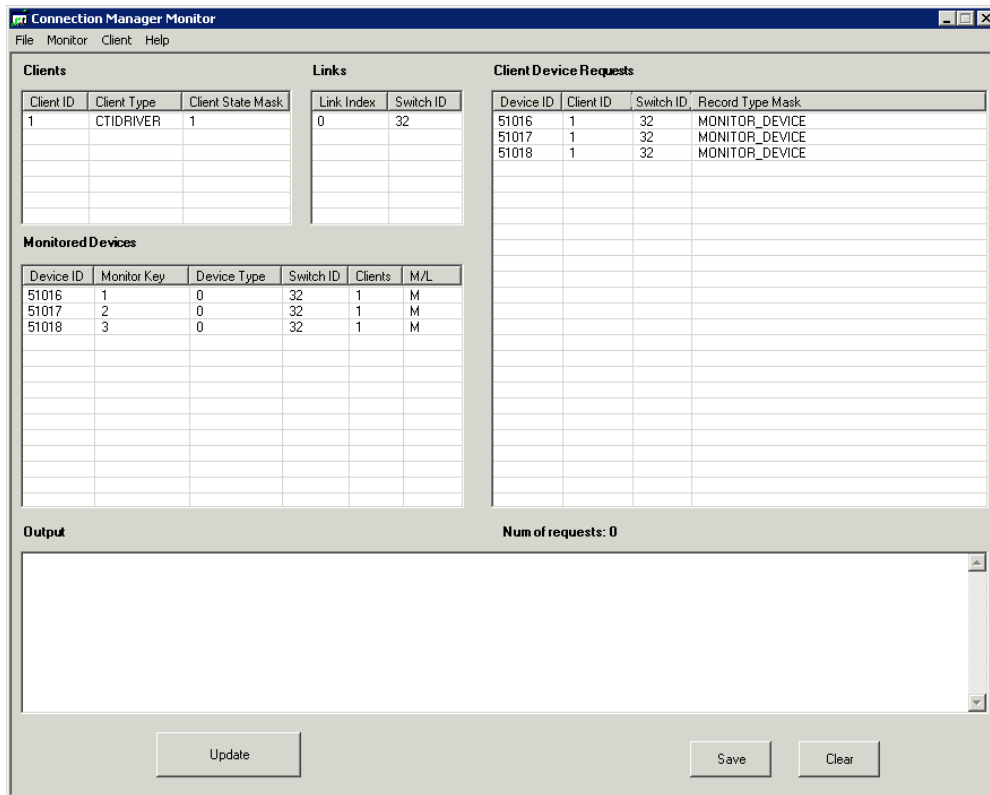
- From the **Monitor** menu, choose **Connect**. The Select Connection Manager window appears.

Figure 8-10 Select Connection Manager Window



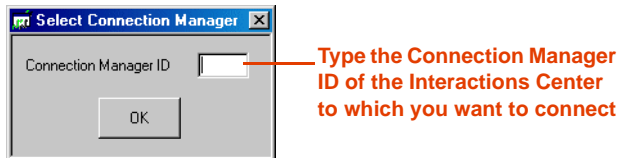
- Type the **Connection Manager ID** of the Interactions Center to which you want to connect. Click **OK**. The Connection Manager Monitor displays the contents of the Connection Manager tables.

Figure 8-11 Connection Manager Window - Tables



- From the **Client** menu of the Connection Manager Monitor window, choose **Connect**. The Select Connection Manager window appears.

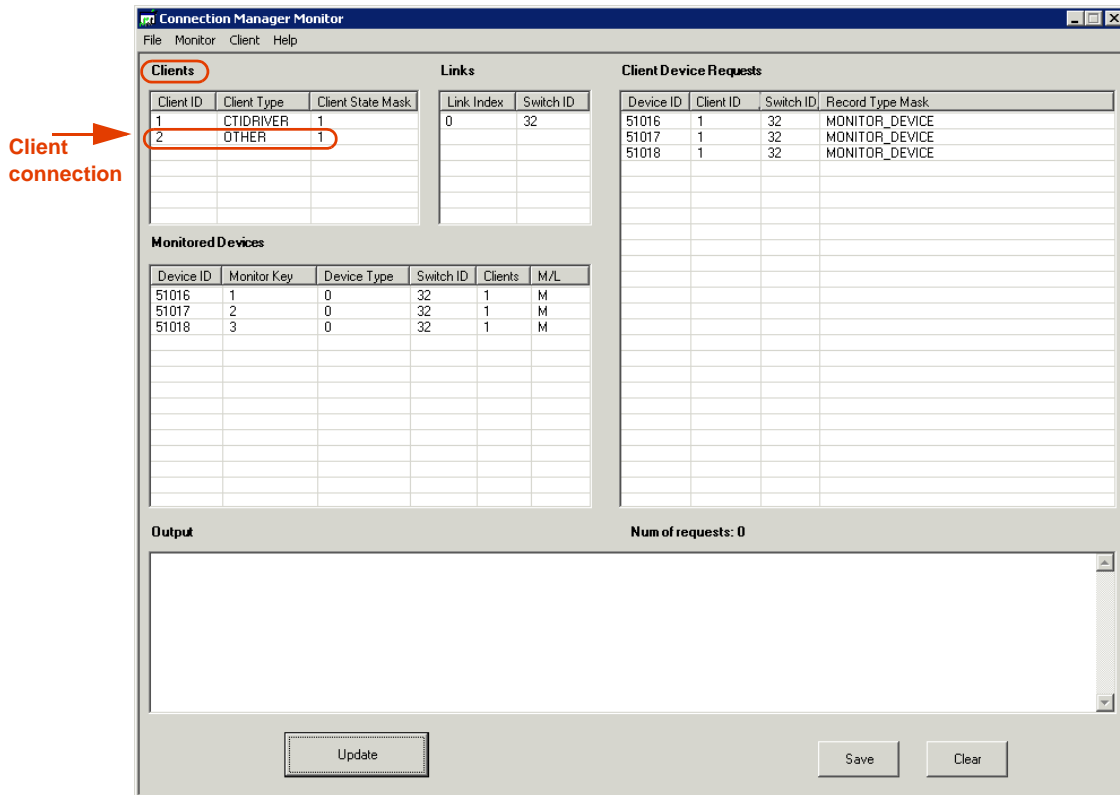
Figure 8-12 Connection Manager Window - Client Menu



- Type the **Connection Manager ID** of the Interactions Center to which you want to connect. Click **OK**.

After the Connection Manager Monitor establishes connection to the desired Connection Manager, the **Monitor**, **Stop Monitor**, and **Disconnect** options in the **Client** menu become enabled. The Client connection appears in the **Clients** area.

Figure 8-13 Connection Manager Monitor - Client Connection in Clients Area



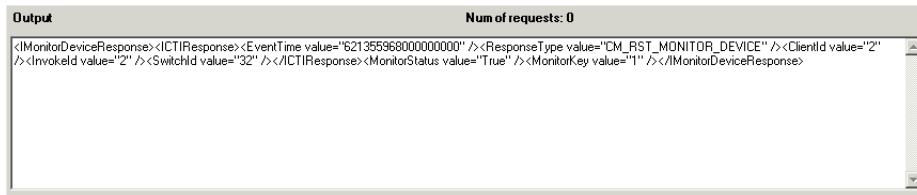
6. From the **Client** menu, choose **Monitor**. The Monitor Device window appears.

Figure 8-14 Monitor Device Window



- a. In the **Device ID** field, type the Device ID number of the Connection Manager to which you want to connect.
- b. In the **Switch ID** field, type the Switch ID number.
- c. From the **Device Type** drop-down list, choose the appropriate device type.
- d. Click **Monitor**. The response appears in the **Output** area.

Figure 8-15 Output Area

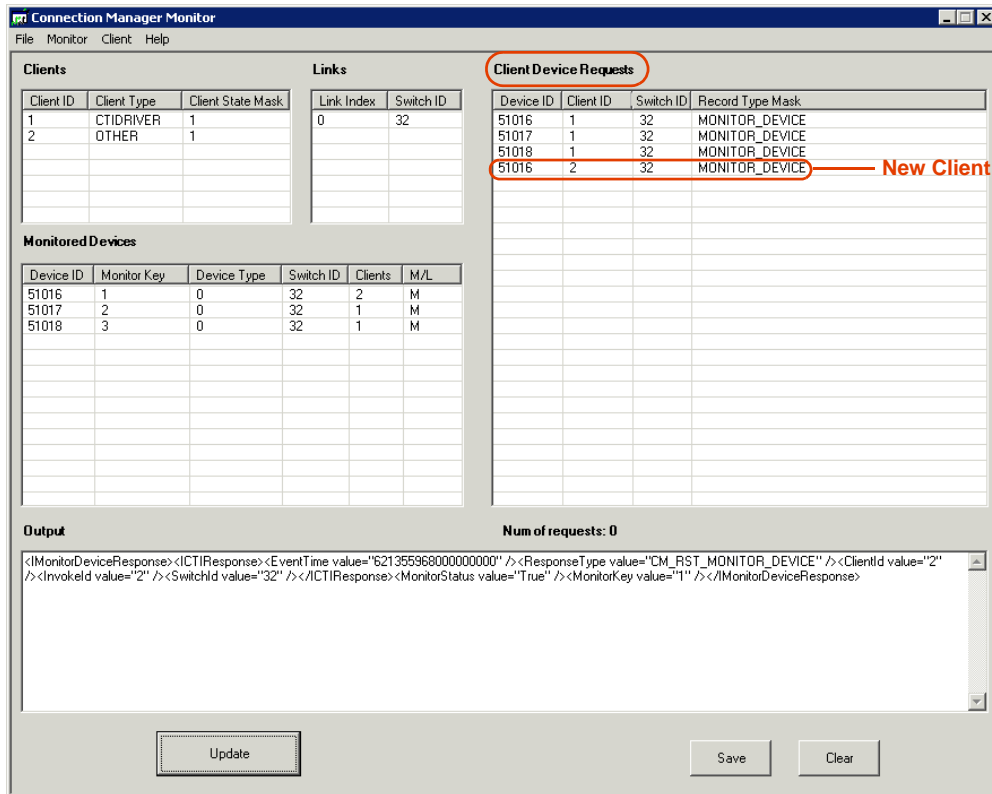


IMPORTANT

The Connection Manager Monitor window does not continuously refresh the data displayed in the window; it only displays the data current at the time you establish the connection. To update the data displayed in the window, click **Update**.

7. Click **Update**. The new Client appears in the **Client Device Requests** area.

Figure 8-16 Connection Manager Monitor - Client Device Requests Area



Managing the Connection Manager Monitor

This section includes the following topics:

- Stopping the Connection Manager Monitor
- Disconnecting the Connection Manager Monitor Client

Stopping the Connection Manager Monitor

This procedure describes how to stop the Connection Manager Monitor when it is functioning as a client.

To stop the Connection Manager Monitor:

1. From the **Client** menu of the Connection Manager Monitor window, choose **Stop Monitor**. The Stop Monitor Device window appears.

Figure 8-17 Stop Monitor Device Window



2. Type the **Device ID** number and the **Switch ID** of the device you want to stop monitoring.
3. Click **Stop Monitor**. The response appears in the **Output** area.

Disconnecting the Connection Manager Monitor Client

This procedure describes how to disconnect the Connection Manager Monitor when it is functioning as a client.

To disconnect the Connection Manager Monitor Client:

- From the **Client** menu of the Connection Manager Monitor window, choose **Disconnect**.
The Client connection of the Connection Manager no longer appears in the **Clients** area and in the **Client Device Requests** area.

Log Manager System

The Log Manager system logs all significant system activity and maintains a log of all data, enabling you to view the history of all relevant system activity.

The Log Manager system has four main components:

- **CTI Console Viewer**
- **Log Manager**
- **Log Manager Services**
- **Log Viewer**

CTI Console Viewer

The CTI Console Viewer enables real-time log tracking of the screens of all integration components installed on the local machine. This application replaces the Console windows in the Reporting Level of the integration process, and provides the user with filtering capability.

CTI Console Viewer has a separate window for each integration process. You can view and filter an event, as well as change the reporting level. You cannot do this in the System Administrator. Files are saved automatically in the Log Manager and can be viewed afterwards in the Log Viewer.

Figure 8-18 CTI Console Viewer



To open the CTI Console viewer:

- To open, double-click the icon in the system tray.

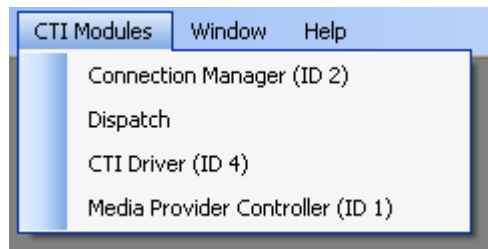


-or-

- Right-click the icon, and select **Open NICE CTI Console Viewer**.

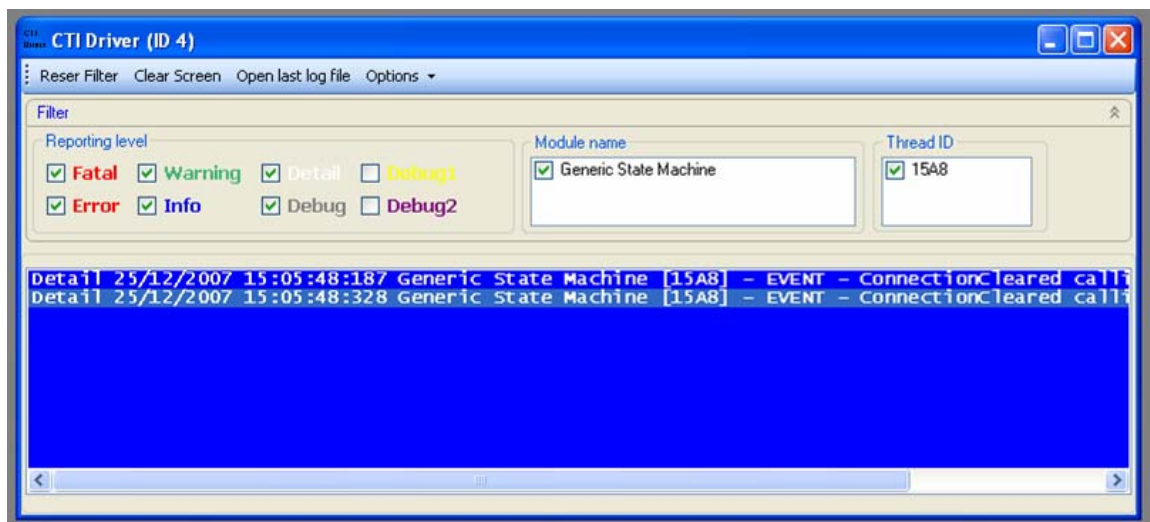
To open a specific integration process window:

1. From the **CTI Modules** menu, choose the relevant integration process.



A log window opens and the integration modules installed on the local machine are listed. (This list is updated when you add/remove any integration modules in the System Administrator).

