



CISCO/CTI

Active IP Recording

INTEGRATION MANUAL

CT Recording System 5.3 (and higher)

Version: 2.0
Date: 16-12-2009
Reference: CT-R5-CTI-CIS-LB



Copyright © 2009 by CyberTech International

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without prior written consent of CyberTech International.

Trademark Acknowledgements

Cisco Systems, the Cisco logo, and the Cisco Systems logo are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation in the United States and other countries.

Microsoft, Windows, Windows Server, and Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

JavaScript is a trademark of Sun Microsystems, Inc.

Table of Contents

1	Introduction	7
1.1	About this Manual.....	7
1.2	Scope.....	7
1.2.1	Recording Methods.....	7
1.2.2	CyberTech Recording System.....	7
1.2.3	Cisco Software	7
1.2.4	Cisco Active IP Installer Kit.....	8
1.3	Intended Audience	8
1.4	Assumptions	8
1.5	Conditions for Installation	8
1.6	Reference Manuals	8
1.7	Conventions and Symbols.....	9
2	Safety	11
2.1	General Safety Rules	11
2.2	ESD Precautions.....	11
3	Requirements and Supported Items	13
3.1	General Requirements for Cisco Components	13
3.2	General Requirements for CyberTech Components.....	13
3.2.1	Operating Systems	13
3.2.2	Workstation	13
3.3	Cisco/CTI Active IP Recording.....	14
3.4	Supported Items	15
3.4.1	Features.....	15
3.4.2	Target Types.....	16
3.4.3	Extrafields / Cisco Call Data	16
3.4.4	Call Scenarios.....	17
3.4.5	Phone Types.....	18
3.4.6	Codecs.....	18
4	System Description	19
4.1	Cisco system elements.....	19

4.2	CyberTech Configuration Types.....	20
4.2.1	Configuration 1 (1-128 channels)	20
4.2.2	Configuration 2 (1-168 channels)	21
4.2.3	Configuration 3 (1-168+ channels)	21
4.3	Hardware Requirements.....	22
4.3.1	Configuration 1 (1-128 channels)	22
4.3.2	Configuration 2 (1-168 channels)	23
4.3.3	Configuration 3 (1-168+ channels)	23
4.4	Software Requirements.....	25
4.4.1	CTI Server.....	25
4.4.2	Core Server	25
4.4.3	Satellite	25
5	Prerequisites	27
5.1	Customer Prerequisites.....	28
5.2	Cisco Prerequisites	28
5.3	CyberTech Prerequisites	28
5.3.1	Preconditions.....	29
5.3.2	Preparatory Steps	29
5.4	Installing Parrot-DSC Firmware	30
5.5	Licensing	32
5.5.1	Cisco Licensing	32
5.5.2	CyberTech Licensing.....	32
5.5.3	Loading License Information	32
5.6	Adding Cisco Call Data (Extrafields)	35
5.7	Updating the File CTI_receiver.exe	36
6	Installation	41
6.1	Installing the CT Cisco CTI Integration Software	41
6.1.1	Configuration with Dedicated CTI Server	42
6.1.2	Stand-alone Installation.....	46
6.2	Post Installation Copying	48
6.3	Setting Up the Secure SIP Trunk	48
6.3.1	Download Certificate	49
6.3.2	Generate Certificates.....	49
6.3.3	Load Certificate in CUCM.....	50

6.3.4	Install Certificates on SIP Server System	50
6.3.5	Configuring the SIP Server	62
6.3.6	Configure the CUCM	63
7	Configuration	65
7.1	Linking Targets to Users.....	65
7.2	Logging On to the CT Web GUI.....	65
7.3	Defining Channel Groups.....	67
7.4	Configuring the Cisco Link Controllers	69
7.5	Defining Targets.....	73
7.5.1	Adding a New Target	73
7.5.2	Monitoring Target States.....	75
7.6	Specifying Cisco Call Data	76
Appendix A	Abbreviations and Terms.....	81
A.1	Abbreviations.....	81
A.2	Terminology.....	82
Appendix B	Quick Install Reference	83
Appendix C	Cisco Configuration Settings	85
C.1	CUCM Configuration Checklist	85
C.1.1	Generic Steps (part 1).....	85
C.1.2	Normal Use of the SIP Trunk Link	85
C.1.3	Use with Secure SIP	86
C.1.4	Generic Steps (part 2).....	86
C.2	Open Port Configuration	87
Appendix D	Troubleshooting	89

<BLANK PAGE>

1 Introduction

1.1 About this Manual

This document describes the prerequisites and procedures for the installation, configuration, and testing of the CyberTech Recording System 5.3 (or higher) on the Cisco Active IP Recording System

In the Cisco Active IP recording system, calls are duplicated from the extension and streamed via the Cisco PBX to the recording system. These duplicated audio stream sessions are initiated by Cisco 3rd generation phones with 'Built-in-Bridge' (BIB).

Call details are read from the Cisco JTAPI interface which is used for the Cisco recording facility. The JTAPI interface also initiates recording start.

1.2 Scope

The Cisco/CTI integration as described in this manual is restricted to specific recording methods and software versions. They are described below.

1.2.1 Recording Methods

The Cisco/CTI integration supports Active IP Recording as recording method.

1.2.2 CyberTech Recording System

The Cisco/CTI integration works in conjunction with the following versions of the CTRS (CyberTech Recording System):

- Version 5.4
- Version 5.3 with Service Repair 5.3.2



Please verify the correct versions (and the applicable Service Repair) of the CT Recording System with your CT contact person (consult Appendix D 'Troubleshooting' for contact details).

1.2.3 Cisco Software

The Cisco/CTI integration as described in this manual supports **Cisco Unified Call Manager (CUCM) version 6.1.2 or higher**. Exclusive support of CUCM version 7 will be mentioned where applicable.

1.2.4 Cisco Active IP Installer Kit

Installation of the CT Cisco CTI Integration Software as described in this manual is supported by version **3.2** of the '**Cisco Active IP**' installer kit.



When you want to upgrade from installer kit 3.1.x, contact your CT contact person about the specific procedure to follow (consult Appendix D 'Troubleshooting' for contact details).

1.3 Intended Audience

This manual is aimed at personnel – usually installation engineers – responsible for connecting the CyberTech Recording System 5.3 (or higher) with the Cisco Active IP Recording system.

1.4 Assumptions

It is assumed that the reader has knowledge about the following:

- CyberTech Recording System:
 - Version 5.4 or higher
 - Version 5.3 with Service Repair 5.3.2
- CyberTech CTI Integration

1.5 Conditions for Installation



The following conditions are essential for a successful progress of the Cisco/CTI integration process:

- During the installation process, presence of a Cisco qualified engineer is required.
- To ensure successful installation, the procedures as described in this manual must be executed by engineers who are trained by CyberTech.

1.6 Reference Manuals

Consult the following manuals for details about the installation and use of the CyberTech Recording System 5.3 (or higher).

Manual	Contents	Version
CT Recording Solutions R5 - Installation Manual	Installation and configuration procedures of the CyberTech Recording System software	5.5
CT Recording Solutions R5 - CTI Manual	Installation and configuration procedures of the CTI Server	1.10

Manual	Contents	Version
CT Recording Solutions R5 – User Manual	System configuration information for the system administrator	5.7
CT Recording Solutions R5 – Maintenance Manual	System maintenance information, VoIP installation	5.7
CT Recording Solutions R5 – OS Hardening Manual	OS hardening options and policies	5.4
Parrot-DSC-MOD-PCI Installation Manual	Installation procedures of the interface cards in the voice recorder	3.4c

Table 1: CyberTech manuals



The manual version shown in the Version column is the version minimally required. Higher versions may also be applicable.



Consult the CyberTech Recording Software CD or go to the website www.cybertech-int.com (login required) for the latest CyberTech manual versions.

1.7 Conventions and Symbols

The following guidelines apply to this manual:

- The name '**Monitor Tool**' is used as a shorter name for 'CT Recording Solutions Monitor'.
- The name '**Programmer**' is used as a shorter name for 'Parrot DSC API Flash Programmer'
- The **Warning symbol** in the left margin is used to emphasise system-critical information.
- The **Information symbol** in the left margin is used to indicate a general remark or a reference to another document.



<BLANK PAGE>

2 Safety

This chapter describes the general safety rules and specific ESD precautions to be taken into account.

2.1 General Safety Rules

Primarily, it is important to adhere to the regulations as dictated by the local authorities or company standards.

Because the hardware components are supplied by Cisco, CyberTech, and one or more third parties, please refer to the respective installation manual(s) for specific safety and security guidelines when installing the individual components.

2.2 ESD Precautions

All ICs and many other electronic components are susceptible to electrostatic discharges (ESD). ESD can cause instant failures, but can also drastically limit the life span of the affected part and cause unexplainable behaviour of the equipment.

When handling printed circuit boards always take the following preventive measures:

- Keep printed circuit boards as long as possible in their protective bags.
- Use an anti-ESD bracelet. The sign on the left of this block of text indicates when ESD-protective measures are required.



<BLANK PAGE>

3 Requirements and Supported Items

This chapter covers the following topics:

- The *general* Cisco and CyberTech requirements for installation and configuration of the Cisco/CTI Recording Solution.
- Characteristics and requirements of the Cisco/CTI Active IP Recording method.
- An overview of supported system items in the Cisco/CTI Recording Solution. For example: features, target types, and call scenarios.

3.1 General Requirements for Cisco Components

For Cisco hardware/software requirements please refer to the requirements as prescribed by Cisco Systems, Inc.

3.2 General Requirements for CyberTech Components

This section describes the *general* software and workstation requirements for the CyberTech recording components. (Consult chapter 4 'System Description' for the *specific* CyberTech requirements.)

3.2.1 Operating Systems

The following operating systems are supported:

- Windows Server 2003 Web Edition
- Windows Server 2003 Standard Edition (R2)
- Windows Server 2003 Enterprise Edition (R2)



Please note that non-supported operating systems may cause system instability and/or poor system performance. If so, CyberTech cannot be held responsible for malfunctioning.

3.2.2 Workstation

The client's workstation requires the following to run the CyberTech Web GUI (see chapter 7 'Configuration' for details):

- Microsoft Internet Explorer 6.0 with JavaScript enabled
- Minimum screen resolution of 1024x768 for correct display

3.3 Cisco/CTI Active IP Recording

The Cisco/CTI Recording Solution supports Active IP Recording. The figure below visualises the corresponding call and audio flows.