Figure 8-19 CTI Log Window



NOTE: These reporting levels are only relevant for the CTI Console.

WARNING

Reporting levels may be helpful for troubleshooting. However, making changes to the reporting levels can greatly add to the load on your system. Changing reporting levels should therefore be done **only** by authorized personnel and in conjunction with NICE Customer Support.

Filtering Messages

You can filter messages in any of the following manners:

- **Reporting level** - Clear the checkboxes of the reporting levels that are irrelevant (message importance).

- **Module name** - Clear the checkboxes of any modules that are irrelevant.
- **Thread ID** - Clear the checkboxes of any Thread IDs that are irrelevant.

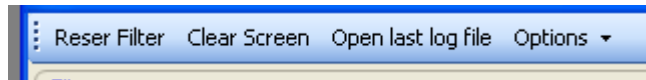
To reset the filter:



NOTE: The filter is applied to new messages. It does not affect old messages.

- Click the **Reset Filter** button.

The filter in Module Name and Thread ID is reset, and all the messages are printed. (The Reset filter option does not affect the reporting level).



To clear the screen of messages:

- Click the **Clear Screen** button.

All the messages are cleared from the screen.

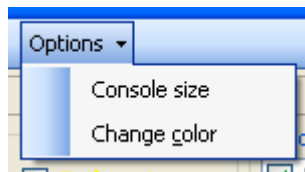
To open the last log file:

- Click the **Open last log file** button.

The current log file with Log Viewer opens (see Log Viewer section). You can see log messages from the specific modules in real-time as they are displayed.

To change console size and color:

1. From the **Options** menu, choose **Console size**.



When the log window is filled with the maximum number of messages, the top rows are automatically deleted.

2. From the **Options** menu, choose **Change color**.
 - a. Select a background color.
 - b. Select a color for each reporting level.

Log Manager

The Log Manager creates log message files and/or sends information regarding the Console and the Event Log according to the predefined Reporting Level filter.

WARNING

Reporting levels may be helpful for troubleshooting. However, making changes to the reporting levels can greatly add to the load on your system. Changing reporting levels should therefore be done **only** by authorized personnel and in conjunction with NICE Customer Support.

You can set the reporting levels in any of the integration branches e.g. in the Connection Managers, in the Drivers, in the Key Managers, in the Media Provider Controllers (Observers), or in the New Driver wizards when you initially set up the driver.

By default, reporting levels are defined for the following:

- **Console** - reports to the standard Console window
- **File** - reports to the Log file located in the Integrations installation folder
- **Event Log** - reports to the Log files located in the Event Viewer



NOTE: The Event Viewer is a Microsoft feature which can be viewed under the **Control Panel > Administrative Tools**.

If necessary, you can also manage the size of the log files, the amount of disk space dedicated to them, and the number of days you wish to keep log files.

To define the reporting levels:

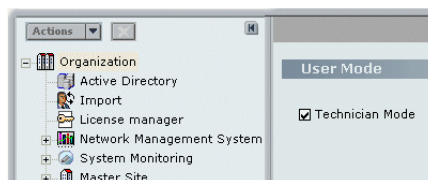
1. Open the System Administrator, as follows:
 - a. Log in to the NICE Perform Applications Suite.
 - b. From the **Accessories** menu, choose **System Administrator**.



The System Administrator appears with a list of NICE components under the **Site** branch in the **Organization** tree.

To add components in the System Administrator, you must work in Technician Mode.

2. Set the System Administrator to Technician Mode:
 - In the Organization Tree, select the **Organization** branch.




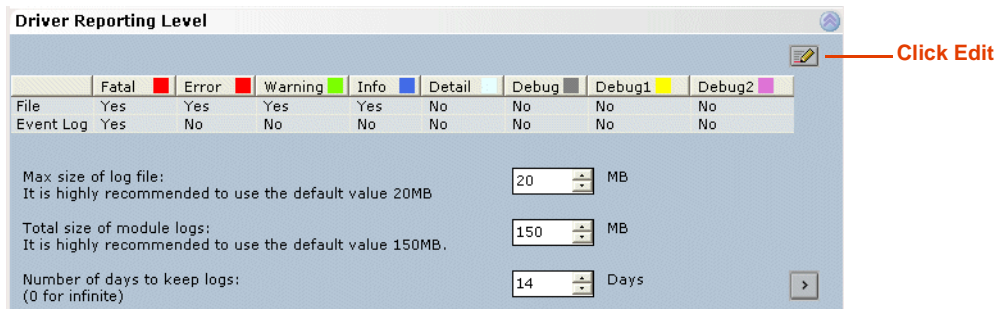








3. Mark the **Technician Mode** checkbox and click **Save** .
4. You can set the Reporting Level in any of the branches, see the examples below:
 - In the **Organization** tree, expand **Master Site > CTI Integrations > Connection Managers** and click the relevant **Connection Manager**. In the **Connection Manager Details** area, expand **Reporting Level**.
 - or-
 - In the **Organization** tree, expand **Master Site > CTI Integrations > Drivers**. In the **Driver General Information** area, expand **Driver Reporting Level**.

Figure 8-20 Driver Reporting Level Area



	Fatal 	Error 	Warning 	Info 	Detail 	Debug 	Debug1 	Debug2 
File	Yes	Yes	Yes	Yes	No	No	No	No
Event Log	Yes	No	No	No	No	No	No	No

Max size of log file:
It is highly recommended to use the default value 20MB MB

Total size of module logs:
It is highly recommended to use the default value 150MB. MB

Number of days to keep logs:
(0 for infinite) Days

5. Choose the desired row and click **Edit** . The Set Reporting Level window appears.

Figure 8-21 Set Reporting Level Window



Set Driver Reporting Level

Set the Reporting Level

File

Choose the Driver reporting levels:

Fatal  Debug 

Error  Debug1 

Warning  Debug2 


Info 

Detail 

6. Mark the checkboxes for the reporting levels you want to include and click **OK**.



NOTE: It is highly recommended that you do not change the settings of the default reporting levels. Changing reporting levels should be done **only** by authorized personnel and in conjunction with NICE Customer Support.

7. In the relevant log field, type the new setting and click **Save** .

Log Manager Services

The Log Manager's second module can be found in **Services**. It consists of two log manager related services:

- Nice Integration Log Retention
- Nice Integration Reporting Level Dumper

WARNING

You should not change any values in the Registry. All changes should be made through the System Administrator application and be done **only** by authorized personnel and in conjunction with NICE Customer Support.

Log Viewer

The Log Viewer enables you to view the log files and to filter them. You can keep several logs open at the same time.

Filtering Logs

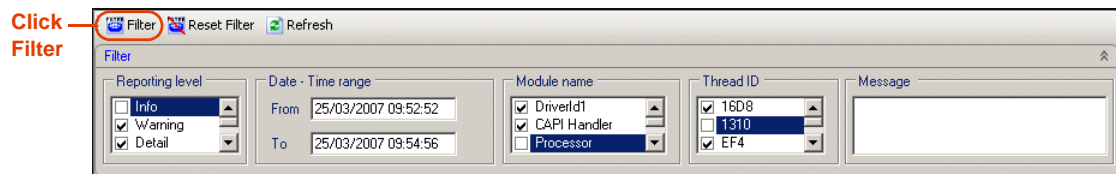
You can filter the logs according to the following criteria:

- **Reporting level:** Clear the reporting levels that are irrelevant.
- **Date:** Choose the appropriate time range.
- **Module name:** Unmark any modules that are irrelevant.
- **Thread ID:** Unmark any thread IDs that are irrelevant.
- **Message:** Type any relevant message.

To filter a log file:

1. In the Interaction Center, navigate to the **Tools** folder (the default location is **D:\NICECTI\Integrations\Tools**).
2. Double-click **LogViewer.exe**. The Log Viewer window appears.
3. Using Windows Explorer, select the relevant log files and drag them to the **Log Viewer**.
4. In the **Filter** area, mark the relevant filter options.

Figure 8-22 Log Viewer Window



5. Click **Filter**. The filtered logs appear in the Log Viewer window.

6. To save the filtered log file for future reference: from the **File** menu, choose **Save as**. The Save as window appears.
7. Name the filtered log file appropriately.

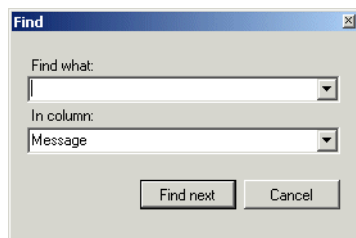
Searching Logs

The Log Viewer enables you to search for specific text within a specific column or within all columns. The Log Viewer remembers past searches.

To search for a specific text value:

1. From the **Edit** menu, choose **Find**. The Find window appears.

Figure 8-23 Find Window



2. Click the **In column** drop-down list and choose the relevant search basis.
3. Click **Find next**.

CAPI Spy

The CAPI Spy enables you to monitor all messages sent by the CTI driver to the CLS CAPI (Call Server). Examination of these messages enables you to pinpoint whether the problem is in the CTI driver or in the CLS CAPI server.

CAPI Spy has two main components:

- CAPI Spy Plug-in
- CAPI Spy Utility

CAPI Spy Plug-in

The CAPI Spy plug-in is one of the standard CTI driver plug-ins. You set it up in the System Administrator. Only marked plug-ins are executed by the CTI driver.

To set up the CAPI Spy Plug-in:

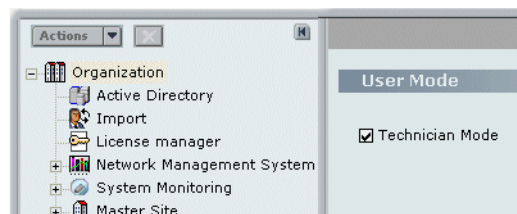
1. Open the System Administrator, as follows:
 - a. Log in to the NICE Perform Applications Suite.
 - b. From the **Accessories** menu, choose **System Administrator**.



The System Administrator appears with a list of NICE components under the **Site** branch in the **Organization** tree.

To add components in the System Administrator, you must work in Technician Mode.

2. Set the System Administrator to Technician Mode:
 - a. In the Organization Tree, select the **Organization** branch.




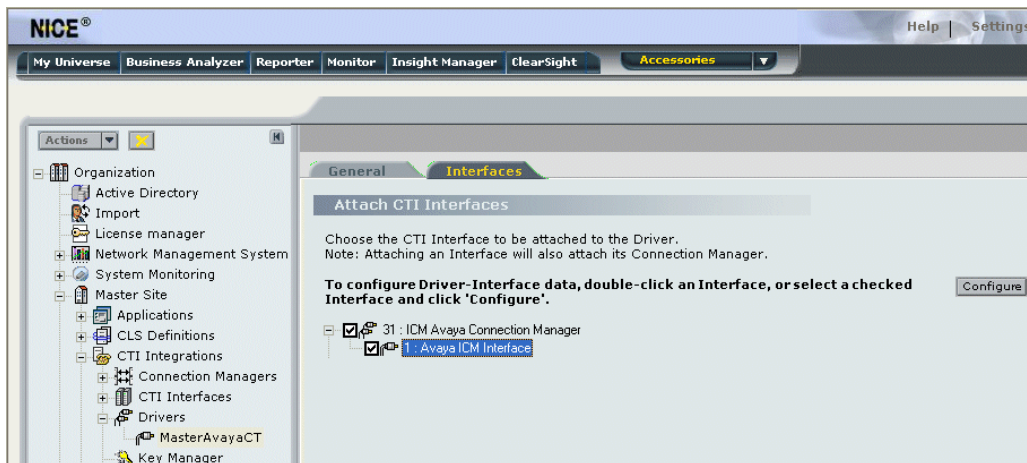
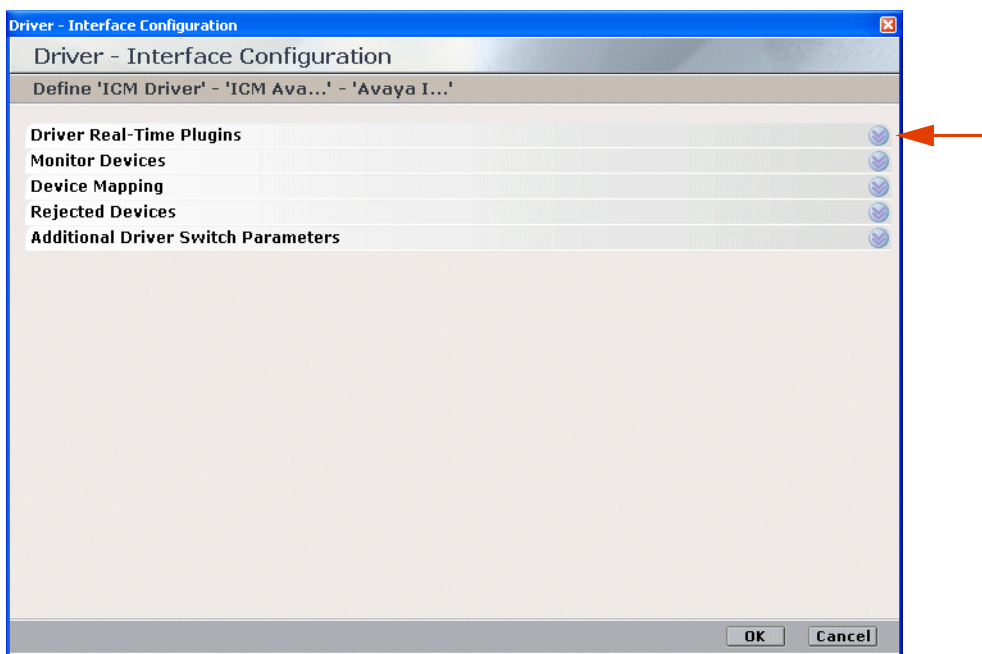
- b. Mark the **Technician Mode** checkbox and click **Save** .
3. In the **Organization** tree, navigate to **Master Site > CTI Integrations > Drivers**. Click the relevant driver.
 4. Click the **Interfaces** tab.

Figure 8-24 Drivers > Interfaces Tab



5. In the **Attach CTI Interfaces** section, click the relevant interface driver and click **Configure**. The Driver - Interface Configuration window appears.

Figure 8-25 Driver - Interface Configuration Window



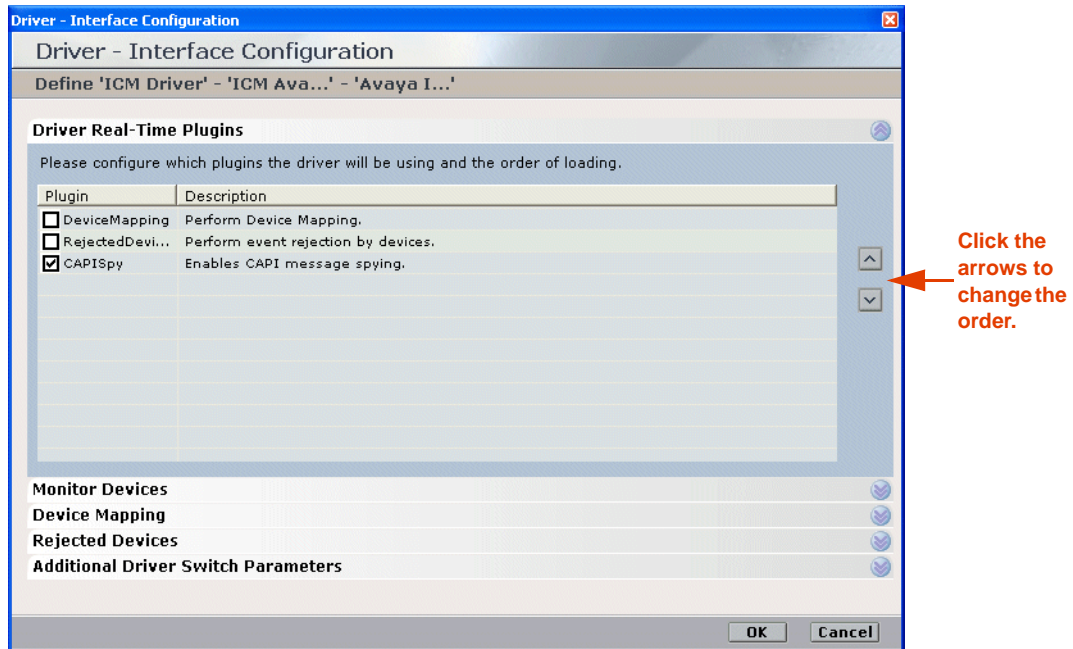
6. Expand **Driver Real-Time Plugins**.



IMPORTANT

You can mark CAPIspy once and then leave it marked, as it has no negative impact on the system.

Figure 8-26 Driver Real-Time Plugins Area



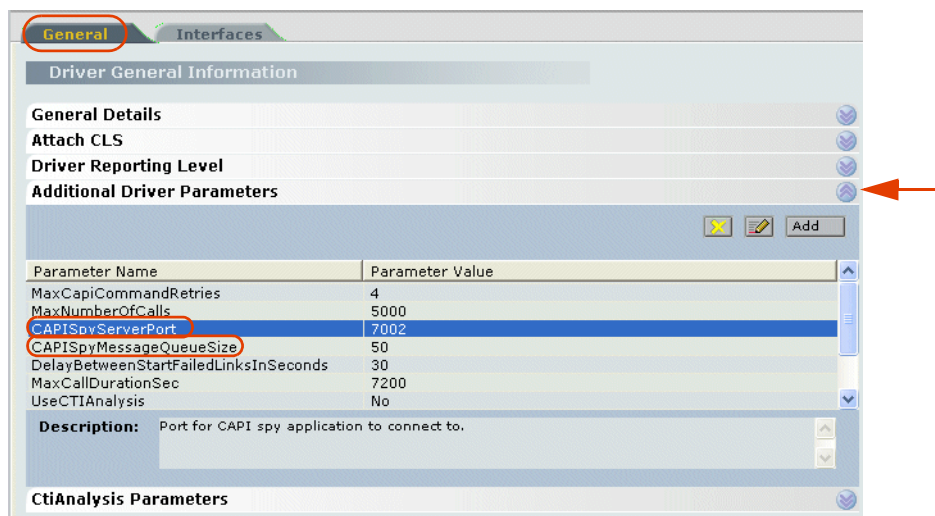
7. Mark the **CAPISpy** checkbox and click **OK**.



NOTE: It is highly recommended that CAPISpy be the last entry in the Driver Real-Time Plugins list. This enables you to see any changes that may have come about because of other plugins. You can change the order of the drivers by clicking the arrows. After you mark or unmark the CAPISpy checkbox, you must restart the driver before the change will take effect.

8. Click the **General** tab and expand **Additional Driver Parameters**. The **Additional Driver Parameters** area displays.

Figure 8-27 Additional Driver Parameters Area



- Define the CAPI Spy parameters according to the following table:

Table 8-2: CAPI Spy Parameters

Parameter Name	Description	Default Value
CAPISpyServerPort	Port to which the CAPI Spy connects. NOTE: You should not change the value of this parameter unless there is another third party application that uses this port. If the value is changed , restart the driver. Then configure the CAPI Spy application to connect to the new port. See Changing Connection Details.	7002
CAPISpyMessageQueueSize	Size of message queue in CAPI Spy server. NOTE: Be careful about setting this to a higher value as it can slow driver performance.	50

- Click **Save** .

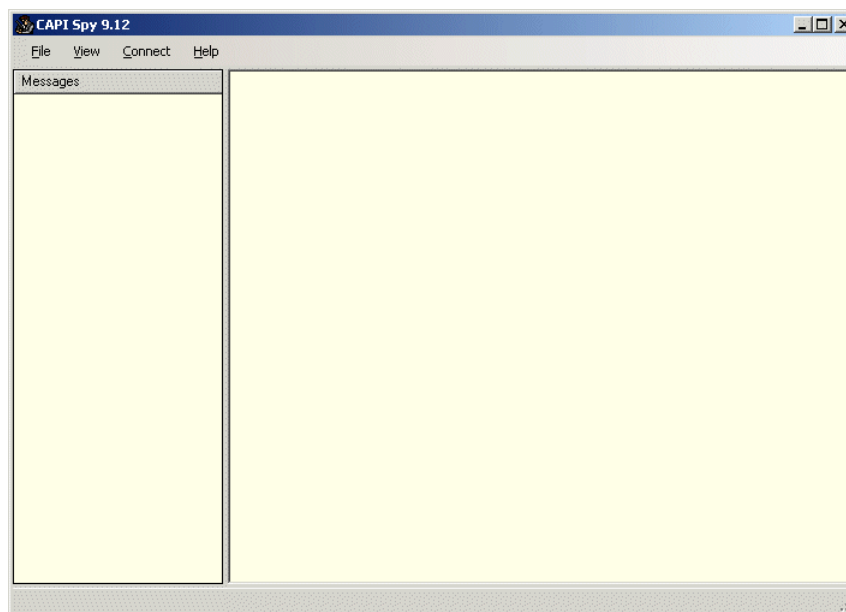
CAPI Spy Utility

NICE Systems provides a utility for viewing the CAPI Spy messages in XML format.

To set up the CAPI Spy:

- In the NICE Interactions Center, navigate to the **Integrations** folder (the default location is **D:\NICECT\Integrations**). Double-click **CAPISpy.exe**. The CAPI Spy window appears.

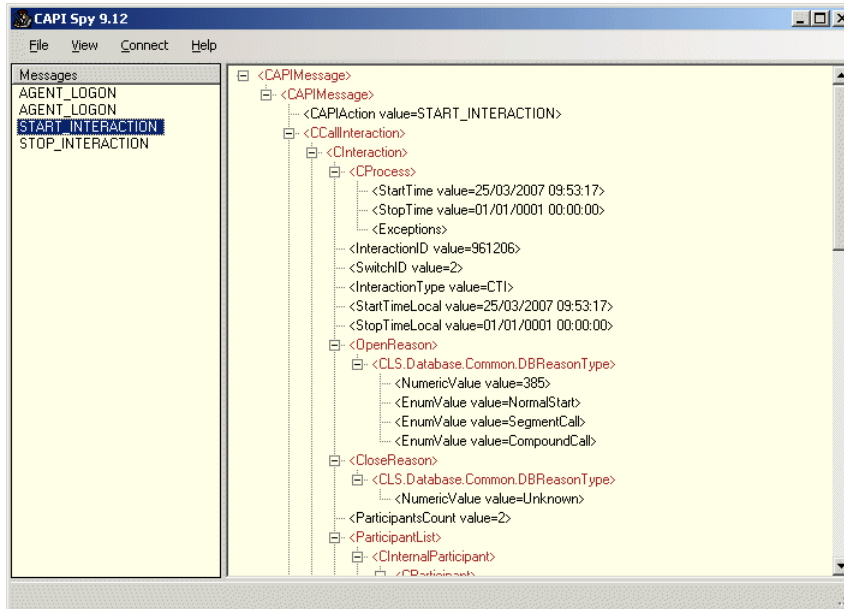
Figure 8-28 CAPI Spy Window



- From the **Connect** menu, choose **Connect to CTI Driver**.

After the CAPI CTI driver and the CAPI Spy utility are connected, the CAPI Spy starts displaying CAPI messages.

Figure 8-29 CAPI Spy Window Displaying Messages



NOTE: If the connection is not successful, an error message appears. Contact NICE Customer Support.

If the connection is dropped, an error message appears. To reconnect the connection, from the **Connect** menu, choose **Connect to CTI Driver**.

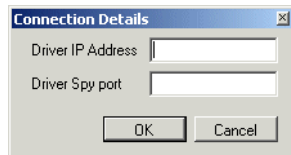
Changing Connection Details

The CAPI Spy by default connects to the localhost CTI driver on the 7002 port. When port 7002 is used by another third party application, you can change the port. See *CAPI Spy Plug-in*.

To change the connection details:

1. From the **Connect** menu, choose **Change connection details**. The Connection Details window appears.

Figure 8-30 Connection Details Window



2. Type the **Driver IP Address** and the **Driver Spy port**.
3. Click **OK**.



NOTE: You can also monitor CAPI messages from a different host. In this case, type the IP address of the remote machine. This can seriously overload the network and should be avoided if possible.

TAPIMonitor

This section describes how to use TAPIMonitor as a debugging tool.

The TAPIMonitor enables you to see the events occurring from the Cisco TSP. You can view the lines that are open and see the events on those lines.



NOTE: This tool should only be used for debugging purposes when you are instructed to do so by the NICE Support personnel.

To run the TAPIMonitor as a debug tool:

1. Follow the instructions in **Verifying the TSP Client Configuration** on [page 67](#).



IMPORTANT

When running TAPIMonitor as a debug tool, it is highly recommended that you stop the NICE Integration Dispatch Service. If you cannot stop it for operational reasons, contact NICE Customer Support.

2. Send the **TAPIMonitor.txt** file to NICE Customer Support.

Blank page for double-sided printing.

Troubleshooting

This chapter provides troubleshooting through the provision of a flow of log files. It also includes TAPI troubleshooting scenarios and VRSP troubleshooting error codes and messages for the NICE Interactions Center and the Cisco Unified Communications Manager integration in an Active Recording environment.



NOTE: The screen-captures in this section show UID (SEP and MAC addresses). If channel-mapping is based on DN, the DN will appear instead of the UIDs.

Contents

TAPI Troubleshooting	174
VRSP (FSP) Troubleshooting	175
VRSP (FSP) Error Codes.....	175
VRSP SNMP Messages.....	175
Total Recording Troubleshooting	176
Flow of Information through the Log Files.....	176
VRSP (FSP) Log File.....	177
MPCM (FLM) Log File	177
CUCM SIP Invite to VRSP in the VRSP (FSP) Log Files	178
RCM <> Call Server <> MPCM.....	179
Call Server Log File	179
RCM Log File.....	179
RCM <> VoIP Logger <> VRSP	180
VRSP (FSP) Log File.....	182
IPCapture Process Log File.....	181
New Call Scenario.....	181
VRSP (FSP) Log File - CUCM and VRSP SIP Communication	181
Ethereal Sniffing Tool Examples	183
Interaction-Based Recording Troubleshooting	185
Flow of Information through the Log Files.....	185
New Call.....	186
RCM <> VoIP Logger <> VRSP	186

TAPI Troubleshooting

The following table describes troubleshooting problem scenarios and solution procedures for the NICE Interactions Center and the Cisco Unified Communications Manager integration:

Problem	Solution
After installing and configuring the Cisco TSP, you run the TapiMonitor.exe . However, a complete list of lines does not appear.	Reboot the computer. The Telephony Service must be synchronized with the Communications Manager. To do this, you need to reboot the computer.
Calls via the IVR are not reported correctly.	Ensure that all CTI ports are attached to your user and are configured in the devices as IVR.
Calls via the ACD are not reported correctly.	Make sure that all hunt groups are configured in the devices as ACD.
Group Pick Up scenarios are not reported correctly.	Make sure that all Pick Up Group numbers are configured in the devices as PickUp Group .
Call Park scenarios are not reported correctly.	Make sure that the Park numbers are attached to your TSP user.

VRSP (FSP) Troubleshooting

VRSP (FSP) Error Codes

The following error codes appear on the VRSP (FSP) during the NICE Interactions Center and the CUCM integration with Cisco IP phones:

Error Code	Short Description	Description
400	Bad request	The VRSP cannot parse the Invite messages from the VoIP logger or the CUCM.
404	Not found	The CUCM or VoIP Logger sends Invite messages for a device that does not appear in the list of Recording Profiles.
503	Service Unavailable	The VRSP receives an error code from the TAPI interface for a Start Record Request .

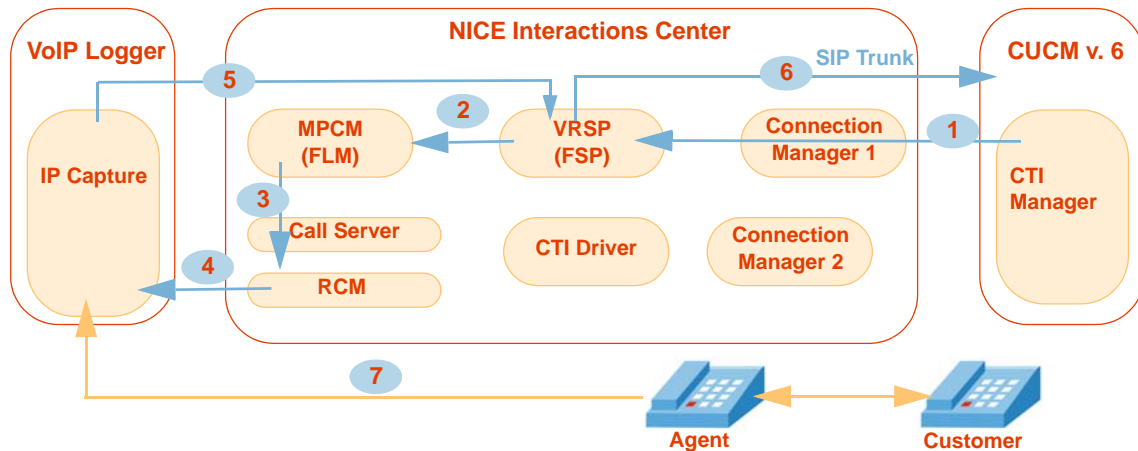
VRSP SNMP Messages

The following VRSP SNMP messages can appear during the NICE Interactions Center and the CUCM integration with Cisco IP phones:

SNMP Message	Description
FSP is up	FSP is up
FSP is down	FSP is down
CTI Manager crash	The VRSP tries to communicate with the TAPI server during Interaction-based recording.
Configuration is missing	A parameter in the configuration is missing.
FSP internal errors	For example, SIP stack errors.