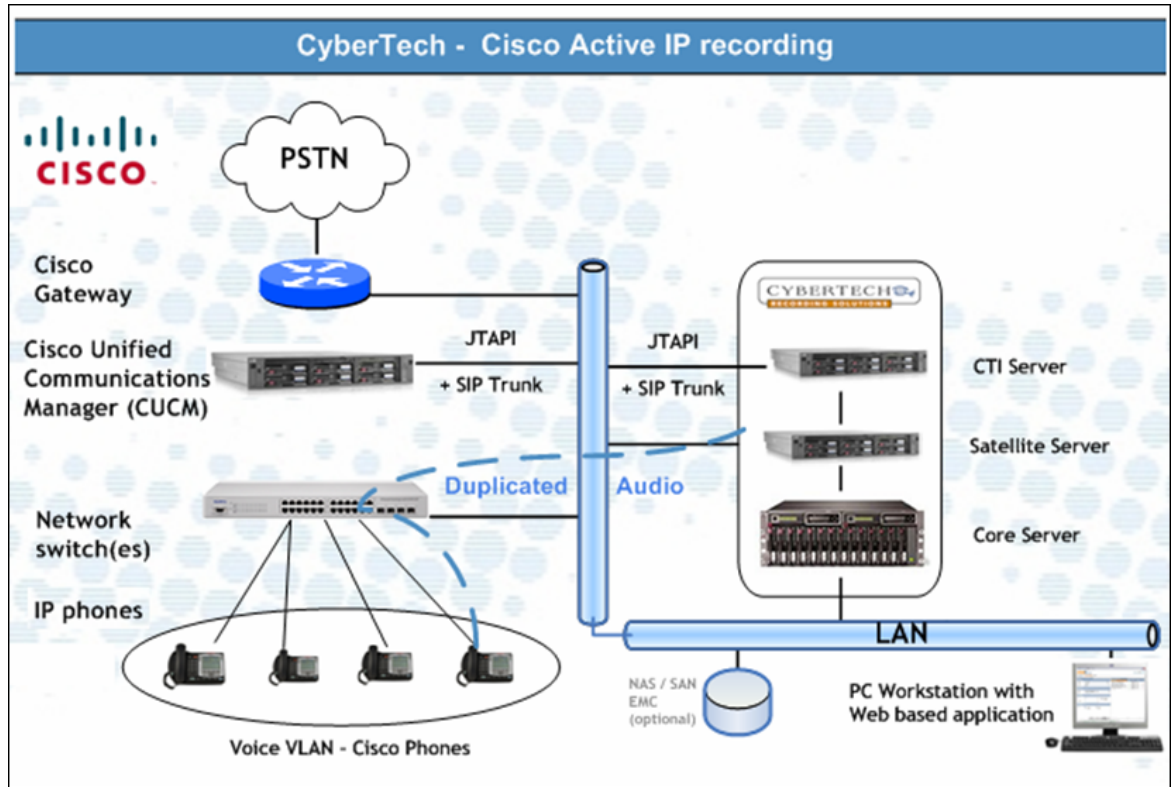


Figure 1: Cisco/CTI Active IP Recording

Call data is transferred to the CTI server via the Cisco JTAPI Server.

In Cisco/CTI Active IP Recording:

- Calls are duplicated from the extension and streamed via a SIP Trunk actively terminated at the recording system.
- Call details are read from the JTAPI interface which connects the CUCM with the CyberTech CTI Server. The JTAPI connection is used for the Cisco recording facility.
- The duplicated audio stream sessions are initiated by the Cisco 3rd generation phones with 'Built-in-Bridge' (BIB).

3.4 Supported Items

This section describes the items that are supported by the Cisco CTI-based Recording System. They comprise:

- Features
- Target types
- Extrafields / Cisco call data
- Call scenarios
- Phone types
- Codecs

3.4.1 Features

The following features are supported:

Feature	Supported	Not supported	Remarks
Ad hoc Recording (Application Invoked Recording)	✓		
Automatic Recording		✓	
CUCM Cluster		✓	
CUCM Fail-over		✓	
Encryption (SRTP)		✓	Under development (for CUCM 8)
Device Mobility		✓	
Extension Mobility	✓		For all phones to which a user can log on, the following preconditions apply: <ul style="list-style-type: none"> • 'Built-in-Bridge' support • CTI controlled device • Device ID in Controlled Devices list of application user (see Appendix C 'Cisco Configuration Settings')
Record on Demand		✓	
Recording Warning Tone	✓		Configurable
SCCP (Skinny)	✓		

Feature	Supported	Not supported	Remarks
Secure SIP Trunk (TLS)	✓		<ul style="list-style-type: none"> Supported by CUCM 7 (or higher) Signalling is supported, secure audio (SRTP) is under development (see: Encryption)
Silent Monitoring		✓	
SIP (Cisco SIP)	✓		
Survivable Remote Site Telephony (SRST)		✓	
Targets (extension)	✓		Max. 2500 per Communication Manager
Targets (extension) – clustered CUCM		✓	Max. 2500 per Communication Manager (under development)

Table 2: Supported features

3.4.2 Target Types

The following target types are supported:

Target type	Supported	Not supported	Remarks
Agent		✓	
Device		✓	
Extension	✓		

Table 3: Supported target types

3.4.3 Extrafields / Cisco Call Data

The following 'Extrafields' or 'Cisco call data' are supported:

Name	Supported	Not supported	Remarks
Agent ID		✓	Under development
All Parties	✓		
Answering Party		✓	
Call ID	✓		
Called Party	✓		

Name	Supported	Not supported	Remarks
Calling Party	✓		
Conference Parties	✓		
Extension	✓		
Last Cause	✓		
Last Party		✓	
Originating ACD		✓	
Recording State	✓		
Ringling Party		✓	
Target ID	✓		

Table 4: Supported call data

3.4.4 Call Scenarios

The following scenarios for call recording are supported:

Scenario	Supported	Not supported	Remarks
Barge	✓		Supported by Cisco Active IP installer kit version 3.2 (or higher)
Call Answered	✓		
Call Conference	✓		
Call Forward	✓		
Call Hold	✓		
Call Parking	✓		
Call Pickup	✓		One and two stage
Call Transfer	✓		
Callback	✓		
cBarge	✓		Supported by Cisco Active IP installer kit version 3.2 (or higher)
Inbound external / inbound from a non-recordable set	✓		
Join	✓		
Multiple calls on same extension	✓		
Outbound external / outbound to a non-recordable set	✓		

Scenario	Supported	Not supported	Remarks
Shared line	✓		

Table 5: Supported call scenarios

3.4.5 Phone Types

The following phone types are supported per recording method:

Phone type	Supported	Not supported	Remarks
IP Phones	✓		3 rd generation with 'Built-in-Bridge' (BIB)
IP Soft Phones	✓		<ul style="list-style-type: none"> With IP Communicator version 7 Supported by Cisco Active IP installer kit 3.2 (or higher)

Table 6: Supported phone types

3.4.6 Codecs

The following codecs are supported:

Codec	Supported	Not supported	Remarks
G711	✓		
G729	✓		
G722*	✓		<ul style="list-style-type: none"> Default Cisco codec Supported by CUCM 6.1.2 (or higher) Supported by Cisco Active IP installer kit 3.2 (or higher)
G723.1	✓		Not supported by Cisco
Other codecs		✓	Not supported

Table 7: Supported codecs



* **Codec G722 requires the following settings: 16 kHz sample frequency, 14 bit sample resolution, and 64 kbit/s line bandwidth.**

4 System Description

This chapter describes the system components of the Cisco/CTI Active IP Recording solution.

This integrated recording system is built around the Cisco Unified Call Manager and the CyberTech CTI Server-based Recording System.

The CUCM recording features are invoked through CTI using JTAPI and the Session Initiation Protocol (SIP).

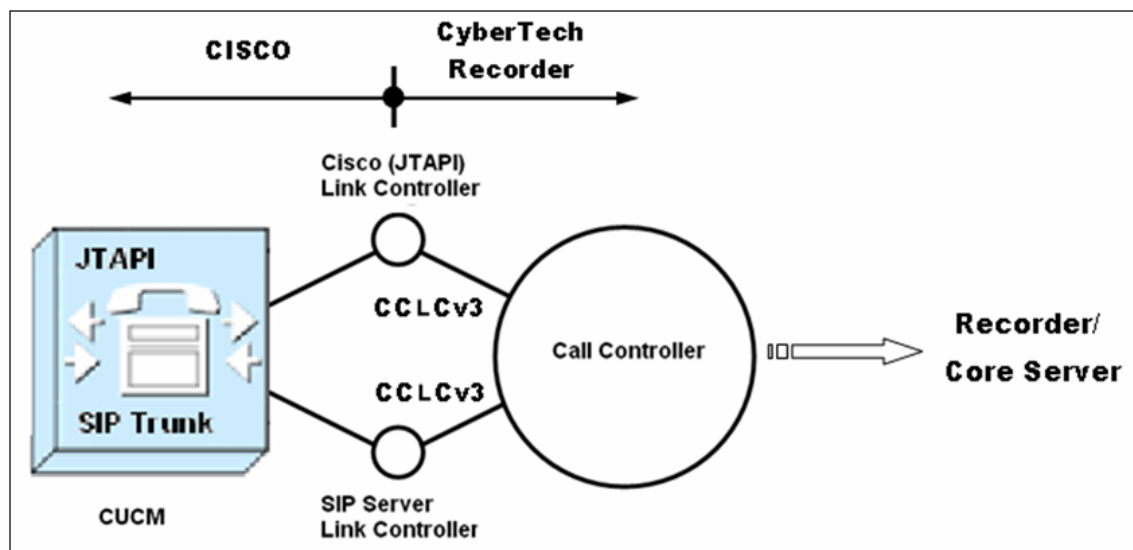


Figure 2: Basic system overview

The following topics are covered:

- Cisco system elements
- CyberTech Configuration Types
- Hardware Requirements
- Software Requirements

4.1 Cisco system elements

The integrated Cisco/CTI Active IP Recording system contains the following basic Cisco elements:

- Cisco Gateway, with pre-installed application software
- Cisco Unified Communication Manager (CUCM) with pre-installed application software
- Cisco Installer Kit 'Cisco_Active_IP_3.2.exe'
- (Cisco) Network Switch(es)



- Cisco (IP/Soft) Phones

Consult the available Cisco documentation for installation of the Cisco components.

4.2 CyberTech Configuration Types

The CT Recording System comes in two versions:

- Stand-alone system (Core Server and Recording channels in one box)
- Server/Satellite system (Core Server with one or more Recording Satellites)

Depending on the number of channels to be recorded, three configuration types are distinguished that use one of the two versions mentioned above. These configuration types are described in the following subsections.

Each configuration type involves specific hardware and software requirements, which are described in sections 4.3 'Hardware Requirements' and 4.4 'Software Requirements', respectively.

4.2.1 Configuration 1 (1-128 channels)



Figure 3: Core Server/Recording Channels with integrated CTI Server

Core Server/Recording Channels with integrated CTI Server (max. 128 recording channels)

- Software:
 - CT Cisco CTI Integration Software
 - CT recording software 5.3 (or higher)
- Parrot-DSC Cards: See section 4.3.1

4.2.2 Configuration 2 (1-168 channels)



Figure 4: Core Server/Recording Channels with separate CTI Server

CTI Server

- Software: CT Cisco CTI Integration Software

Core Server/Recording Channels (max. 168 recording channels)

- Software: CT recording software 5.3 (or higher)
- Parrot-DSC Cards: See section 4.3.2

4.2.3 Configuration 3 (1-168+ channels)

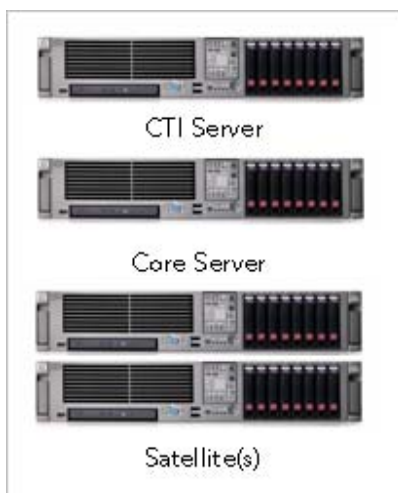


Figure 5: Core Server with separate CTI Server and Satellite(s)

CTI Server

- Software: CT Cisco CTI Integration Software

Core Server

- Software: CT 5.3 (or higher) recording software
- Parrot-DSC Cards: See section 4.3.3

Satellite(s) (1 satellite serves up to 480 recording channels)

- Software: CT 5.3 (or higher) recording software
- Parrot-DSC Cards: See section 4.3.3

4.3 Hardware Requirements

This section describes the minimum hardware requirements per configuration type (see section 4.2 'CyberTech Configuration Types' for a description).

The following topics are covered:

- Server hardware requirements on CTI Server, Core Server, and Satellite
- Parrot-DSC card requirements. The total number of cards depends on:
 - The number of channels to be recorded
 - The add-on modules as required by the – active or passive – recording method
 - The size of the Parrot-DSC card(s) used (short, medium, long)



Consult the 'CT Recording Solutions R5 – Installation Manual' and the 'Parrot-DSC-MOD-PCI Installation Manual' for details about Parrot-DSC Cards.