Total Recording Troubleshooting

Flow of Information through the Log Files



- 1 VRSP (FSP) acquires the UID, DN, Recording Mode from the CTI Manager via TAPI: see **VRSP (FSP) Log File** on **page 177**.
- 2 The following information is saved in the MPCM (FLM): UID, DN, VRSP URI: see **MPCM (FLM) Log File** on **page 177**.
- 3 The following information is delivered to the RCM: UID, DN, VRSP URI: see **RCM Log File** on **page 179**.
- 4 The following information is delivered to the IPCapture process in the VoIP Logger: UID, DN, VRSP URI.
- 5 The following information (SDP) is delivered to the VRSP (FSP): VoIP Logger IP, Ports, UID, DN: see **IPCapture Process Log File** on **page 181**.
- 6 Call start (SIP **Invite** from CUCM) and then the following information (SDP) is replied to the CUCM: UID, DN, VoIP Logger IP, Ports: see **VRSP (FSP) Log File - CUCM and VRSP SIP Communication** on **page 181**.
- 7 RTP (Rx & Tx) is sent from the agent phone to the VoIP Logger.

VRSP (FSP) Log File

The VRSP (FSP) stores the following information which is very useful for troubleshooting purposes in its log files:

DN	UID	Recording Mode
2000	SEP1	Automatic Recording
2001	SEP2	Application Invocation

Each time a Device Number is added or deleted in the CUCM, this information is updated in the VRSP (FSP).

To troubleshoot from the VRSP (FSP) log files:

- Navigate to **D:\NICECT\Integration\Log**

Figure 9-1 VRSP (FSP) Log File

```

FSP_2012_1647.log - Notepad
File Edit Format View Help
[Detail] 20/12/2007 16:47:49:109 RCI - Recording Handler 1350
DN:6437 DeviceName:SEP00192FC56897
RecordingProfile:eAutomaticInvocation
[Info] 20/12/2007 16:47:49:125 REDUNDANCY_UNIT 17D8
CActivityControllerFactory.GetActivityController: Creating dummy
activity controller for FSP.
[Info] 20/12/2007 16:47:49:140 FSP - Manager 1350
CFSPManager::onRCIFirstNotificationIsFinished: RCI Finished notifying
telephony devices, Loading SIP stack and activity controller.
[Info] 20/12/2007 16:47:50:125 REDUNDANCY_UNIT 17D8
CDummyActivityController.Start - Started
ActivityControllerLib.CDummyActivityController activity controller.
[Info] 20/12/2007 16:47:50:125 FSP - Observer 17D8
CSipStackObserver::StartReceivingMessages: waiting for SIP messages.
[Detail] 20/12/2007 16:47:50:140 FSP - Observer 414
CSipStackObserver::onCallLegStateChangedEv: Session: 305726792,
Received INVITE message, passing it to
FSP.Core.CForwardingReceiverUnit Unit.
[Detail] 20/12/2007 16:47:50:281 FSP - FLM Unit 13B8
CForwardingLocationManagerUnit::HandleStateChanged: FLM session
305726360 is connected, FSP will send INFO messages for known Media
Sources.
[Detail] 20/12/2007 16:47:50:312 FSP - FR Unit 414
CForwardingReceiverSession::HandleOfferingState: Accepting FR session
Session: 305726792 , [TS: DeviceName: SEP00192FC56897, Direction: Tx],
[TS: DeviceName: SEP00192FC56897, Direction: Rx].
[Detail] 20/12/2007 16:47:51:203 FSP - FLM Unit 1794
CForwardingLocationManagerUnit::HandleOkResponseForInfoMessage:
Telephony Source: DN: 6437, DeviceName: SEP00192FC56897 registered in
FLM.
[Detail] 20/12/2007 16:47:51:203 FSP - FLM Unit 1794
CForwardingLocationManagerUnit::HandleOkResponseForInfoMessage:
Telephony Source: DeviceName: SEP00192FC56897 registered in FLM.

```

MPCM (FLM) Log File

The MPCM (FLM) stores the following information which is very useful for troubleshooting purposes in its log files:

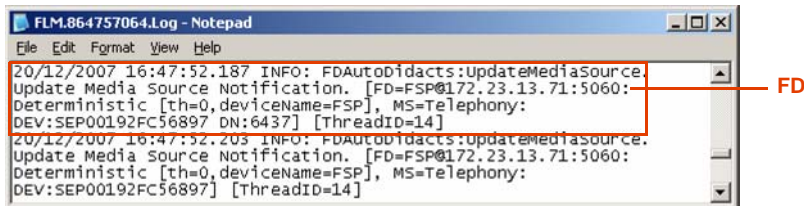
DN	UID	Forwarding Device
2000	SEP1	VRSP1
2001	SEP2	VRSP1

Each time a Device Number is added or deleted in the CUCM, this information is updated in the VRSP (FSP).

To troubleshoot from the MPCM (FLM) log file:

- Navigate to **C:\Program Files\Common Files\Nice\LogService\Logs\FLM**

Figure 9-2 FLM Log Files



```

FLM.864757064.Log - Notepad
File Edit Format View Help
20/12/2007 16:47:52.187 INFO: FDAutoDidacts:UpdateMediaSource.
Update Media Source Notification. [FD=FSP@172.23.13.71:5060:
Deterministic [th=0,deviceName=FSP], MS=Telephony:
DEV:SEP00192FC56897 DN:6437] [ThreadID=14]
20/12/2007 16:47:52.203 INFO: FDAutoDidacts:UpdateMediaSource.
Update Media Source Notification. [FD=FSP@172.23.13.71:5060:
Deterministic [th=0,deviceName=FSP], MS=Telephony:
DEV:SEP00192FC56897] [ThreadID=14]
  
```

CUCM SIP Invite to VRSP in the VRSP (FSP) Log Files

The CUCM SIP Invite message found in the VRSP (FSP) log files can be very useful for troubleshooting purposes.

To troubleshoot from the CUCM SIP Invite Message in the VRSP (FSP) log files:..

Figure 9-3 CUCM SIP Invite Message in the VRSP (FSP) Log File



```

FSP_2012_1647.log - Notepad
File Edit Format View Help
Detail 20/12/2007 16:47:50:312 FSP - FR Unit 414
CForwardingReceiverSession:HandleOfferingState: Accepting FR session
Session: 305726792, [TS: DeviceName: SEP00192FC56897, Direction: Tx],
[TS: DeviceName: SEP00192FC56897, Direction: Rx].
  
```

RCM <> Call Server <> MPCM

The first total recording scenario is described in **Flow of Information Between RCM, Call Server, and MPCM (FLM)** on [page 23](#). When this scenario finishes, the NICE Interactions Center, acting as Controller, contains the following information:

UID	Forwarding Device
SEP1	VRSP1
SEP1	VRSP1

You can use this information for troubleshooting purposes. See:

- [Call Server Log File](#) on [page 179](#)
- [RCM Log File](#) on [page 179](#)

Call Server Log File

To troubleshoot from the Call Server log files:

- Navigate to **D:\Program Files\NICE Systems\NICE CLS\Log**

Figure 9-4 Call Server Log File

```

20/12/07 16:48:19.062 INFO [7732]: FLMMANAGER: [RCMwrapper :
SendToRCM] sending MapVoipRequest to RCM:
VoipMapRequest: requestID=0; switchID=1;
timeReceived=633337660987812500; timeUpdatedCounter=0; UnMap=False;
UniqueDeviceID=SEP00192FC56897; RxPort=0; TxPort=0;
FLMMediaSource=DEV:SEP00192FC56897 DN:6437 ; ForwardingDevice[0]
=FD:FSP@172.23.13.71:5060,Level=0,ReportTime=4:47:51 PM;
  
```

UID — UniqueDeviceID=SEP00192FC56897; RxPort=0; TxPort=0;
 VRSP — FLMMediaSource=DEV:SEP00192FC56897 DN:6437 ; ForwardingDevice[0]

RCM Log File

To troubleshoot from the RCM log files:

- Navigate to **D:\Program Files\NICE Systems\NICE CLS\Log**

Figure 9-5 RCM Log File

```

20/12/07 16:48:19.062 INFO [7332]: [VoipMapRequest: id 0] Received
Request:
VoipMapRequest: requestID=0; switchID=1;
timeReceived=633337660990625000; timeUpdatedCounter=1; UnMap=False;
UniqueDeviceID=SEP00192FC56897; RxPort=0; TxPort=0;
FLMMediaSource=DEV:SEP00192FC56897 DN:6437 ; ForwardingDevice[0]
=FD:FSP@172.23.13.71:5060,Level=0,ReportTime=4:47:51 PM;
  
```

UID — UniqueDeviceID=SEP00192FC56897; RxPort=0; TxPort=0;
 VRSP — FLMMediaSource=DEV:SEP00192FC56897 DN:6437 ; ForwardingDevice[0]

RCM <> VoIP Logger <> VRSP

After **Flow of Information Between RCM, VoIP Logger, and VRSP (FSP)** on [page 24](#) takes place and the IP Capture on the VoIP Logger has sent the forwarding command to the VRSP, the VRSP (FSP) contains the following information:

UID	SDP Value
SEP1	Logger IP, Rx Port
SEP1	Logger IP, Tx Port
SEP2	Logger IP, Rx Port
SEP2	Logger IP, Tx Port

VRSP (FSP) cache consists of the following:

- **VRSP (FSP) Log File** on [page 182](#)
- **IPCapture Process Log File** on [page 181](#)

You can use this information for troubleshooting purposes.

IPCapture Process Log File

To troubleshoot from the IP Capture process log file:

- Navigate to **D:\NTLogger\VoIPCapture\Log**

Figure 9-6 IP Capture Log File

```

IPCapture.765632064.Log - Notepad
File Edit Format View Help
20/12/2007 16:47:05.181 INFO: SIPintSessionController.openSession.
Opening session. ForwardDeviceUri=FSP@172.23.13.71:5060,
MediaSource=DEV=SEP00192FC56897, Direction=Incoming,
TargetIP=172.23.13.88, TargetPort=1177, Participants 2 [ThreadID=6]
20/12/2007 16:47:05.181 INFO: SIPintegrationChannel.Start.
SIPintegrationchannel 1: SIP channel is pending for start [ThreadID=6]
20/12/2007 16:47:05.181 INFO: SIPintSessionController.openSession.
Opening session. ForwardDeviceUri=FSP@172.23.13.71:5060,
MediaSource=DEV=SEP00192FC56897, Direction=outgoing,
TargetIP=172.23.13.88, TargetPort=1178, Participants 2 [ThreadID=6]
  
```

New Call Scenario

The **Flow of New Call Recording** on [page 25](#) then takes place. You can troubleshoot the SIP communication between the CUCM and VRSP (FSP) using:

- **VRSP (FSP) Log File - CUCM and VRSP SIP Communication** on [page 181](#)
- **Ethereal Sniffing Tool Examples** on [page 183](#)

VRSP (FSP) Log File - CUCM and VRSP SIP Communication

To troubleshoot from log file showing SIP communication between CUCM and VRSP:

- Navigate to **D:\NICECT\Integration\Log**

Figure 9-7 SIP Communication Between the CUCM and VRSP (FSP) Log File

```

FSP_2012_1647.log - Notepad
File Edit Format View Help
Detail 20/12/2007 16:48:59:125 FSP - Observer 1690
CSipStackObserver::onCallLegStateChangedEv: Session: 305728520, Received
INVITE message, passing it to FSP.Core.CCallManagerUnit.

Detail 20/12/2007 16:48:59:125 FSP - CCM Unit 1690
CCallManagerSession::HandleOfferingState: Accepting CCM session 305728520.
Telephony Source - DN: 6437, DeviceName: SEP00192FC56897, X-RefCI:
49006098, Direction: Rx, SDP - IP: 172.23.13.88, Port: 1178, Channel: Rx,
Codecs: 0 8 18 4 9

Detail 20/12/2007 16:48:59:156 FSP - Observer 1388
CSipStackObserver::onCallLegStateChangedEv: Session: 305728952, Received
INVITE message, passing it to FSP.Core.CCallManagerUnit.

Detail 20/12/2007 16:48:59:156 FSP - CCM Unit 1388
CCallManagerSession::HandleOfferingState: Accepting CCM session 305728952.
Telephony Source - DN: 6437, DeviceName: SEP00192FC56897, X-RefCI:
49006098, Direction: Tx, SDP - IP: 172.23.13.88, Port: 1177, Channel: Tx,
Codecs: 0 8 18 4 9

Detail 20/12/2007 16:49:11:578 FSP - CCM Unit 16C0
CCallManagerSession::HandleDisconnectedState: Closing CCM session
305728520 for Telephony source - DN: 6437, DeviceName: SEP00192FC56897, X-
RefCI: 49006098, Direction: Rx.

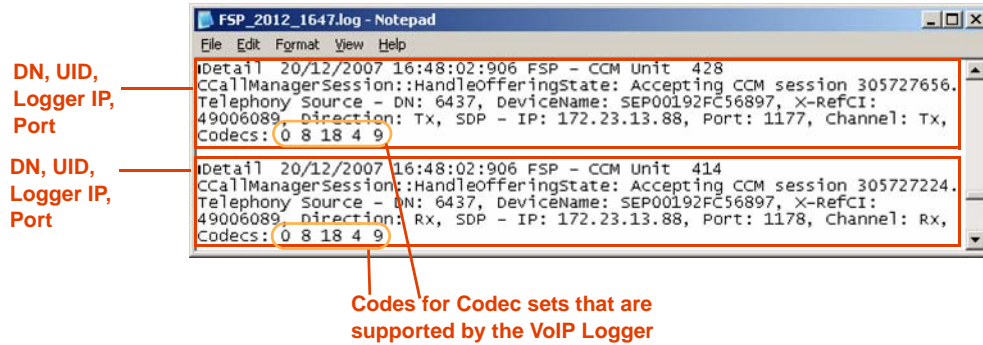
Detail 20/12/2007 16:49:11:578 FSP - CCM Unit 16C4
CCallManagerSession::HandleDisconnectedState: Closing CCM session
305728952 for Telephony source - DN: 6437, DeviceName: SEP00192FC56897, X-
RefCI: 49006098, Direction: Tx.
  
```

VRSP (FSP) Log File

To troubleshoot from the VRSP (FSP) log file:

- Navigate to **D:\NICECTI\Integration\Log**

Figure 9-8 VRSP (FSP) Log File



Codes for Codec sets:

- 0 - G711 (PCM MU-Low)
- 8 - G711 (PCM A-Low)
- 18 - G729
- 4 - G723
- 9 - G722

Ethereal Sniffing Tool Examples

This is the Invite message that arrives from the CUCM that you should expect to see at the beginning of each call. This indicates to you that the CUCM has been configured correctly for this integration.

To troubleshoot using the Ethereal sniffing tool:

1. Run the Ethereal Sniffer.
2. Capture the traffic of the Interactions Center NIC while performing a call.
3. In the **Filter** field, type **SIP**.
4. Click **Apply**.
5. Look for the packet going between the CUCM and the NICE Interactions Center showing the Invite SIP command seen below.

Figure 9-9 Ethereal Sniffing Tool - Invite from the CUCM

The screenshot displays the Ethereal interface with the following details:

- Filter:** sip
- Packet List:**

No.	Time	Source	Destination	Protocol	Info
328	7.143878	192.168.241.228	172.16.1.31	SIP	Request: INVITE sip:87150@172.16.1.31:5060
329	7.144774	172.16.1.31	192.168.241.228	SIP	Status: 100 Trying
330	7.145977	172.16.1.31	192.168.241.228	SIP/SD	Status: 200 OK, with session description
- Packet Details (Frame 328):**
 - Ethernet II, Src: Cisco_2d:ee:00 (00:0d:66:2d:ee:00), Dst: HewlettP_ad:26:5c (00:0e:7f:ad:26:5c)
 - Internet Protocol, Src: 192.168.241.228 (192.168.241.228), Dst: 172.16.1.31 (172.16.1.31)
 - User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
 - Session Initiation Protocol
 - Request-Line: INVITE sip:87150@172.16.1.31:5060 SIP/2.0
 - Message Header
 - Remote-Party-ID: <sip:6437@192.168.241.228>;party=calling;screen=yes;privacy=off
 - From: <sip:6437@192.168.241.228>;x-nearend;x-refci=48390221;x-nearenddevice=SEP00192FC56897;
 - To: <sip:87150@172.16.1.31>

Labels and connections in the image:

- DN** points to the **To** header field.
- Direction** points to the **From** header field.
- UID** points to the **x-nearenddevice** parameter in the **From** header field.

Figure 9-10 Ethereal Sniffing Tool - OK from VRSP with SDP

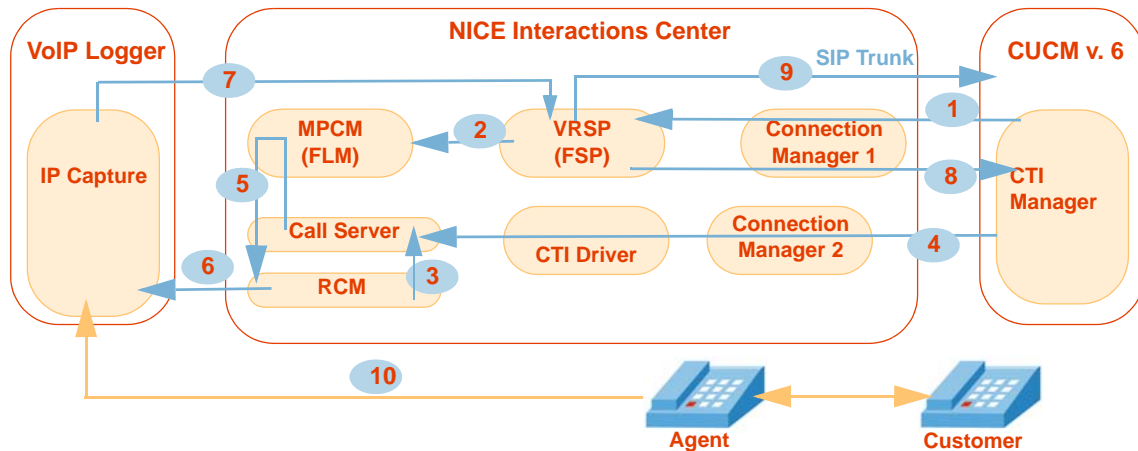
The screenshot shows the Wireshark interface with the following details:

- Filter:** sip
- Packet List:**

No.	Time	Source	Destination	Protocol	Info
329	7.144774	172.16.1.31	192.168.241.228	SIP	Status: 100 Trying
330	7.145977	172.16.1.31	192.168.241.228	SIP/SDP	Status: 200 OK, with session description
331	7.165589	192.168.241.228	172.16.1.31	SIP	Request: INVITE sip:87150@172.16.1.31:5060
- Packet Details (Frame 330):**
 - Ethernet II, Src: HewlettP_ad:26:5c (00:0e:7f:ad:26:5c), Dst: Cisco_2d:ee:00 (00:0d:66:2d:ee:00)
 - Internet Protocol, Src: 172.16.1.31 (172.16.1.31), Dst: 192.168.241.228 (192.168.241.228)
 - User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
 - Session Initiation Protocol
 - Status-Line: SIP/2.0 200 OK
 - Message-Body:
 - Connection Information (c): IN IP4 172.16.1.48
 - Time Description, active time (t): 0 0
 - Media Description, name and address (m): audio 1118 RTP/AVP 0 8 18 4 9
 - Media Type: audio
 - Media Port: 1118
 - Media Proto: RTP/AVP
 - Media Format: ITU-T G.711 PCMU
 - Media Format: ITU-T G.711 PCMA
 - Media Format: ITU-T G.729
 - Media Format: ITU-T G.723
 - Media Format: ITU-T G.722
 - Media Attribute (a): recvonly

Interaction-Based Recording Troubleshooting

Flow of Information through the Log Files



- 1 VRSP (FSP) acquires the UID, DN, Recording Mode from the CTI Manager via TAPI.
- 2 The following information is saved in the MPCM (FLM): UID, DN, VRSP URI.
- 3 The following information is delivered from the RCM to the Call Server: UID.
- 4 **Start Call** event arrives from the CTI Manager to the Call Server: a decision to record the call is being taken.
- 5 The Call Server asks the MPCM (FLM) for the VRSP URI of the UID from the **Start Call** event, and delivers it to the RCM.
- 6 The following information is delivered to the IPCapture process in the VoIP Logger: UID, DN, VRSP URI, Call ID.
- 7 The following information (**SDP**) is delivered to the VRSP (FSP): VoIP Logger IP, Ports, UID, DN.
- 8 VRSP (FSP) intrudes the call via a TAPI command to the CTI Manager.
- 9 Call start (SIP **Invite** from CUCM) and then the following information (**SDP**) is replied to the CUCM: UID, DN, VoIP Logger IP, Ports, Call ID.
- 10 **RTP** (Rx & Tx) is sent from the agent phone to the VoIP Logger.

New Call

The first Interaction-based recording scenario is described in **New Call Flow** on **page 26**. When this scenario finishes, the NICE Interactions Center, acting as Controller, contains the following information:

UID	DN	Forwarding Device
SEP1	2000	VRSP1

You can use this information for troubleshooting purposes.

RCM <> VoIP Logger <> VRSP

After **Flow of Information Between RCM, VoIP Logger, and VRSP (FSP)** on **page 27** takes place, and the VoIP Logger has sent the forwarding command to the VRSP, the VRSP (FSP) contains the following information:

Key	Call ID	SDP Value
DN@SEP	Call ID	Logger IP, Rx Port
DN@SEP	Call ID	Logger IP, Tx Port

You can use this information for troubleshooting purposes.

A

Cisco Additional Parameters

CTI Interface - Additional Switch Parameters	188
Importing Available Devices from the Switch	190
Reporting Levels	193
Connection Manager - Additional Parameters.....	195
Connection Manager - Interface Parameters	197
Driver - Additional Driver Parameters.....	199
Driver - CTI Analysis Parameters	201
Driver Interface - Additional Driver Switch Parameters	203

CTI Interface - Additional Switch Parameters

Additional Parameters for configuring the CTI Interface are located in the Additional Switch Parameters window of the CTI Interface wizard, see [Configuring the CTI Interface](#) on [page 85](#).

The following predefined additional parameters appear for the TAPI and Cisco Communications Manager switch:



NOTE: You can also create and add additional parameters by clicking **Add**.



IMPORTANT

This configuration is needed if you intend to import devices from the switch.

To set the additional switch parameters:

Figure A-1 Additional Switch Parameters Area

New Switch
Set New CTI Interface Wizard Step 2 of 3
Switch Connection And Additional Information

General Switch Info

Switch Connection Details

Additional Switch Parameters

Display ReadOnly Information Mandatory fields are marked in red ✕ ✎ Add

Name	Value
AxlIpAddress	192.168.241.27
AxlPortId	8443
AxlUserId	Cisco
AxlPassword	*****
AxlSecured	True

Description: Password for the AXL

Back Next Cancel

1. In the **Additional Switch Parameters** area, set the parameters listed in the table below.

Parameter Name	Description	Default Value
AxIIPAddress	Indicates the IP Address of the Axl server.	X.X.X.X.
AxIPortId	Indicates the Port ID of the Axl server.	*
AxIUserId	Indicates the User ID of the Axl server.	**
AxIPassword	Indicates the Password of the Axl server.	**
AxISecured	Indicates whether the connection to the Axl server is secure.	Communications Manager 5 = True Call Manager prior to 5 = False

* If this is a **secure** connection, the port number is usually either 443 or 8443. If it is a **non-secure** connection, the port number is 80.

** Contact the Cisco engineer on-site for this information, see [Defining the CUCM for Cisco IP Phone-based Active Recording](#) on [page 35](#).

2. When finished, click **Next**.

Importing Available Devices from the Switch

The following procedures are carried out to import UniqueDeviceID information for the TAPI and Cisco Unified Communications Manager switch. The imported information is used for Channel Mapping. See the *Channel Mapping* guide.



IMPORTANT

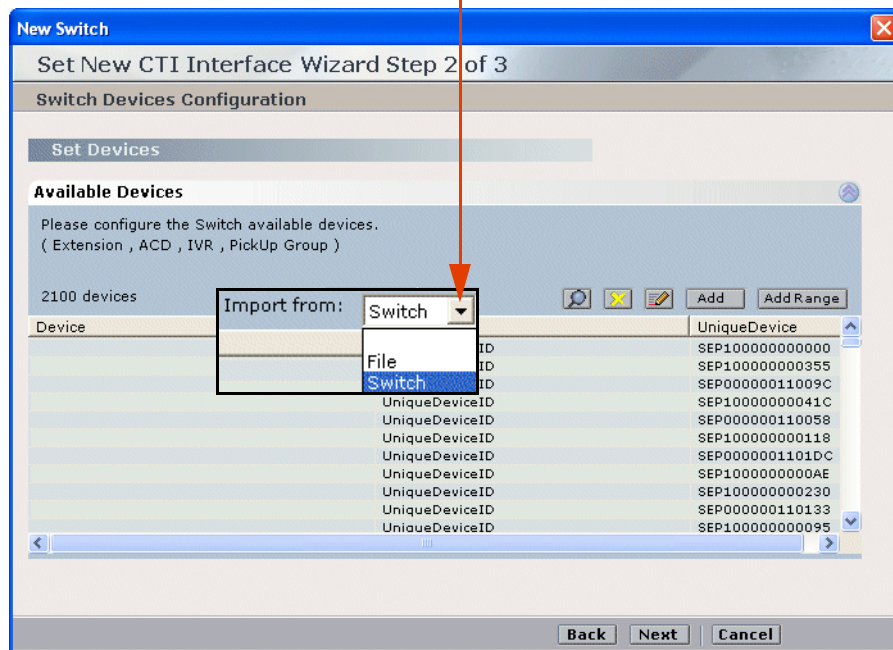
Before importing available devices, verify that you have configured the **CTI Interface - Additional Switch Parameters** on [page 188](#).

To import Available Devices from the switch:

1. Expand **Available Devices**.

Figure A-2 Set Devices Window

Click the Switch drop-down list to import all devices from the switch



2. In the **Set Devices** area, click the **Import from** drop-down list and choose **Switch**.
3. Click **Apply**. The list of devices is imported from the Switch.

Importing Text Files

You can save time when you configure your CTI Interface(s) by importing the device number and the corresponding device type from existing .txt files. For information about configuring your CTI interface, see **Configuring the CTI Interface** on **page 85**, especially the note on **page 92**.



NOTE: The file(s) must be in .txt format. If you have existing files in any other format, you must first convert them to .txt format and then perform the procedures described below.

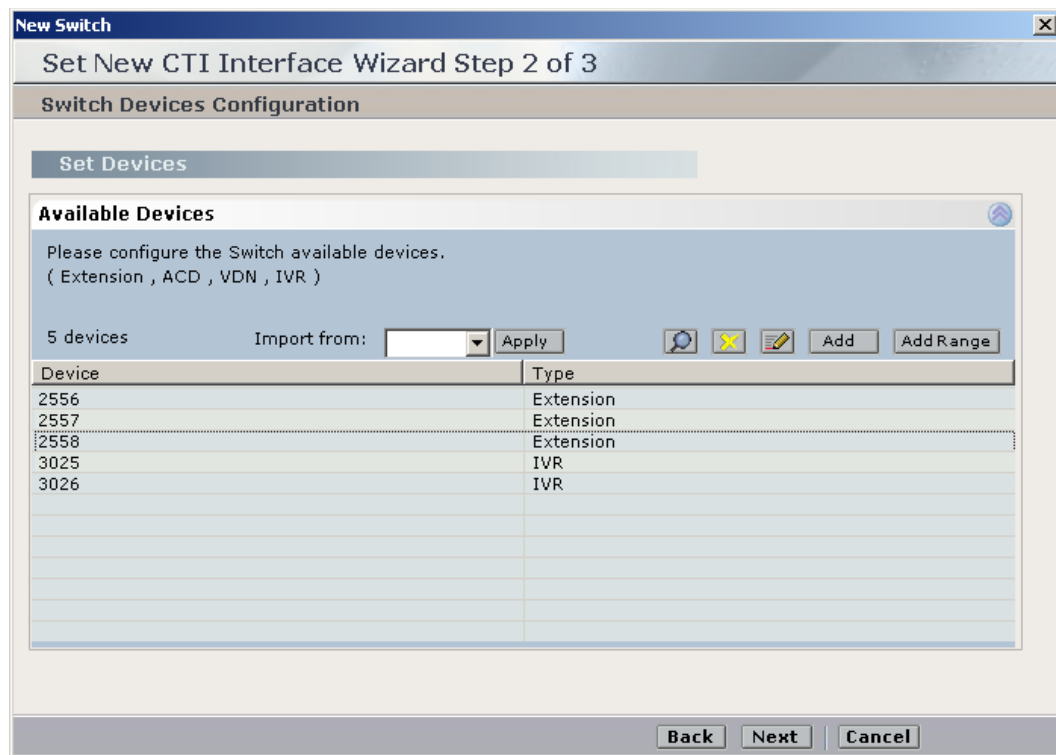
To use the import feature, the .txt file must be formatted as follows:

- Each line in the .txt file must represent one device.
- Each line must include both the device number and its corresponding device type.
- The device number and its corresponding device type must be separated by either a single space or by one tab increment.