Consult the Server Hardware Requirements on www.cybertech-int.com (login required) or contact the CyberTech Presales department for details.

4.3.1 Configuration 1 (1-128 channels)

This section lists the minimum hardware requirements that apply specifically to configuration 1: Core Server/Recording Channels with integrated CTI Server.

Server hardware

A distinction is made between configurations in which up to 64 and 128 channels can be monitored.

Up to **64** channels:

- Processor:
 - Intel Xeon Dual Core 2.0 GHz
 - AMD Opteron 2.2 GHz
- RAM: 2 GB

Up to **128** channels:

- 2 Processors:
 - Intel Xeon Dual Core 2.0 GHz
 - AMD Opteron 2.2 GHz
- RAM: 2 GB

Parrot DSC PCI Cards

Item	Specification	Location
Card 1	Cisco JTAPI license for VoIP	Core Server/Recording Channels with integrated CTI Server
Card 2	SIP Server license	Core Server/Recording Channels with integrated CTI Server

Table 8: Parrot-DSC Cards - Configuration 1



Consult section 4.2.1 ‘Configuration 1 (1-128 channels)’ for details.

4.3.2 Configuration 2 (1-168 channels)

This section lists the minimum hardware requirements that apply specifically to configuration 2: Core Server/Recording Channels with separate CTI Server.

Server hardware

- Processor:
 - Intel Xeon Quad Core 2.0 GHz
 - AMD Opteron 2.4 GHz
- RAM: 2 GB

Parrot DSC PCI Cards

Item	Specification	Location
Card 1	Cisco JTAPI license for VoIP	Core Server/Recording Channels with integrated CTI Server
Card 2	SIP Server license	Core Server/Recording Channels with integrated CTI Server

Table 9: Parrot-DSC Cards - Configuration 2



Consult section 4.2.2 ‘Configuration 2 (1-168 channels)’ for details.

4.3.3 Configuration 3 (1-168+ channels)

This section lists the minimum hardware requirements that apply specifically to configuration 3: Core Server with separate CTI Server and Satellite(s).

Server hardware

A distinction is made between configurations in which up to 240 and 480 channels can be monitored.

Up to **240** channels:

- Processor:
 - Intel Xeon Quad Core 2.0 GHz
 - AMD Opteron 2.4 GHz
- RAM: 2 GB

Up to **480** channels:

- 2 Processors:
 - 2 x Intel Xeon Quad Core 2.0 GHz
 - 2 x AMD Opteron 2.4 GHz
- RAM: 4 GB



Configurations with 480 channels require Windows Server 2003 Standard Edition or higher.

Parrot DSC PCI Cards

A distinction is made between a configuration with one satellite and a configuration with multiple satellites.



The 'satellite cluster' mentioned in the following table is applicable to 240-channel monitoring. For 480-channel monitoring, a duplicate of such a cluster must be used.

Item	Specification	Location
First Satellite		
Card 1	Cisco JTAPI license for VoIP	1 st Satellite
Card 2	SIP Server license	1 st Satellite
Remaining Satellites (Per Satellite)		
1 Card per extra Satellite	Cisco JTAPI license for VoIP	Extra satellite

Table 10: Parrot-DSC Cards - Configuration 3



Consult section 4.2.3 'Configuration 3 (1-168+ channels)' for details.

4.4 Software Requirements

This section lists the *minimum* software requirements that apply to the server components of the CyberTech configurations as described in section 4.2 'CyberTech Configuration Types'.

4.4.1 CTI Server

- CT Cisco CTI Integration software (installer kit 'Cisco_Active_IP_3.2.exe') which installs these services:
 - Call Controller (v3 or higher)
 - Cisco (JTAPI) Link Controller (including JTAPI libraries)
 - SIP Server Link Controller
 - Virtual C++ Runtime Components
 - Java Runtime Engine

4.4.2 Core Server

- CT Recording Software 5.3 (or higher)
- Microsoft.NET Framework 3.5 Service Pack 1

4.4.3 Satellite

- CT Recording Software 5.3 (or higher)
- Parrot-DSC Card firmware: CTI_VOX_VoIP_16 or higher (Consult the firmware history for details.)



Consult www.cybertech-int.com for the latest software and firmware versions (login required).

<BLANK PAGE>

5 Prerequisites

This chapter describes the preconditions that must be met before you start installing and configuring the components of the Cisco/CTI Recording Solution.

The following topics are covered:

- Customer Prerequisites
- Cisco Prerequisites
- CyberTech Prerequisites
- Installing Parrot-DSC Firmware
- Licensing
- Adding Cisco Call Data (Extrafields)
-

Updating the File CTI_receiver.exe

5.1 Customer Prerequisites

Before you start the installation process, the customer must have made a number of arrangements. They comprise:

- Allocation of servers
- Accounts needed for logging on to the server
- Access rights for installation of Cisco system components
- Recordable target types (see section 7.5 'Defining Targets' for details)

5.2 Cisco Prerequisites

Before you install the components of the Cisco/CTI Recording Solution, be sure to have verified the following preconditions on the 'Cisco side' of the configuration.

- The CUCM software (version 6 or higher) is installed.
- The license information on the Cisco system is verified. (Consult section 5.5.1 'Cisco Licensing' for details.)
- For all supported phone types to which a user can log on, the following preconditions apply:
 - Device is CTI enabled
 - Extensions are CTI enabled

Then, execute the following steps:

1. Enable the Cisco CTI manager service on the CUCM.
2. Create an application user for CUCM access for the JTAPI link.
3. Register the username and password, as these are required for the GUI configuration (see chapter 7 'Configuration' for details).



Consult Appendix C 'Cisco Configuration Settings' and the available Cisco documentation for more details about Cisco system configuration.

5.3 CyberTech Prerequisites

This section describes the preconditions to be verified and preparatory steps to be taken on the 'CyberTech' side of the configuration.

5.3.1 Preconditions

Before you install the components of the Cisco/CTI Recording Solution, be sure to have verified the following preconditions on the 'CyberTech side' of the configuration.

- You have version **CTI_VOX_VoIP_16** of the Parrot-DSC firmware available. (Consult section 5.4 'Installing Parrot-DSC Firmware' for details.)
- The 'Cisco Active IP' installer kit version 3.2 requires the following (versions of) files:
 - PrtDCMP.dll (version 1.8.2.27 or higher)
 - PrtSRTP.dll
 - PrtVoip0.dll (version 1.2.16.1246 or higher)
 - CTI_receiver.exe (version 3.2.2.109 or higher) and all other files that are located in the same directory as this file



Consult www.cybertech-int.com for the latest software and firmware versions (login required).

5.3.2 Preparatory Steps

Execute the following steps before you configure the CTI Server application and enable the Cisco/CTI functionality:

1. Install Parrot cards (including the associated drivers) for hosting the applicable licenses.



The installation procedure of Parrot-DSC cards is described in the 'Parrot-DSC Installation Manual'.

2. Install the latest released CyberTech Recording software (release 5.3 or higher, with the applicable Service Repair; see section 1.2.2 'CyberTech Recording System') on the Core server.

Please note that the software requirements depend on the number of channels to be served:

- For up to and including 64 channels, the **CyberTech Myracle Recording** software package applies. (You can, however, install the **CyberTech Pro Recording** package if so desired.)
- For more than 64 channels, install the **CyberTech Pro Recording** software package.



The installation procedure of the CT recording software is described in the 'CT Recording Solutions R5 - Installation Manual'.

3. Install the Parrot-DSC firmware.
(Consult section 5.4 'Installing Parrot-DSC Firmware' for details.)
4. Load the applicable license information.
(Consult section 5.5 'Licensing' for details.)
5. Copy the files 'PrtDCMP.dll', 'PrtSRTP.dll' and 'PrtVoip0.dll' to the Parrot-DSC folder.
(Consult section 5.3.1 'Preconditions' for version information, and the 'CT Recording Solutions R5 - Maintenance Manual' for details about VoIP installations.)
6. Add specific Cisco call data.
(Consult section 5.6 'Adding Cisco Call Data (Extrafields)' for details.)
7. Update the file 'CTI_receiver.exe'.
(Consult section 5.7 'Updating the File CTI_receiver.exe'.)



Consult www.cybertech-int.com for the latest software and firmware versions (login required).

5.4 Installing Parrot-DSC Firmware

You install the latest Parrot-DSC firmware using the **(API) Programmer** service which is accessed through the **Monitor Tool**.



Before you install the Parrot-DSC firmware (see below), do the following:

- For *all* Parrot-DSC cards, verify that you have firmware version **CTI_VOX_VoIP_16** available (see previous section). If not, download the firmware from www.cybertech-int.com.
- Consult the **CT Recording Solutions R5 - Installation Manual** and **Parrot-DSC Installation Manual** for details about Parrot-DSC Cards and the associated firmware.

Instructions

1. First, verify that you are using the latest firmware (see notes above).
2. If the firmware version on the website is more recent than the one installed, download it to a specified location on your local system.
3. Start the **Monitor Tool** by clicking the shortcut on your desktop. The following window appears:

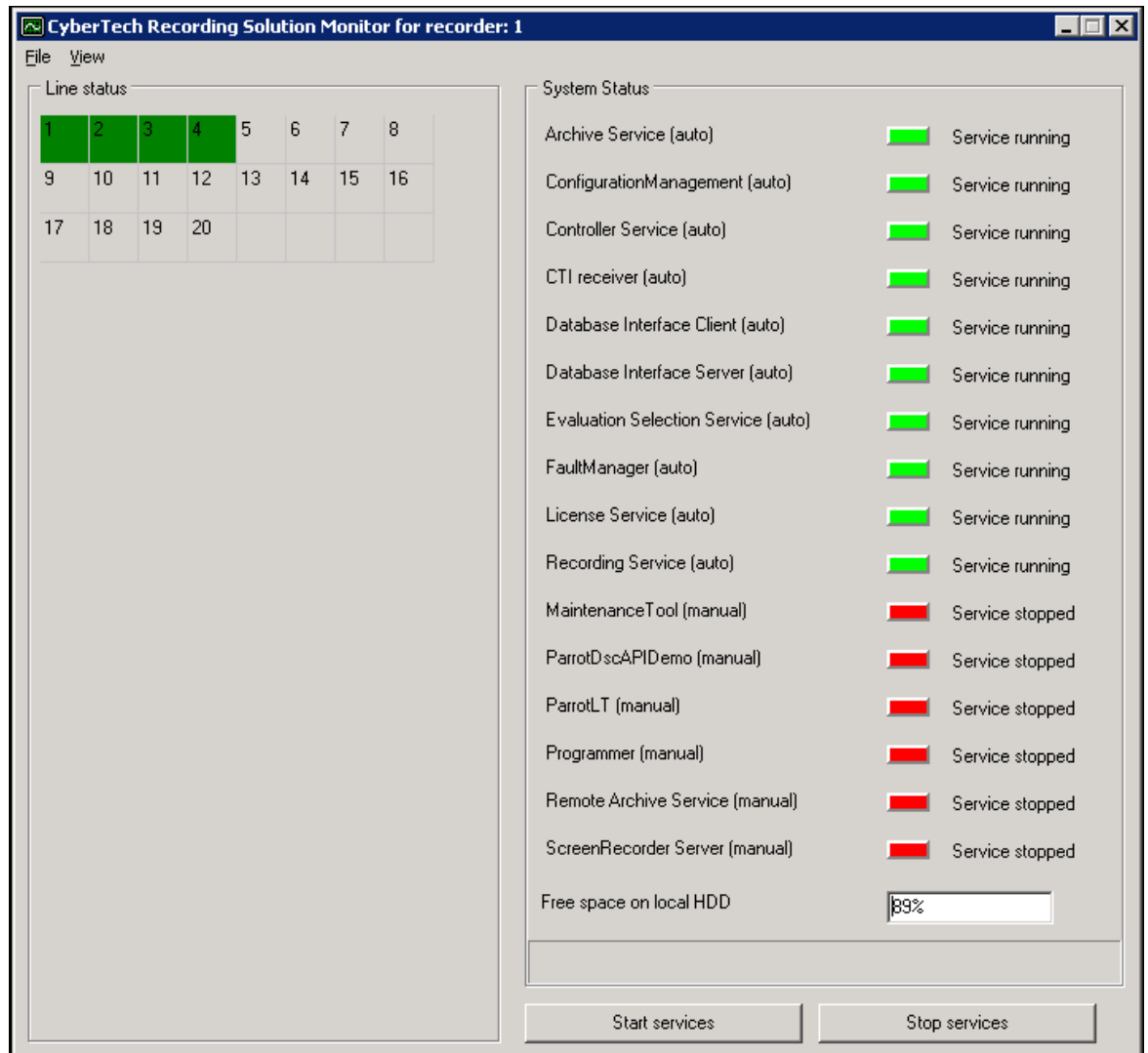


Figure 6: Monitor Tool

4. Click [Ctrl]+[Space] to enable the service start/stop modes.
5. Start the **Programmer** service. A window appears that shows all Parrot-DSC cards that are included in the system, with their properties.
6. Select the card for which you want to update the firmware. It is marked with a green "√" symbol.
7. Browse to the location on your hard drive where the firmware is located.
8. Install the firmware. (Consult the 'CT Recording Solutions R5 - Installation Manual' for details on locating and installing Parrot-DSC firmware.)



Be sure to REBOOT the CT Recording System after a firmware update. Otherwise, the settings mentioned above are not applied properly.

5.5 Licensing

The Cisco/CTI Recording Solution requires specific licenses. They are described in sections 5.5.1 'Cisco Licensing' and 5.5.2 'CyberTech Licensing', respectively.

Section 5.5.3 'Loading License Information' describes the instructions for loading licenses using the Parrot License Tool (LT).

5.5.1 Cisco Licensing

No specific Cisco licenses are required. The CT Recording System does not consume any DLUs.

5.5.2 CyberTech Licensing

The following CT licences are required:

- CT 5 license for the applicable recording method.
- VoIP license* for the required number of VoIP recording channels.
- Cisco JTAPI Link Controller license. When installed, this license is represented as string "8015" in the field **Data12** of the Parrot License Tool. (See section 5.5.3 'Loading License Information').
- SIP Server Link Controller license. When installed, this license is represented as string "8019" in the field **Data12** of the Parrot License Tool. (See section 5.5.3 'Loading License Information').
- Each recording channel using codec G729 requires a separate license ('concurrent licensing').



* **One Parrot DSC card can contain a VoIP channel license in combination with a license for the JTAPI or a SIP Server Link Controller.**

5.5.3 Loading License Information

License information is loaded using the **Parrot-DSC License Tool (ParrotLT)**, which is accessed through the **Monitor Tool**.

Instructions

1. Start the **Monitor Tool** by clicking the shortcut on your desktop. The following window appears:

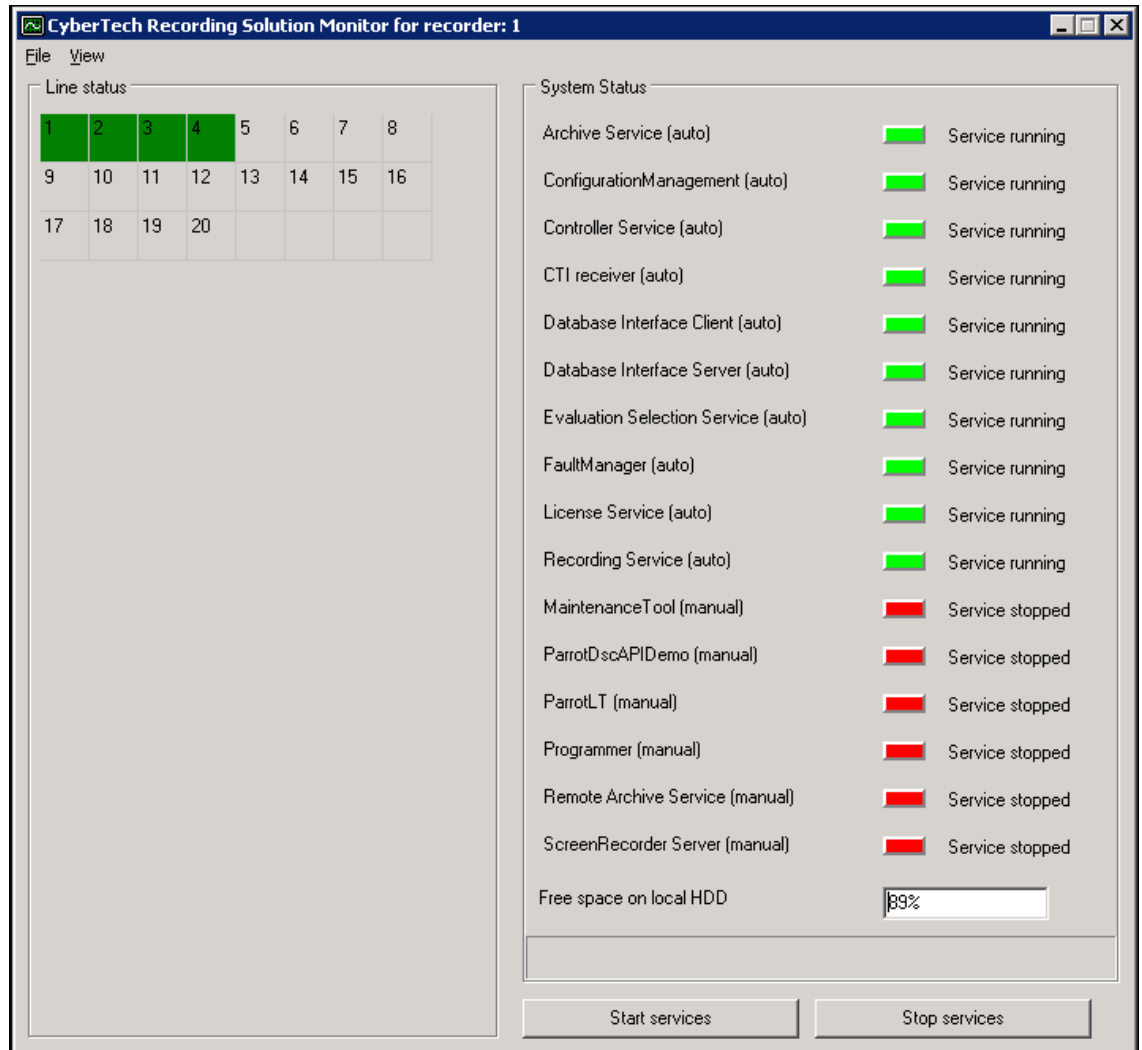


Figure 7: Monitor Tool (EXAMPLE)

2. Click [Ctrl]+[Space] to enable the service "start"/"stop" modes.
3. Start the **ParrotLT** Service. The following window appears, showing the licenses per installed board (two in the example):

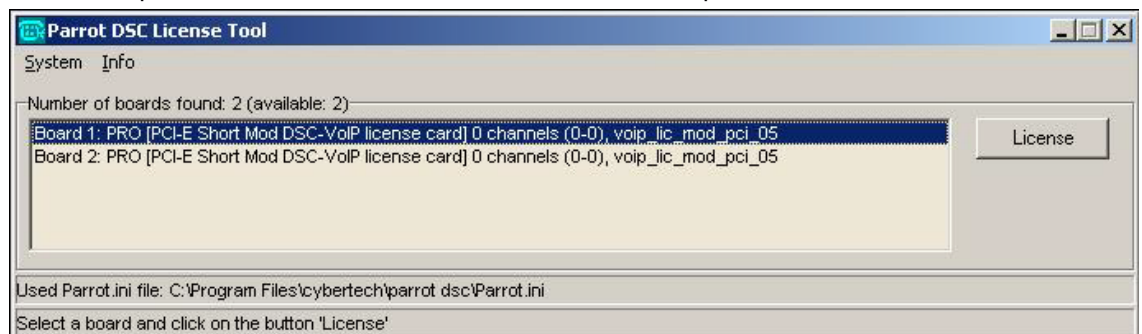


Figure 8: Parrot-DSC License Tool (EXAMPLE)

4. Select the board for which you want to load the license information and click **License**. A window with license information for the selected board appears.
5. Click **Get license**. The current license information for the selected board is displayed:

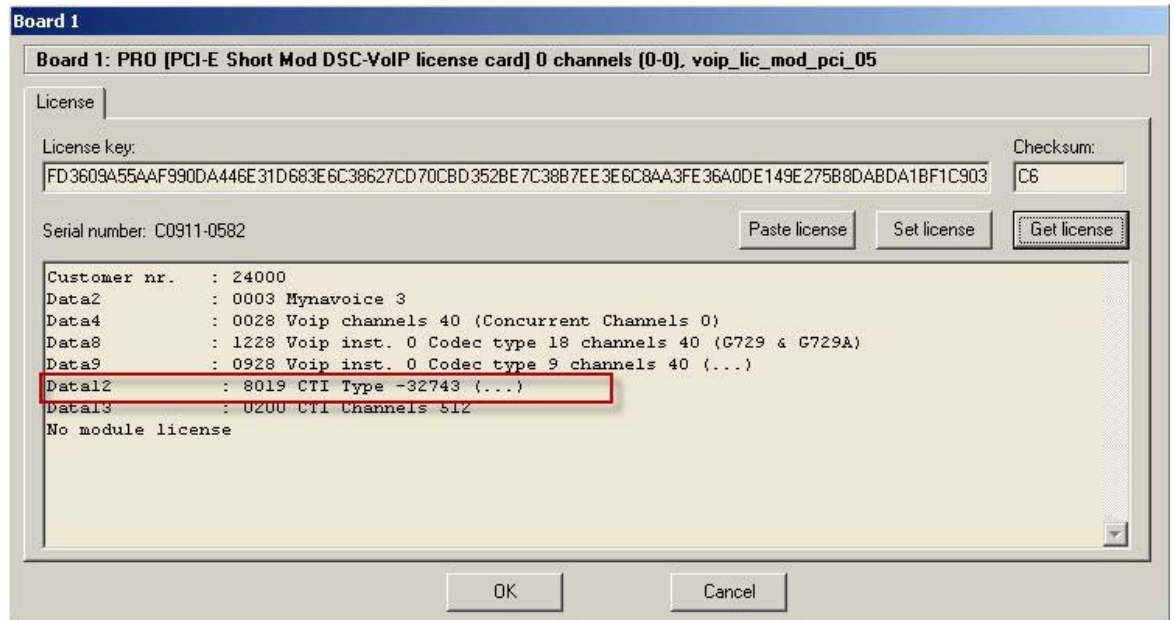


Figure 9: Loaded license for board 1 (EXAMPLE)

6. Verify that the field **Data12** starts with the string "8019" to indicate a SIP Server Link Controller license:

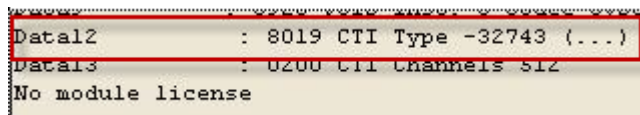


Figure 10: Loaded license for board 1 (EXAMPLE)