To import text files:

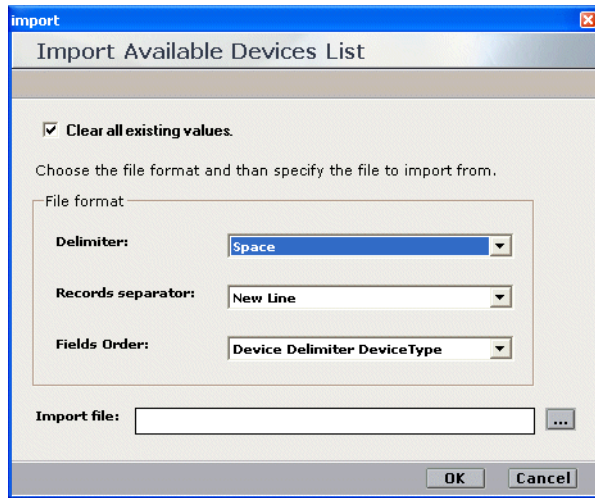
1. In the Switch Devices Configuration window, expand **Available Devices**.

Figure A-3 Switch Devices Configuration Window



2. Click the **Import from** drop-down list and choose **File**. The Import window appears.

Figure A-4 Import Window



3. If you want to overwrite **all** the devices that currently appear in the Available Devices window, mark the **Clear all existing values** checkbox.

WARNING

By default, the **Clear all existing values** checkbox is marked. **If you want to retain the devices that are currently listed in the Available Devices window, you must unmark the checkbox.**

4. In the **Delimiter** drop-down list, choose if the delimiter that separates the device number from its corresponding type is a **Space** or a **Tab** increment.
In the **Records separator** drop-down list, accept the default **New Line**.
In the **Fields order** drop-down list, choose if the order in which the device number and its corresponding type that appears in the txt file is **Device Delimiter Device Type** (that is, first the device number followed by the device type), or **Device Type Delimiter Device** (that is, first the device type followed by the device number).
5. Click the **Import File** browse button and browse to the file you want to import.
6. Click **OK**. The devices listed in the .txt file are configured into the CTI Interface.

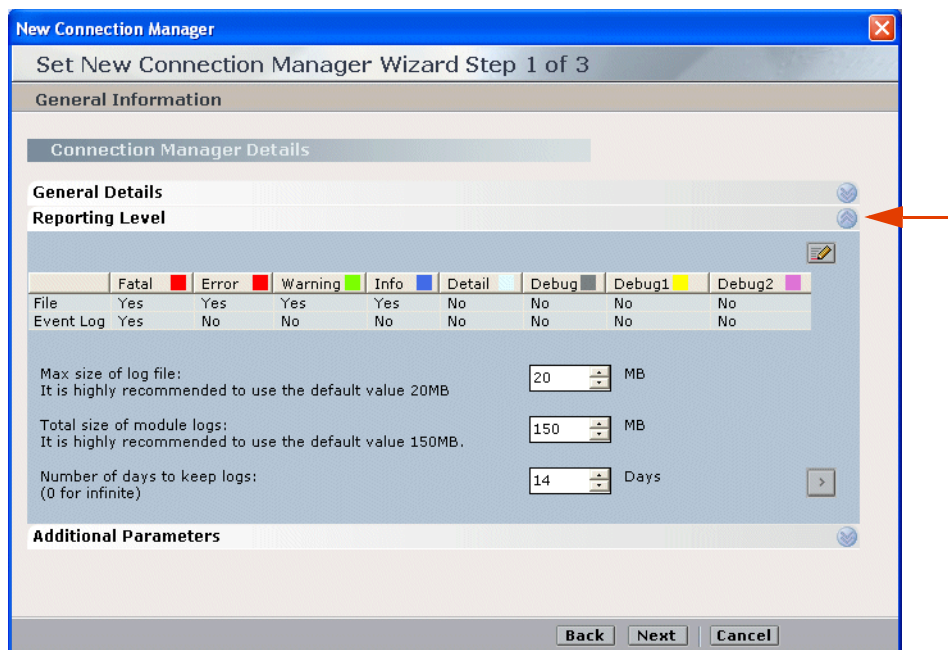
Reporting Levels

WARNING

Reporting Levels may be helpful for troubleshooting. However, making changes to the Reporting Levels can greatly add to the load on your system. Changing Reporting Levels should therefore be done **only** by authorized personnel and in conjunction with NICE Customer Support.

Reporting Levels are defined in the Connection Manager and the New Driver wizards in the General Information window, see [Configuring the Connection Manager](#) on [page 97](#) and [Configuring the Driver](#) on [page 101](#).

Figure A-5 Reporting Level Area



By default, reporting levels are defined for the following:

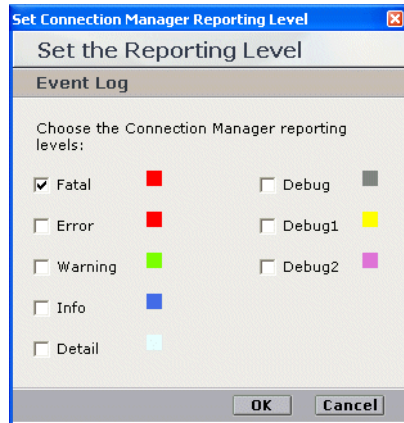
- **File** - reports to the Log file located in the Integrations installation folder
- **Event Log** - reports to the Log files located in the Event Viewer



NOTE: The Event Viewer is a Microsoft feature which can be viewed in **Control Panel > Administrative Tools**.

To define reporting levels:

1. Choose the desired row and click **Edit**. The Set Reporting Level window appears.

Figure A-6 Set Reporting Level Window

2. Mark the checkboxes for the reporting levels you want to include and click **OK**.

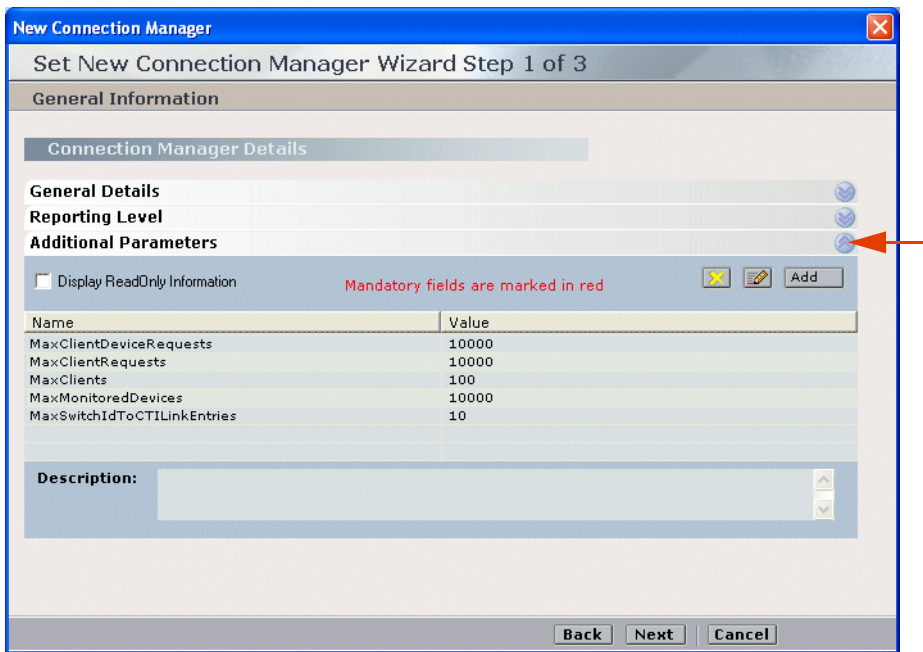
Connection Manager - Additional Parameters

WARNING

Changing parameters may have severe effects on your system. Therefore changing the Connection Manager Additional Parameters, or creating new ones, should be done **only** by authorized personnel and with authorization by NICE Customer Support.

Additional Parameters for configuring the Connection Manager are located in the Connection Manager wizard in the General Information window, see **Configuring the Connection Manager** on **page 97**.

Figure A-7 Additional Parameters Area



NOTE: The read-only parameters do not display unless you mark the **Display ReadOnly Information** checkbox.

The following predefined additional parameters appear.

Parameter Name	Description	Default Value
MaxClientDeviceRequests	Defines the maximum number of device requests Connection Manager can handle.	1000
MaxClientRequests	Defines the maximum number of client requests Connection Manager can handle.	1000
MaxClients	Defines the maximum number of clients that can be attached to Connection Manager.	100

Parameter Name	Description (Continued)	Default Value
MaxMonitoredDevices	Defines the maximum number of monitored devices up to which the Connection Manager can handle. For example, if the value is 1000 the Connection Manager can handle 999 monitored devices.	1000
MaxSwitchIdToCTILinkEntries	Defines the maximum number of CTI links Connection Manager can handle.	10

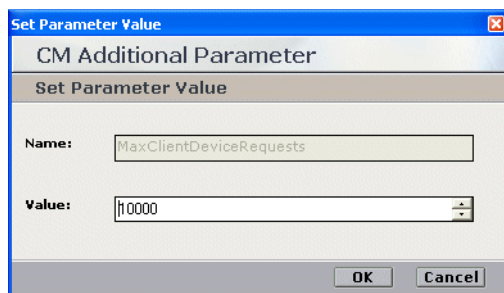


NOTE: You can also create and add additional parameters by clicking **Add**.

To change the default value:

1. Double-click the row of the relevant parameter. The CM Additional Parameter window appears.

Figure A-8 CM Additional Parameter Window



2. In the **Value** field, type the desired value and click **OK**.

Connection Manager - Interface Parameters

WARNING

Changing parameters may have severe effects on your system. Therefore changing the Connection Manager Interface Parameters, or creating new ones, should be done **only** by authorized personnel and with authorization by NICE Customer Support.

Interface parameters for the Connection Manager are located in the Connection Manager wizard in the Connection Manager Switches Information window, see **Configuring the Connection Manager** on **page 97**.

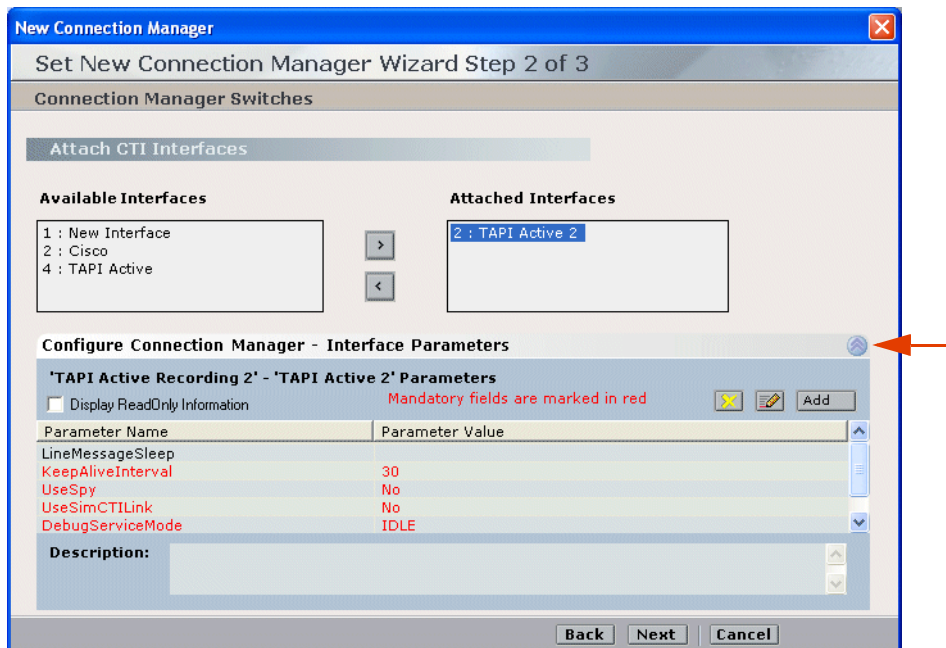
Configure Connection Manager - Interface Parameters

The Connection Manager - Interface has its own predefined parameters.



NOTE: You can also create and add additional parameters by clicking **Add**.

Figure A-9 Configure Connection Manager - Interface Parameters Area



The following predefined additional parameters appear.

Parameter Name	Description	Default Value
DllName	The name of the DLL that contains the CTI Link translator. This DLL is dynamically installed when you define a new Connection Manager.	Read-only
LineMessageSleep	The sleep interval for debug service.	
KeepAliveInterval	Defines the Keep Alive Interval time. The value is defined in seconds.	30
UseSpy*	Defines if the Connection Manager reports link events to the NICE Events Spy tool.*	No
SpyMailSlotName	Defines the name of the mailslot between the Connection Manager and the NICE Events Spy tool. IMPORTANT: Define this parameter only if you defined Yes for the UseSpy parameter.	
UseSimCTILink**	Defines if the Connection Manager uses the SimCTILink tool to read events.**	No
SimMailSlotName	Defines the name of the SIM mailslot between the Connection Manager and the Spy tool. IMPORTANT: Define this parameter only if you defined Yes for the UseSimCTILink parameter.	

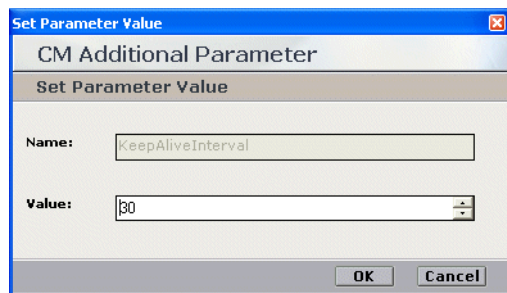
* For details, see [NICE Events Spy](#) on [page 142](#).

** For details, see [Setting up the SimCTILink Tool](#) on [page 146](#).

To change the default value:

1. Double-click the row of the relevant parameter. The CM Additional Parameter window appears.

Figure A-10 CM Additional Parameter Window



2. In the **Value** field, type the desired value and click **OK**.

Driver - Additional Driver Parameters

WARNING

Changing parameters may have severe effects on your system. Therefore changing the Driver Additional Parameters, or creating new ones, should be done **only** by authorized personnel and with authorization by NICE Customer Support.

Additional parameters for configuring the Driver are located in the New Driver wizard in the General Information window, see [Configuring the Driver](#) on [page 101](#).

Figure A-11 Additional Driver Parameters Area

The screenshot shows the 'New Driver' wizard, Step 1 of 3, titled 'Set New Driver Wizard Step 1 of 3'. The 'General Information' section is expanded to show 'Driver General Information'. Under 'Additional Driver Parameters', there is a checkbox for 'Display ReadOnly Information' and a red note: 'Mandatory fields are marked in red'. An 'Add' button is visible. Below this is a table of parameters:

Parameter Name	Parameter Value
MaxCapiCommandRetries	4
MaxNumberOfCalls	5000
CAPISpyServerPort	7002
CAPISpyMessageQueueSize	50
NotifyFailoverOnAllCLSFailureOnly	No
DelayBetweenStartFailedLinksInSeconds	30
MaxCallDurationSec	18000

Below the table is a 'Description:' field and 'CtiAnalysis Parameters' section. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

The following predefined additional parameters appear.



NOTE: You can also create and add additional parameters by clicking **Add**.