7. Click **Paste license** to load the license information as delivered by CyberTech. The license string is pasted into the field **License key**.
8. Click **Set license** to write the license information to the specified location.
9. Perform the above steps for all installed boards. For the second board in the example, the loaded JTAPI Link Controller license (represented by the string "8015" in the field **Data12**) looks like the following:

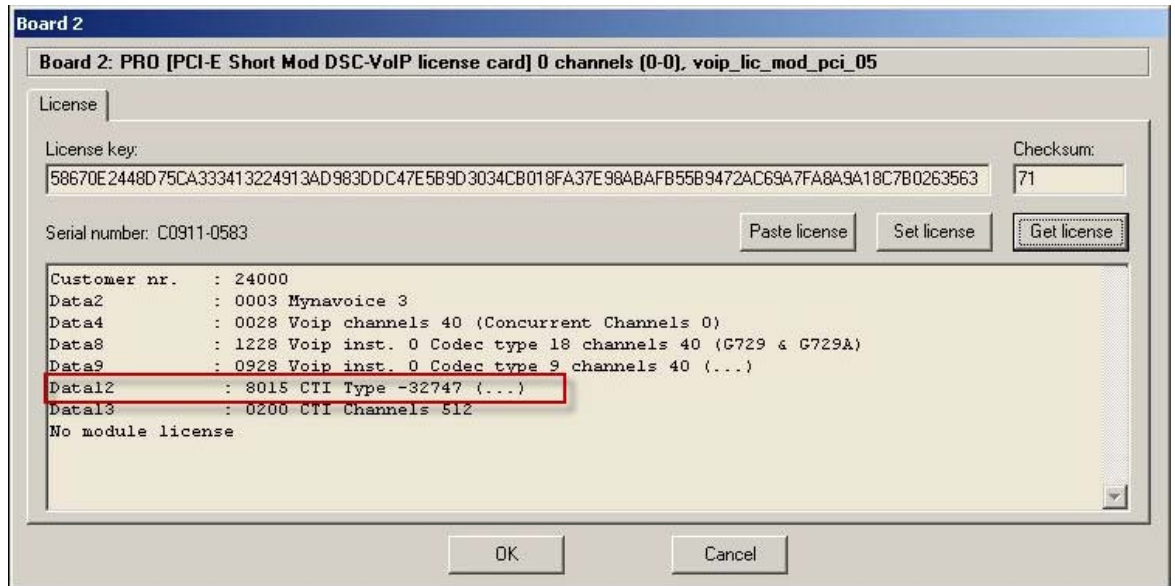


Figure 11: Loaded license for board 2 (EXAMPLE)

And the field **Data12** starts with the string "8015" to indicate a JTAPI Link Controller license:

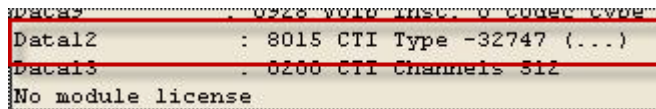


Figure 12: Loaded license for board 2 (EXAMPLE)



Consult the Parrot-DSC License Tool manual for details.

5.6 Adding Cisco Call Data (Extrafields)

In this step, you specify the Cisco-specific call data which will be available on the Core Server. This call data is read from the file 'extrafields.ini'.

To accomplish this, you have to copy the files 'extrafields.ini' from the CD to the folder 'C:\Program Files\cybertech\INI_files'.

5.7 Updating the File CTI_receiver.exe

Before configuring the CTI server, you must update the current version of the file 'CTI_receiver.exe' to the latest version.

The new version is delivered with version 3.2 of the 'Cisco Active IP' installer kit (see section 5.3.1 'Preconditions').

Instructions

1. Open the command window.
2. Go to the folder where the file 'cti_receiver.exe' resides. (The default location is: 'C:\Program Files\cybertech\cti_receiver'.)
3. Execute the following command to uninstall the current version:
cti_receiver2.exe -u
(Use all **lower case** characters.)
4. Rename this current version to 'cti_receiver2.exe.old'.
5. Copy the new 'CTI_receiver.exe' (and all other files that are located in the same directory as this file) to the directory 'C:\Program Files\cybertech\CTI_receiver'.
(Consult section 5.3.1 'Preconditions' for version information.)
6. Execute the following command to install the new version:
cti_receiver.exe -I
(Use the **upper case** version of the character 'I' (= "Install").)
7. Restart the pc.
8. After a system restart, activate the **Monitor Tool** by clicking the shortcut on your desktop. The following window appears:

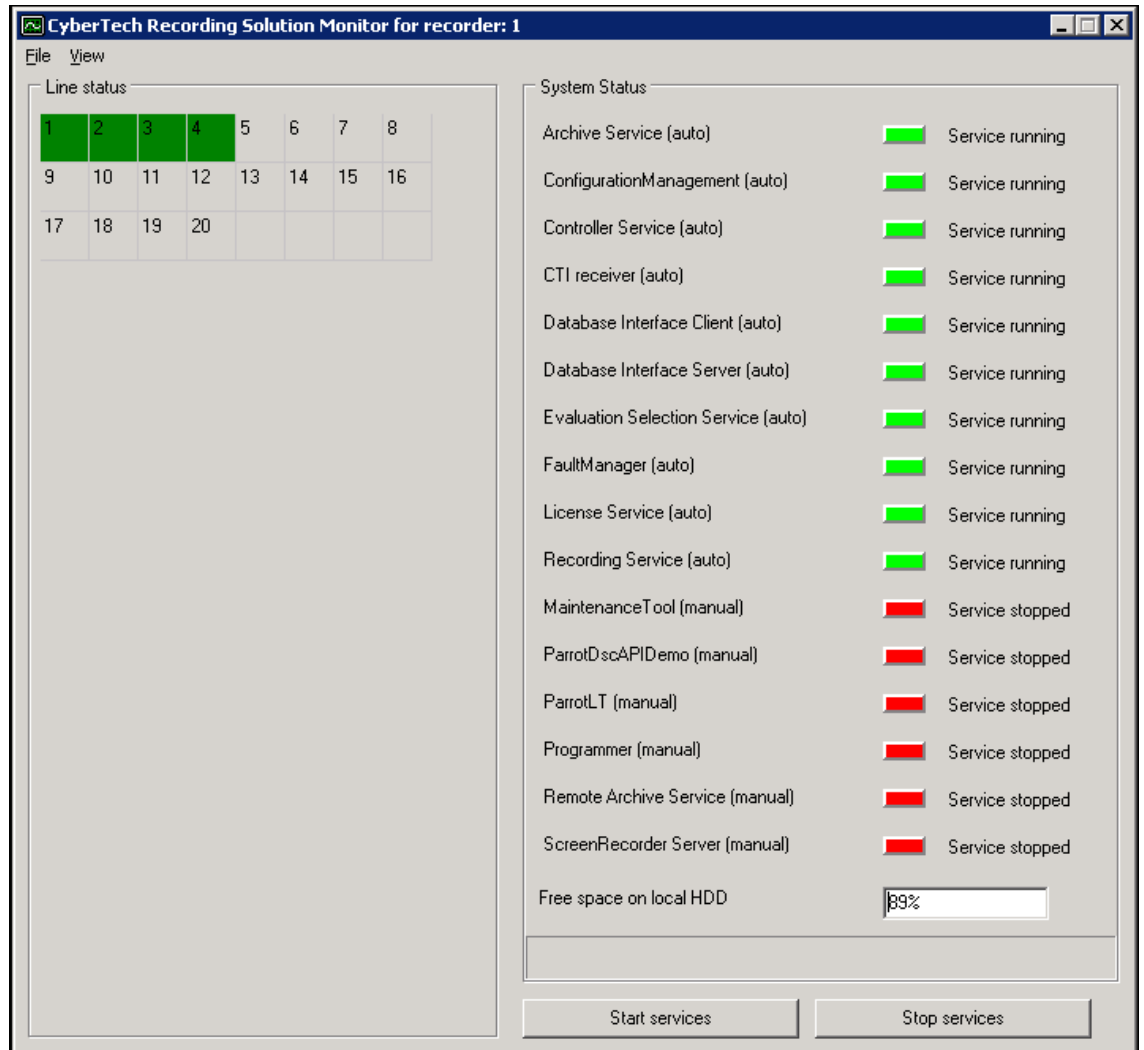


Figure 13: Monitor Tool

- Verify that the CTI receiver service has been started automatically. It should have the suffix "(auto)" and the value "Service running" as shown below:

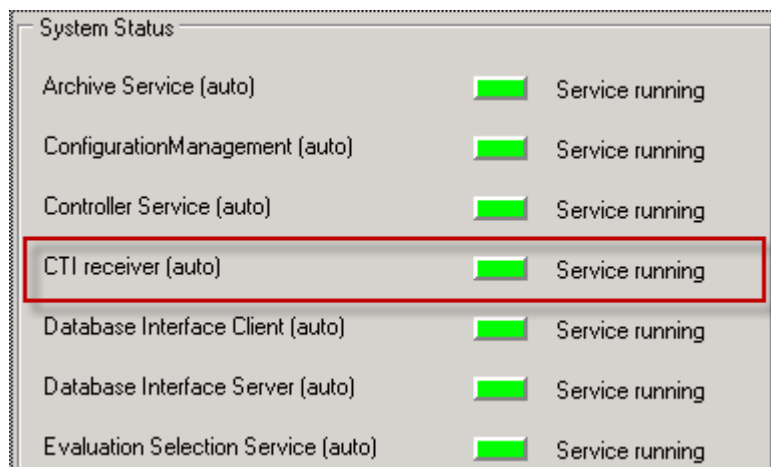


Figure 14: CTI receiver service started

10. If the CTI Receiver is disabled, apply the following procedure to enable it:
 - a. Start the (Microsoft) **Computer Management** tool.
 - b. In the left pane, select **Services and Applications** and then **Services**, respectively.

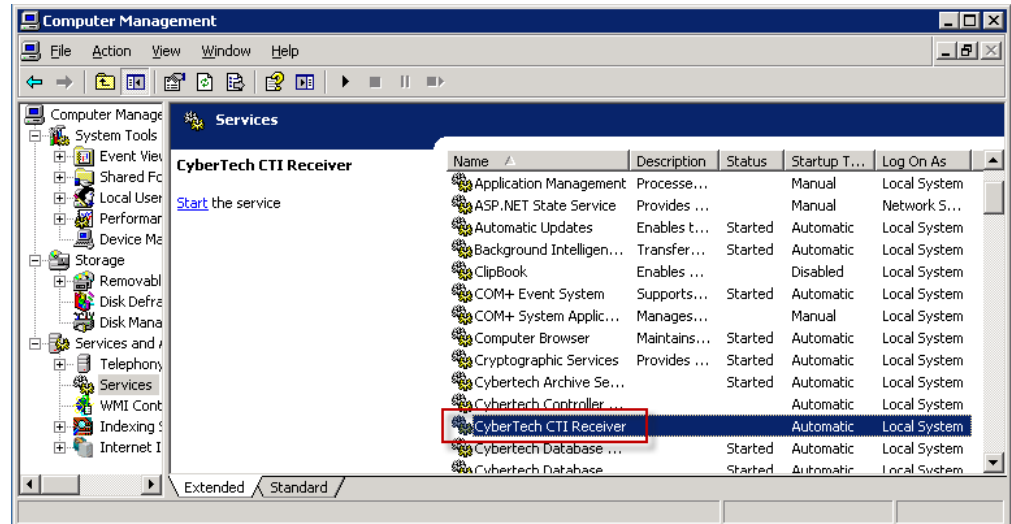


Figure 15: Computer Management: services

- c. In the right pane, double-click the **CyberTech CTI Receiver** service:

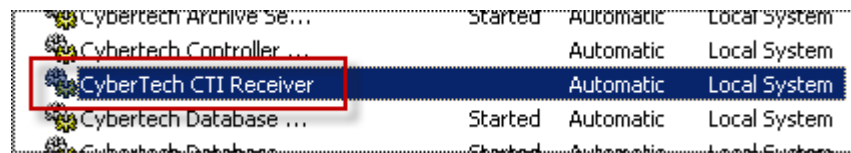


Figure 16: CyberTech CTI Receiver

The *Properties* window appears:

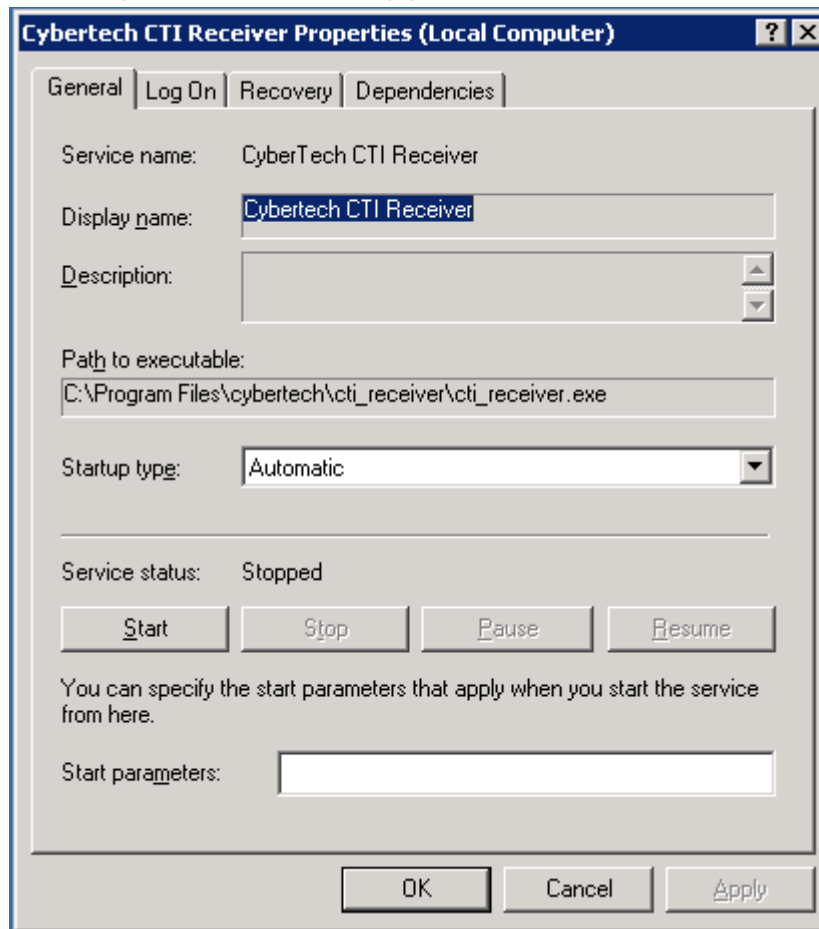


Figure 17: CTI Receiver stopped

- d. Select "Automatic" in the **Startup type** field if this is not already the case.
- e. Click the **Start** button to start the service.
- f. Click **OK** to save your settings and close the *Properties* window.
- g. Restart the Monitor Tool to verify that the CTI Receiver service is now enabled.

<BLANK PAGE>

6 Installation

This chapter describes the necessary actions to install the CT Cisco CTI Integration Software.



Please be aware that the procedures described in this chapter must be executed by trained staff, to prevent system damage.

Before installing, verify that the Prerequisites are met as described in chapter 5 'Prerequisites'.

The following topics are covered:

- Installing the CT Cisco CTI Integration Software
- Post Installation Copying
- Setting Up the Secure SIP Trunk

6.1 Installing the CT Cisco CTI Integration Software

You install the CT Cisco CTI Integration Software (via version 3.2 of the Cisco Active IP installation kit) on a dedicated CTI server or an integrated Core Server.

Instructions

1. Run the 'Cisco Active IP' installation kit from a local drive or CD. The *Setup Wizard* appears:



Figure 18: Setup Wizard: Configuration 2

2. Click **Next**. The window *Select Components* appears.



In the *Select Components* window, you choose whether to install a stand-alone system or a system with separate CTI Server and – optionally – one or more satellites (consult section 4.2 'CyberTech Configuration Types' for details).

6.1.1 Configuration with Dedicated CTI Server

3. In the *Select Components* window, select the option **Dedicated CTI server** (default option):

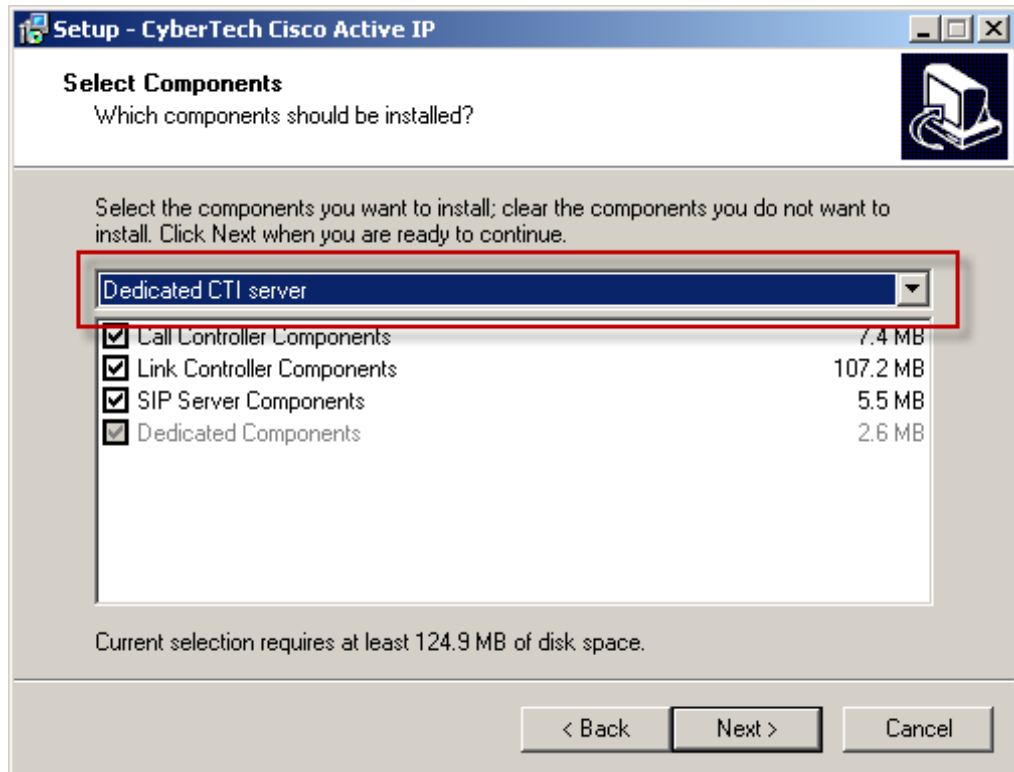


Figure 19: Select Components: Dedicated CTI server

4. Click **Next**. The window *Database Connect* appears:

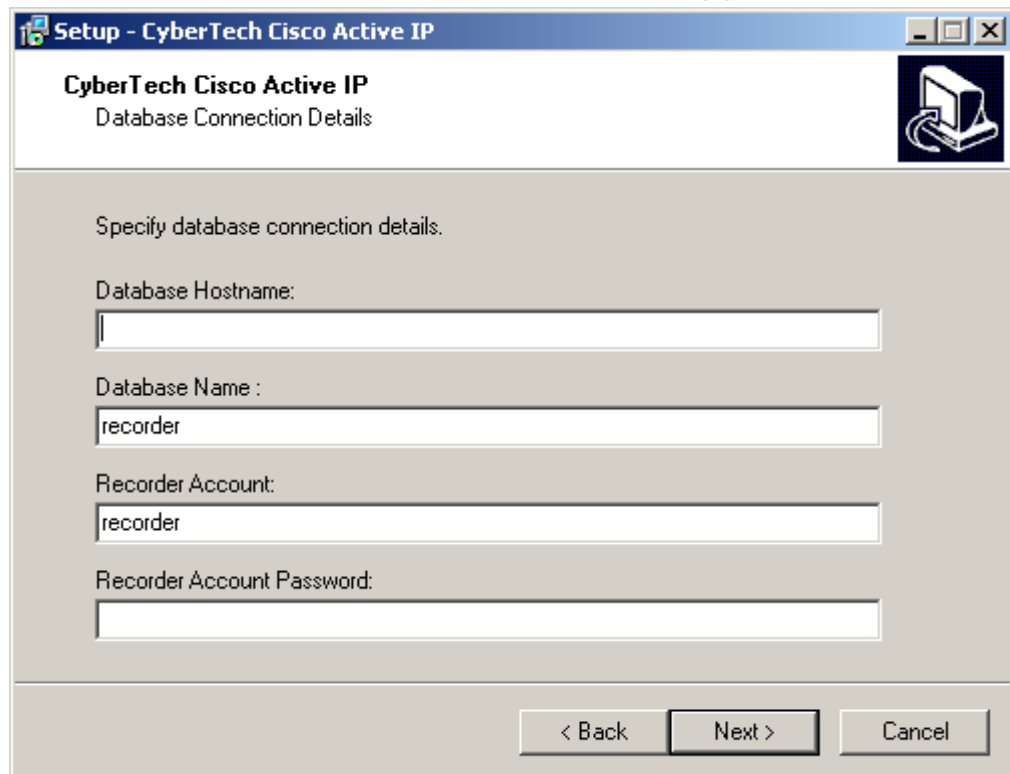


Figure 20: Database Connection Details

5. Enter the following data:
 - a. **Host Name:** Local host name (in a stand-alone configuration) or IP address of the Core Server
 - b. **Database Name:** The value "recorder" (default)
 - c. **User Name:** The value "recorder" (default)
 - d. **Password:** The password that is used for recorder installation
6. Click **Next**. The window *Ready to Install* appears:



Figure 21: Ready to Install

7. Click **Install** to start the installation process. The following progress windows are displayed:



Figure 22: Installing

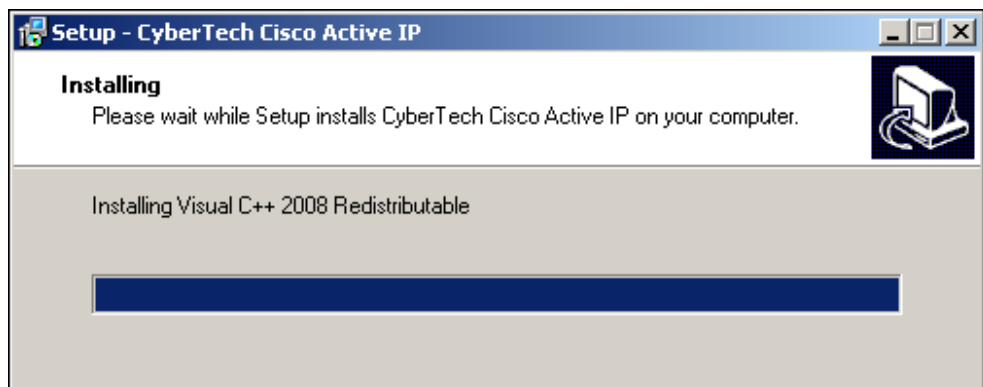


Figure 23: Installing Visual C

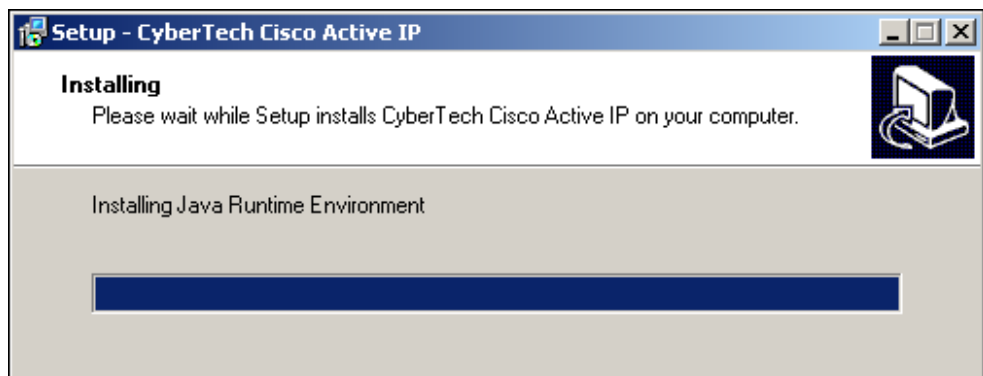


Figure 24: Installing JRE

8. Wait until the installation completes. The following window appears:



Figure 25: Installation Completed

9. Click **Finish** to exit the installation.
10. Depending on the situations distinguished above, perform one of the following actions:
 - Upon successful completion, verify that the following desktop shortcuts are created on the CTI and/or Core Server (depending on the configuration):
 - CTI Server: Monitor Tool
 - Core Server: CT Recording Software
 - If installation did **not** complete, solve the problem causing the premature ending and run the set-up procedure again.