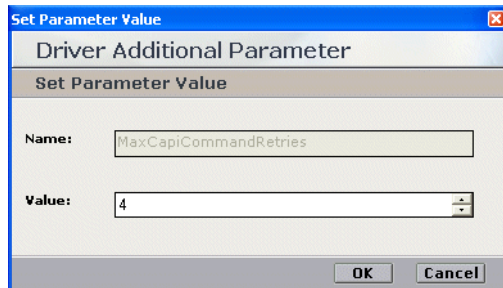
Parameter Name	Description	Default Value
MaxCapiCommandRetries	Defines the number of times the driver attempts to send a command to the CAPI following a failure.	4
MaxNumberOfCalls	Defines the maximum number of calls in the concurrent calls buffer.	5000
CAPISpyServerPort	Defines the port to which the CAPI spy application connects.	7002
CAPISpyMessageQueueSize	Size of the message queue in the CAPI Spy server.	50

Parameter Name	Description (Continued)	Default Value
UseEventDB	Defines if the driver uses the EventDB database for CTI Analysis.	No
DelayBetweenStartFailed LinksInSeconds	Defines the amount of time before the driver reconnects to the CTI link following a failure. The value is defined in seconds.	30
MaxCallDurationSec	Defines the maximum time the driver allows a call to last until it is automatically disconnected. The value is defined in seconds.	7200
UseCTIAnalysis	Defines if CTIA is in use in the driver.	No
CallTableHost	Host name of the Call Table.	localhost
CallTablePort	Port number of the Call Table.	7272
AlwaysConnectToLocalCLS	Defines if the driver always connects to the NICE Interactions Center on the local machine regardless of the NICE Interactions Center's real address. Useful when working with CLS as a cluster.	No

To change the default value:

1. Double-click the row of the relevant parameter. The Driver Additional Parameter window appears.

Figure A-12 Driver Additional Parameter Window



2. In the **Value** field, type the desired value and click **OK**.

Driver - CTI Analysis Parameters

WARNING

Changing parameters may have severe effects on your system. Therefore changing the Driver CTI Analysis Parameters, or creating new ones, should be done **only** by authorized personnel and with authorization by NICE Customer Support.

CTI Analysis parameters for configuring the Driver are located in the Driver wizard in the General Information window, see [Configuring the Driver](#) on page 101.

Figure A-13 CTI Analysis Parameters Area

The screenshot shows the 'New Driver' wizard window, titled 'Set New Driver Wizard Step 1 of 3'. The 'General Information' section is expanded to show 'CtiAnalysis Parameters'. A checkbox labeled 'Check the box if using CTI Analysis' is checked. Below it is a table with two columns: 'Parameter Name' and 'Parameter Value'. The table contains the following entries:

Parameter Name	Parameter Value
HostName	localhost
Port	4003
NumberOfCompoundsToBulk	50
TimeOutToPerformBulkInsert	600000
SQLTimeoutForBulkInsert	60
DBFileSizePrecentAlarm	95
DBTransactionLogSizeAlarm	95

At the bottom of the wizard, there are 'Back', 'Next', and 'Cancel' buttons.

The following predefined CTI Analysis parameters appear.



NOTE: You can also create and add additional parameters by clicking **Add**.

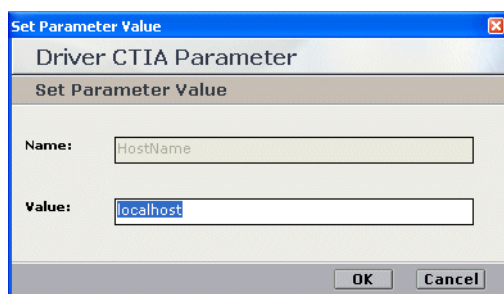
Parameter Name	Description	Default Value
HostName	Host name for the Analyzer server.	localhost
Port	Port for the Analyzer server.	4003
NumberOfCompoundsToBulk	Defines the number of compounds to bulk insert on each set.	50
TimeOutToPerformBulkInsert	Defines the number of milliseconds as timeout to perform bulk insert.	600000
SQLTimeoutForBulkInsert	Defines the number of seconds as SQL timeout for bulk insert.	60

Parameter Name	Description (Continued)	Default Value
DBFileSizePrecentAlarm	Defines the warning percentage size of the nice_cti_analysis database file. When this size is reached, an alarm is sent.	95
DBTransactionLogSizeAlarm	Defines the warning percentage size of the nice_cti_analysis transaction log file. When this size is reached, an alarm is sent.	95
DBFileSizesMonitorInterval	Defines the interval time (in minutes) to monitor the database file sizes.	10

To change the default value:

1. Double-click the row of the relevant parameter. The Driver CTIA Parameter window appears.

Figure A-14 Driver CTIA Parameter Window



2. In the **Value** field, type the desired value and click **OK**.

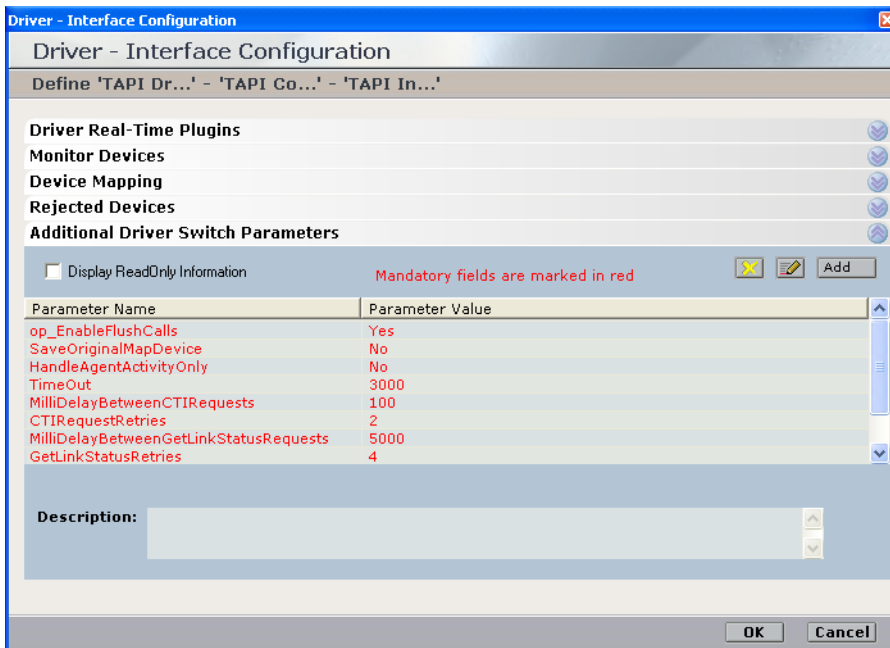
Driver Interface - Additional Driver Switch Parameters

WARNING

Changing parameters may have severe effects on your system. Therefore changing the Additional Driver Switch Parameters, or creating new ones, should be done **only** by authorized personnel and with authorization by NICE Customer Support.

Additional Parameters for configuring the Driver Interface are located in the Driver wizard in the Driver Interface Configuration window, see [Configuring the Driver](#) on [page 101](#).

Figure A-15 Additional Driver Switch Parameters Area



The following predefined additional parameters appear.



NOTE: You can also create and add additional parameters by clicking **Add**.

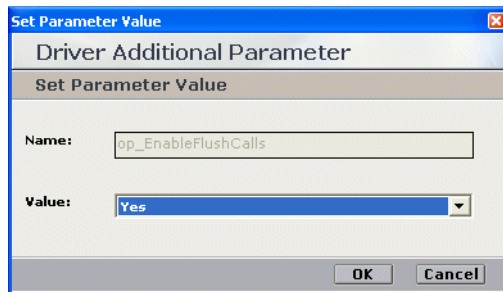
Parameter Name	Description	Default Value
op_EnableFlushCalls	Defines if the driver flushes open calls when initializing connection.	Yes
SaveOriginalMapDevice	Defines if the driver reports to the source device.	No
HandleAgentActivityOnly	Defines if the driver handles login/logout events only from this link. Note: This parameter is NOT used in the ICM integration.	No
TimeOut	Defines the response time for a request. The value is defined in milliseconds.	3000

Parameter Name	Description (Continued)	Default Value
MilliDelayBetweenCTIRequests	Defines the waiting time between CTI requests. The value is defined in milliseconds.	100
CTIRequestsRetries	Defines the number of times the CTI tries to request events for Query and Monitor devices.	2
MilliDelayBetweenGetLinkStatusRequests	Defines the waiting time between "Get Link Status" requests. The value is defined in milliseconds.	5000
GetLinkStatusRetries	Defines the number of times "Get Link Status" requests can be made.	4
FailedMonitoredThreadMinutesDelay	Defines the waiting time before reactivating a thread to monitor devices that the link had previously failed to monitor. The value is defined in minutes.	10

To change the default value:

1. Double-click the row of the relevant parameter. The Driver Additional Parameter window appears.

Figure A-16 Driver Additional Parameter Window



2. In the **Value** field, type the desired value and click **OK**.

Defining an AXL - Application User

You can facilitate your channel mapping by configuring an AXL application user in the CUCM. The AXL application user enables the importing of all Unique Device IDs from the Call Manager (i.e. you import the Unique Device IDs straight from the switch).



IMPORTANT

A Cisco System Administrator must perform the CUCM configuration!

If you are configuring Cisco's IP Phone based Active Recording, you cannot use Secured Connections.

The AXL client does not look at which devices are attached to which TSP client. If you have several TSP clients and different devices are attached to each one, AXL ignores this and only looks at the devices that are attached to the switch.

The AXL client needs to be connected to the CUCM. To connect it, you define it as a user in the CUCM. The procedures you follow to make this definition depends on the version of the CUCM you are using.



NOTE: You use the user and password that you create here when configuring the CTI interface, see [CTI Interface - Additional Switch Parameters](#) on [page 188](#).

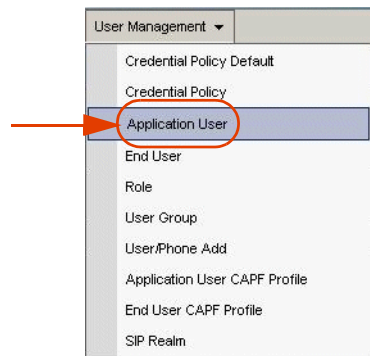
For version 5x and 6x:

The user must be an **Application User**. Permissions can be limited to **AXL Service** access, see [To define an application user:](#) on [page 205](#).

To define an application user:

1. Log in to the CUCM Administration application.
2. From the **User Management** menu, choose **Application User**.

Figure B-1 Choosing Application User



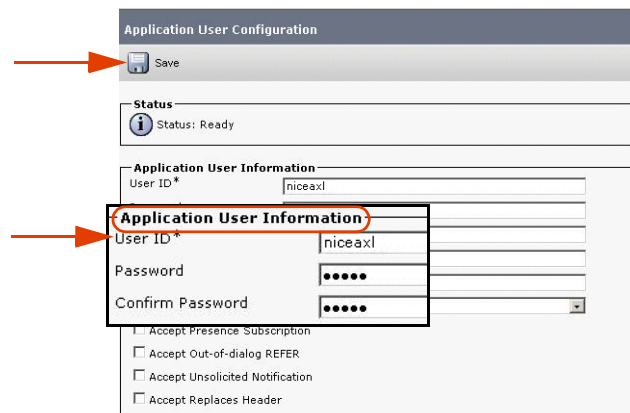
The Find and List Application Users window appears.

Figure B-2 Find and List Application Users Window



a. Click **Add New**. The Application User Configuration window appears.

Figure B-3 Application User Configuration Window



b. In the **Application User Information** area:

- In the **User ID** field, type **niceaxl**.

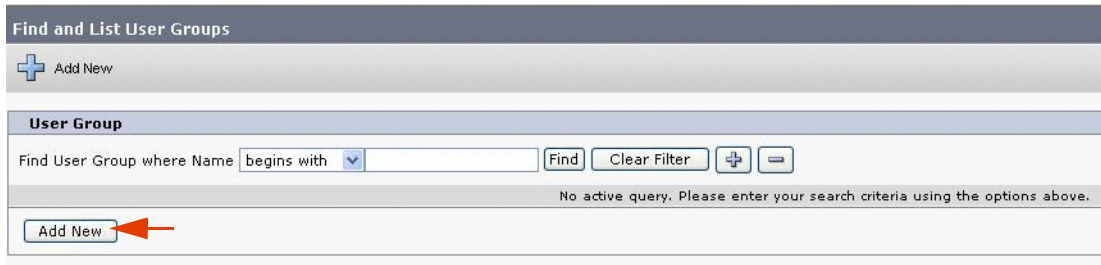
- In the **Password** field, type the password.



NOTE: Save this user ID and password in a safe place. You need it later when configuring AXL for NICE Perform, see **CTI Interface - Additional Switch Parameters** on **page 188**.

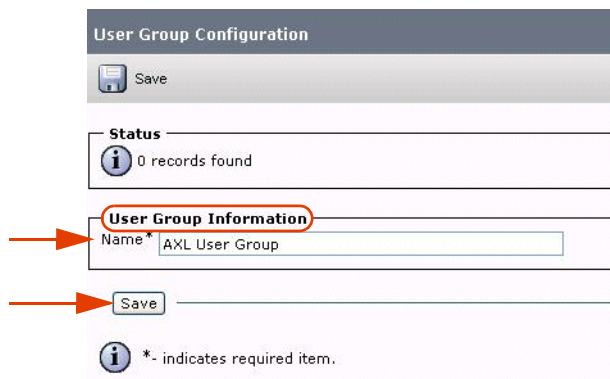
- c. Click **Save**.
3. From the **User Management** menu, choose **User Group**. The Find and List User Groups window appears.

Figure B-4 Find and List User Groups



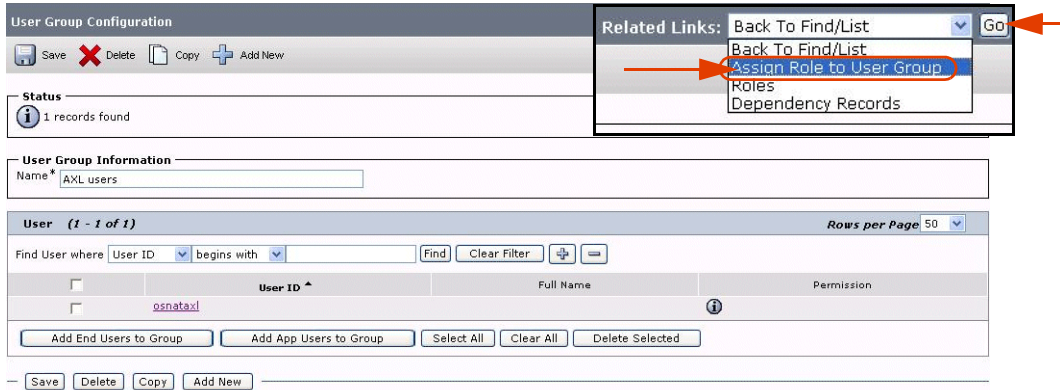
- a. Click **Add New** group. The User Group Configuration window appears.