6.1.2 Stand-alone Installation

3. In the *Select Components* window, select the option **CTI on Core server**:

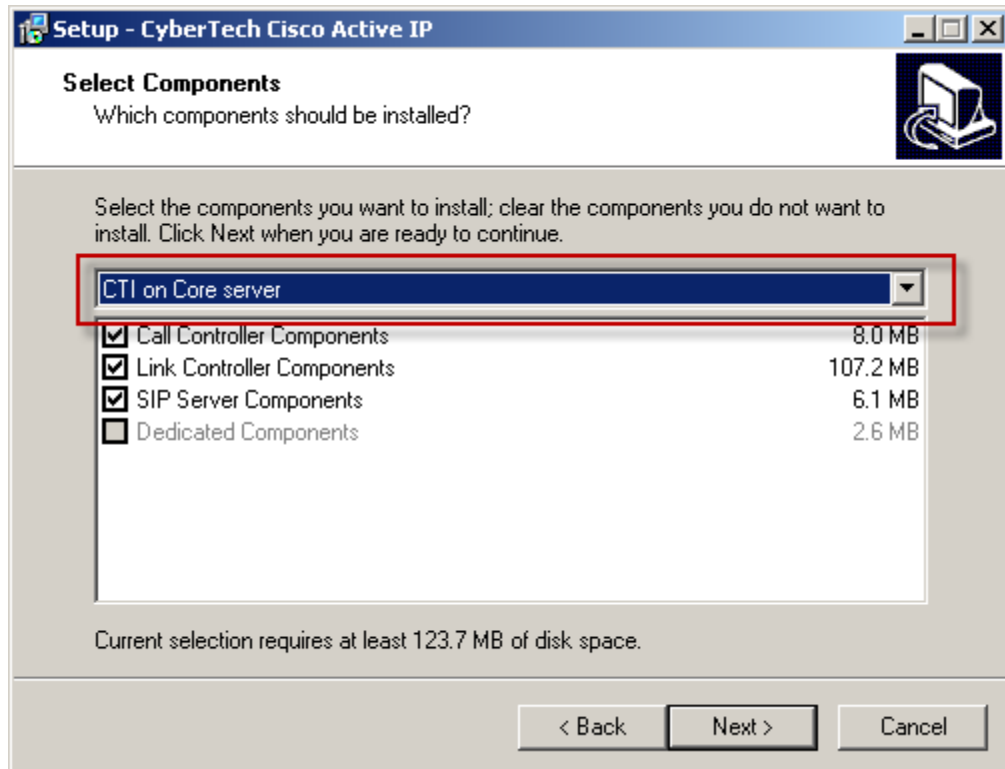


Figure 26: Select Components: CTI on Core server

4. Click **Next**. The window *Ready to Install* appears:

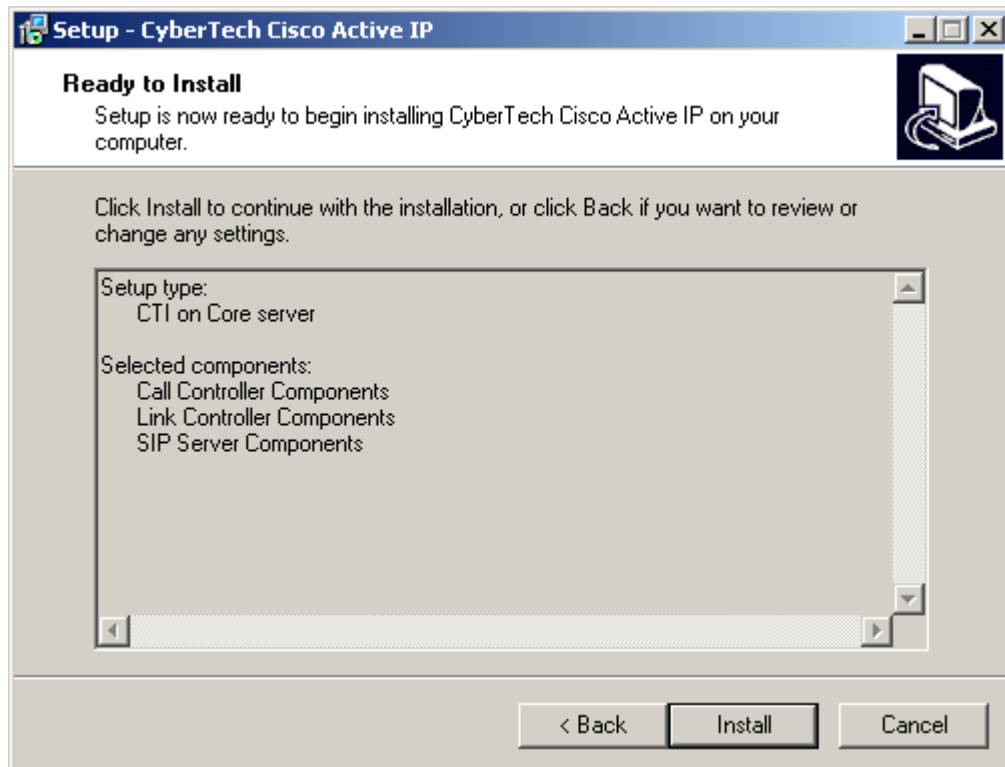


Figure 27: Ready to Install

5. Click **Install** to start the installation process. Follow the procedure from this point onward as described in the previous subsection (for the **CTI on Core Server** option).

6.2 Post Installation Copying

To complete the installation, you have to perform the following steps manually:

1. Copy the folder 'CTI_receiver' to the folder C:\Program Files\cybertech' on your system.
2. Copy the file 'PrtDCMP.dll' to the '\Parrot DSC' folder. This facilitates the use of codecs G722 and G723.1 when using version 5.4 of the CT Recording System.
3. Copy the files 'PrtSRTP.dll' and 'PrtVoip0.dll' to the '\Parrot DSC' folder to facilitate VoIP recording.

6.3 Setting Up the Secure SIP Trunk

This section describes the procedure to set up a Secure SIP Trunk using Windows certificates.



The Secure SIP Trunk feature is supported for CUCM 7 and higher.

The procedure is subdivided into six main steps. Some of these steps are performed by a CyberTech installation engineer, others by a Cisco-certified engineer. These main steps comprise:

1. Download certificate from CUCM (by Cisco-certified engineer)
2. Generate certificates (by CyberTech engineer)
3. Load certificate in CUTM (by Cisco-certified engineer)
4. Install certificate on SIP Server system (by CyberTech engineer)
5. Configure SIP Server (by CyberTech engineer)
6. Configure CUCM (by Cisco-certified engineer)

Each of these steps is described in a separate subsection below.

Prerequisite

The Cisco Active IP installation kit (see previous section) has placed the so called 'security kit' in the folder 'C:\Program Files\cybertech\CTI\SipServer\security':



Figure 28: Security kit for Secure SIP trunk

6.3.1 Download Certificate



This step must be executed by a Cisco-certified engineer and is not described in this manual.

6.3.2 Generate Certificates

1. Copy the downloaded **CallManager** certificate to the folder 'C:\Program Files\cybertech\CTI\SipServer\security'.
2. Execute the file 'make_cert.bat' to generate the root, client and server certificates. (The Root certificate will be loaded in the CUCM by the Cisco engineer. The client, server, and call manger certificates will be installed on the CTI Server.)
3. In the command window that appears, enter your personal data and a securing password that apply to the generated certificates. Keep the following in mind:
 - No spaces are allowed.
 - No backspace is allowed in the password.



Figure 29: Personal Data & Password

4. Confirm your password and press <Enter>. After a successful certificate generation, the following window is displayed:

```

C:\WINDOWS\system32\cmd.exe

Succesfully Generated all neede certificates

Created Root Certificate for Call Manager: SipRoot.pem
Renamed Root Certificate for SIP server: CallManager.crt
Created Server Certificate for SIP server: client.pfx
Created Client Cettificate for SIP server: server.pfx

Root certificate name <CN>: SipRoot
Client certificate name <CN>: SipCient
Server certificate name <CN>: SipServer

Country: US
State: New_York
City: White_plains
Company: Cybertech_US
Email: info@cybertech-int.com
Password: *****

Generated Root has a lifetime of: 3650 days
Generate Client and Server certificates have a lifetime: 1096 days

Press any key to continue . . . -
    
```

Figure 30: Successful generation

5. Verify that the data corresponds to the personal data as entered.
6. Verify that the following files have been generated:

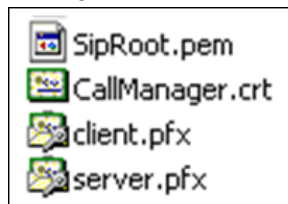


Figure 31: Generated files



6.3.3 Load Certificate in CUCM

This step must be executed by a Cisco-certified engineer and is not described in this manual.