Figure B-5 User Group Configuration Window



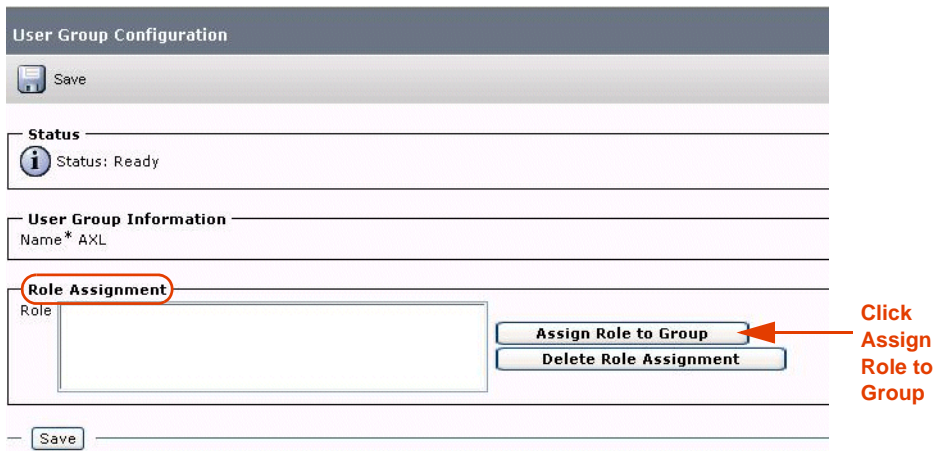
- b. In the **User Group Information** area, in the **Name** field, type the user group name.
- c. Click **Save**.

Figure B-6 User Group Configuration Window



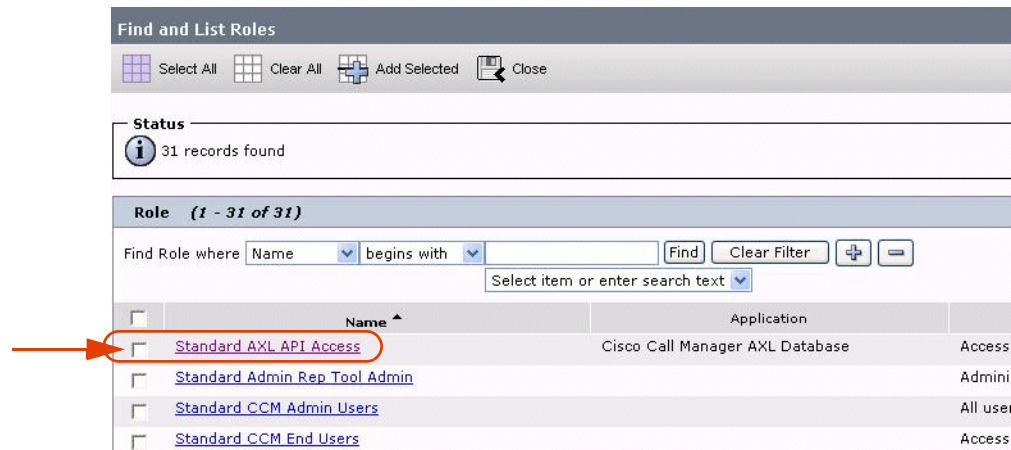
4. Click the **Related Links** drop-down list and choose **Assign Role to User Group**.
5. Click **Go**. The **Role Assignment** area appears.

Figure B-7 User Group Configuration Window - Role Assignment Area



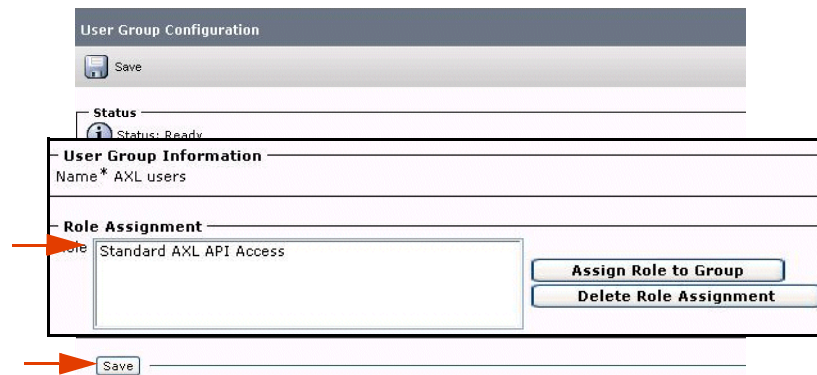
- a. In the **Role Assignment** area, click **Assign Role to Group**.
- b. Click **Find**. The Find and List Application Users Groups window appears with a list of roles.

Figure B-8 Find and List Roles Window



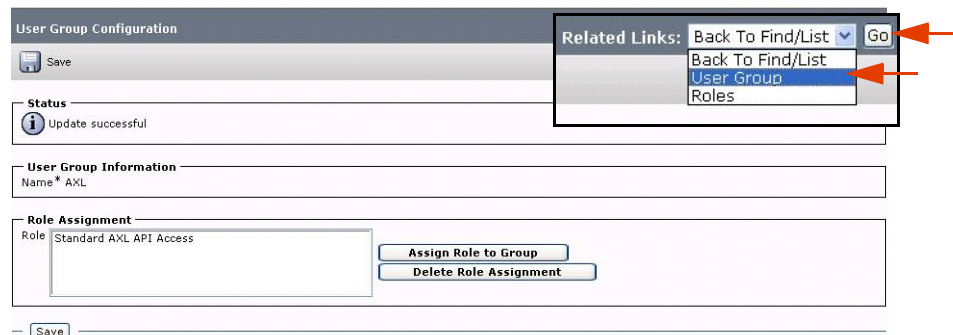
- c. Select **Standard AXL API Access**.
- d. Click **Add Selected**. In the **Role Assignment** list, the new role and the **Status: Update is successful** appears.

Figure B-9 User Group Configuration Window



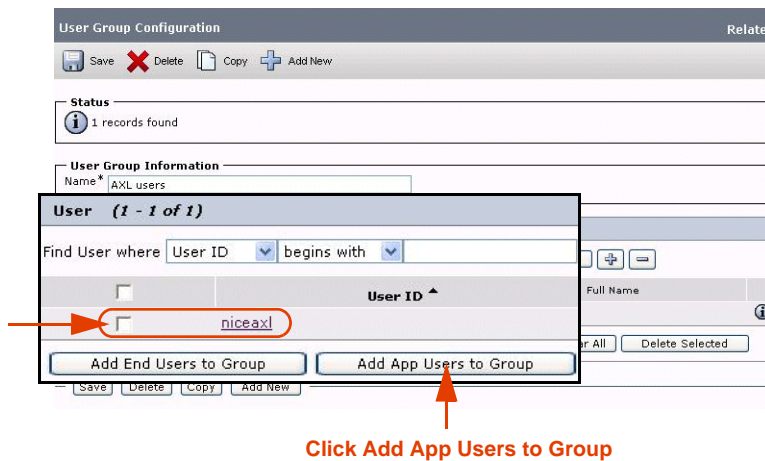
- e. Click **Save**.

Figure B-10 Related Links Drop-down List



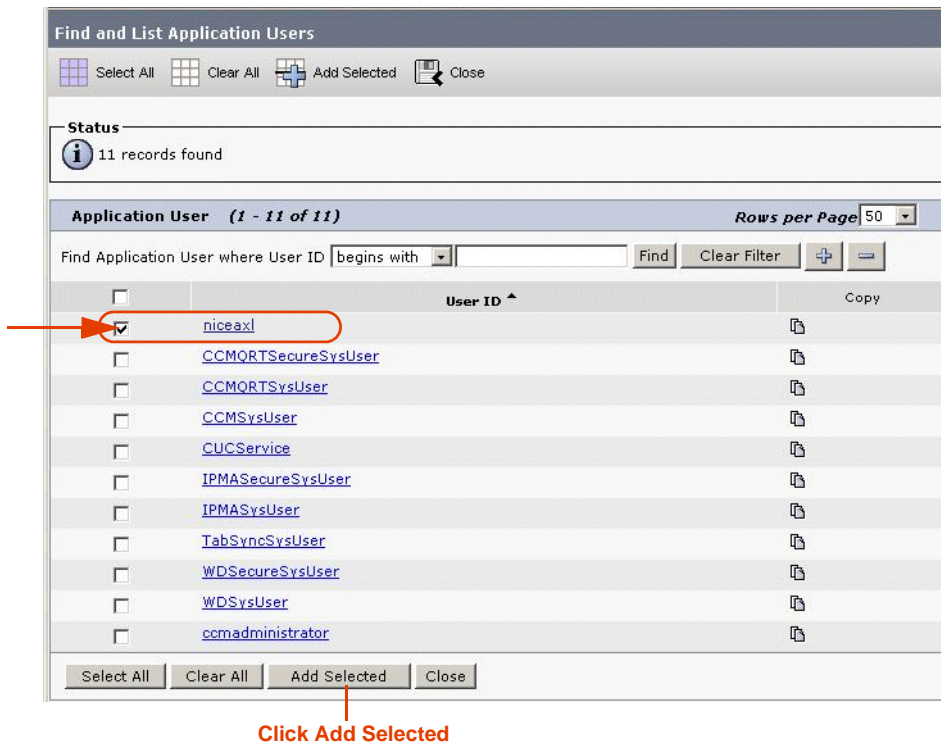
- f. From the **Related Links** drop-down list, choose **User Groups** and click **Go**. The User Group Configuration window appears.

Figure B-11 User Group Configuration Window



6. Click **Add App Users to Group**. The Find and List Application Users window appears.

Figure B-12 Find and List Application Users Window



- a. In the **Search Results** list, mark the new **AXL user** (**niceaxl**) that you created.
- b. Click **Add Selected**. In the **User Group Information** area, the AXL user appears in the **User In Group** list.
- c. Click **Save**.

Channel Mapping Guidelines

When configuring Cisco Active IP Phone-based channel mapping, use the following guidelines:

- For static device mapping, map all channels to **Unique Device IDs**.
- For dynamic device mapping, map a pool of channels to a pool of **Unique Device IDs**.
- For Interaction-based recording, mark **Observation by Call + Device (FSP)**.
- For monitored shared lines that need to be recorded, map all the devices that share this line by mapping the SEP (MAC address) of each device that you are sharing.



IMPORTANT

Click the **Recording Type** drop-down list and choose **Active VoIP**.

Channels can be configured as either **Total** or **Interaction-based**.

Total recording channels cannot be associated with Device Numbers that are configured to work in **Application Invocation** (Interaction-based) mode.



NOTE: You can facilitate your channel mapping by configuring an AXL application user in the CUCM, see **Defining an AXL - Application User** on **page 205**.

For detailed information regarding Device Mapping and Channel Mapping, see the *NICE Perform Release 3 Channel Mapping Guide*.

Blank page for double-sided printing.

Index

A

ACD

- adding device **93**
- adding range of devices **94**
- explanation **13**

additional parameters

- Connection Manager **195, 197**
- CTI interface **188**
- driver interface **203**
- switch driver **199**

AXL **13**

- defining Application User **205**
- ports **188**

B

- Built In Bridge (BIB), configuring **46**

C

Channel Mapping **91**

- guidelines **101**

channel mapping

- defining an AXL user **205**

Cisco

- IP Phone **19**
- Softphone **19**

Cisco Unified Communications Manager

- configuration information **82**
- configuring the CTI interface **85**

Codec sets **182**

Connection Manager

- additional parameters **195, 197**
- attaching CTI Interfaces **112**
- attaching CTI interfaces **99**
- configuration prerequisites **83**
- configuration wizard **97**

CTI Interface

- adding devices **92**
- additional parameters **188**
- configuration prerequisites **82**
- configuration wizard **85**
- importing text files **191**

CTI Manager

- system architecture **18**

CTI port

- adding device **93**
- adding range of devices **94**
- explanation **13**
- monitoring devices **96**

CTI Route Point

- explanation **13**

D

Destination Port **37**

driver

- attaching CLS **103, 104**
- configuration prerequisites **83**
- configuration wizard **101**
- defining monitor devices **106**

driver interface

- additional parameters **203**

E

End User

- associating User Groups **33**
- defining **30**

Ethereal Sniffing Tool **183**

Events **142**

Events Spy

- defining SpyMailSlot Name parameter **143**
- defining the UseSpy parameter **143**
- sending events **146**

Extension mobility **67**

- guidelines **101**
- monitoring devices **107**
- switch side **32**

F

FLM **13**

FLM, see MPCM (FLM)

FSP **13**

G

Glossary **16**

H

hunt group

- adding device **93**
- adding range of devices **94**
- explanation **13**

I

- Integration
 - installation **121, 137**
- Interaction-based recording
 - flow of information log files **185**
- IP Capture **13**
- IP Phone

- BIB, configuring **46**

IVR

- adding device **93**
- adding range of devices **94**
- explanation **14**
- monitoring devices **96**

L

- Log Files
 - Call Server **179**
 - CUCM SIP invite **178**
 - flow of information - interaction-based recording **185**
 - flow of information - total recording **176**
 - IP Capture tool **181**
 - MPCM (FLM) **177**
 - RCM **179**
 - VRSP (FSP) **177, 181, 182**

M

- Mirroring **14**
- MPCM
 - explanation **14**
- MPCM (FLM) **19**
 - Installing and configuring **69**

N

- ne **13**
- New Route List, defining **42**
- New Route Pattern, defining **44**
- NICE Events Spy
 - setting up the SimCTILink tool **146**
- nicecti User
 - defining in CUCM **30**
- Notification Tones
 - defining **52**
 - defining on Device level **54**
 - defining on system wide level **52**

P

- Phone Device

- Beep Tones, configuring **52**

- Pickup group
 - adding device **93**
 - adding range of devices **94**
 - explanation **14**
- Pickup groups
 - monitoring devices **96**
- ports selection
 - configuring on SIP Logger **79**

R

- Recording Method, selecting **50**
- Recording Profile, associating with Recorded Device Number **50**
- Recording Profile, defining **38**
- Redundancy, system architecture **19**
- reporting levels
 - defining **193**
- Route Group, defining **40**

S

- Shared lines **14**
- shared lines
 - monitoring **211**
- SimCTILink tool **146**
- SIP Trunk, defining **35**
- SPAN **14**
- SpyMailSlot Name parameter **143**
- switch driver
 - additional parameters **199**
- System architecture
 - redundant **19**
- system architecture **18**

T

- TAPIMonitor **67**
- Terms and Concepts **13**
- text files
 - importing **191**
- Total recording
 - flow of information through log files **176**
- Troubleshooting
 - TAPI **174**
 - Total recording **176**
 - VRSP (FSP) **175**
 - VRSP error codes **175**
 - VRSP log files **175**
 - VRSP SNMP messages **175**
- TSAPI Ports **83**

U

- UseSpy parameter **143**

V

version

 Cisco TSP Client **58**

 VRSP (FSP) **19**

 configuring for redundancy **135**

 redundancy **134**

 requirements **134**