6.3.4 Install Certificates on SIP Server System

This section describes the steps to install a certificate on the SIP Server system. The steps are grouped into three categories:

- Installing the Cisco Certificate
- Installing the Client Certificate
- Installing the Server Certificate

Installing the Cisco Certificate

1. Browse to the folder 'C:\Program Files\cybertech\CTI\SipServer\security':

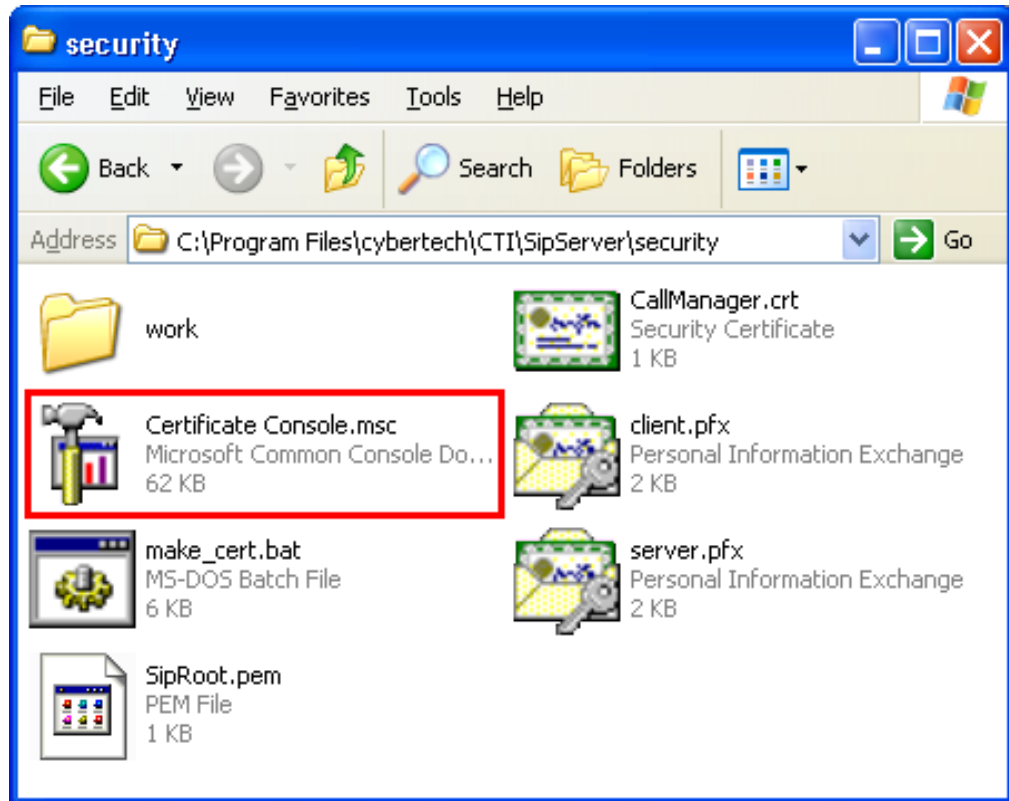


Figure 32: Location of certificate installer

2. Double-click the file 'Certificate Console.msc'. The following window appears:

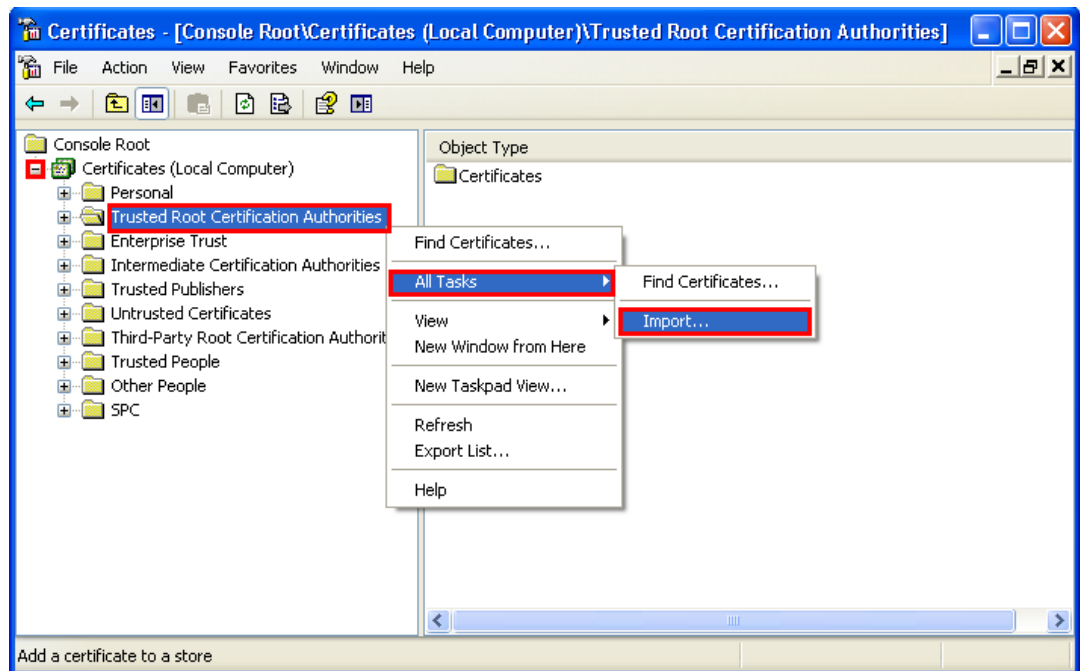


Figure 33: Certificate Console

3. Expand the entry **Certificates (Local Computer)**.

4. Right-click the entry **Trusted Root Certification Authorities**.
5. In the context menu that appears, click the subsequent entries **All Tasks** > **Import...** The *Certificate Import Wizard* opens as follows:



Figure 34: Certificate Import Wizard

6. Click **Next**. The window *File to Import* is displayed:

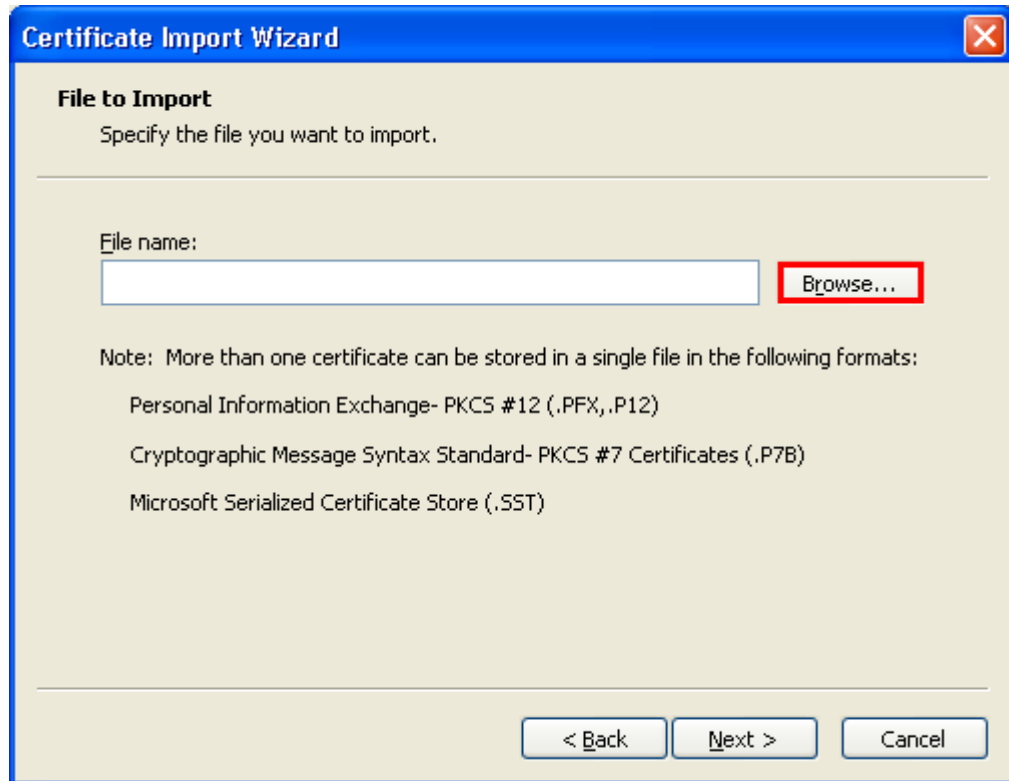


Figure 35: File to import

7. Click **Browse**, and browse to the security folder of the Sip Server.

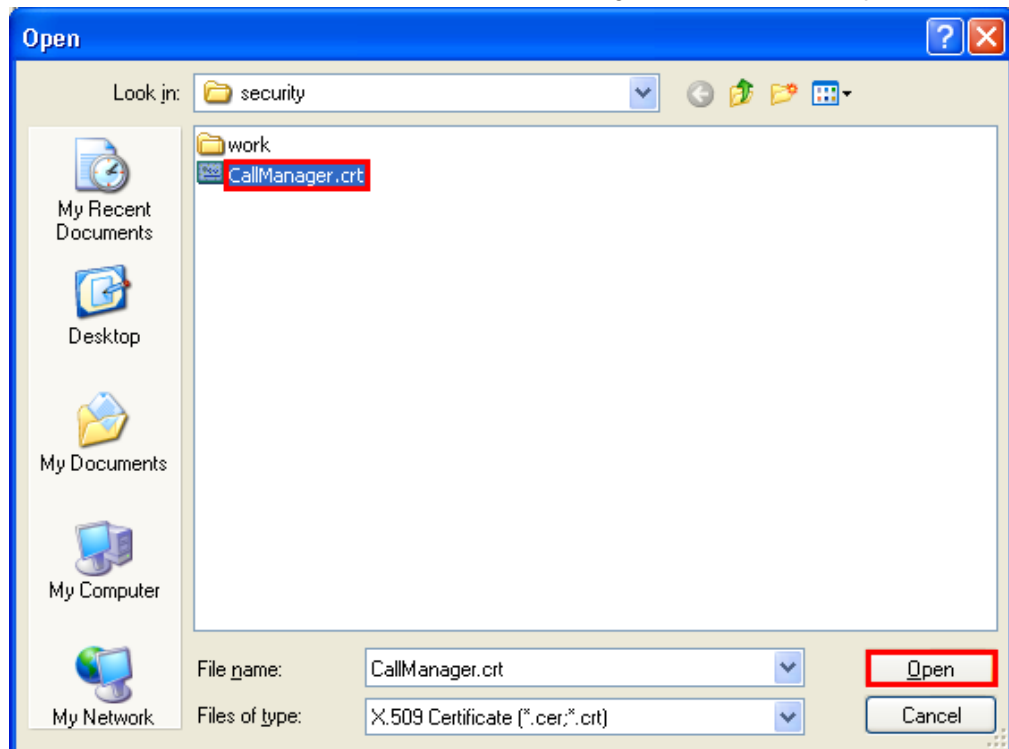


Figure 36: Security folder

8. Select the call manager certificate 'CallManager.crt' and click **Open**. The name of the file appears in the **File name** field of the *File to Import* window:

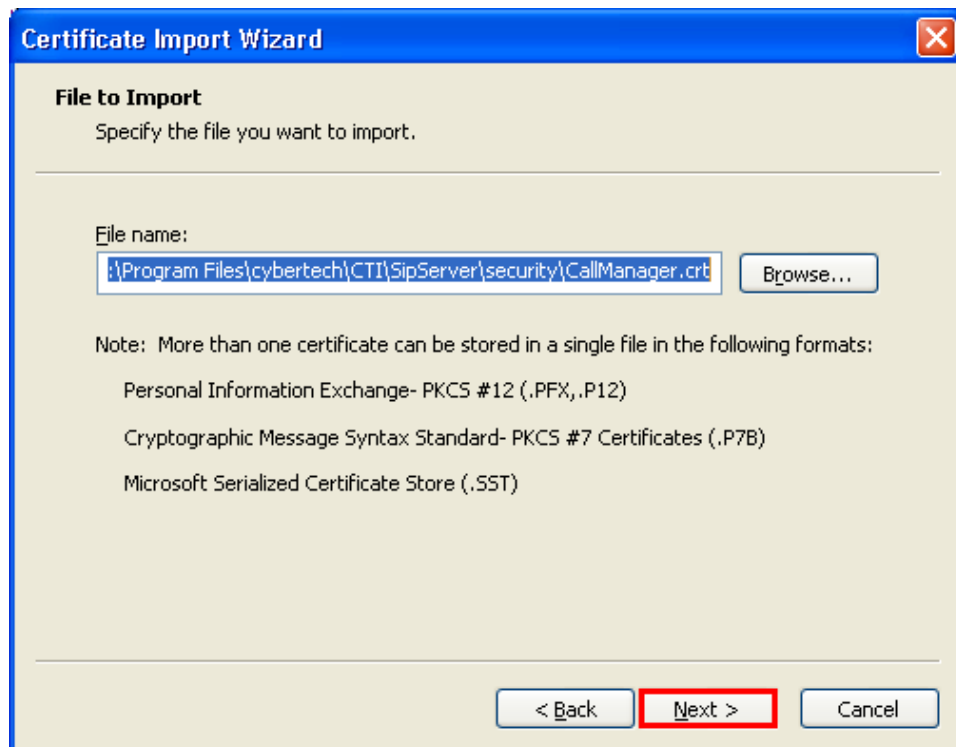


Figure 37: Cisco certificate

9. Click **Next**. The *Certificate Store* window is displayed:

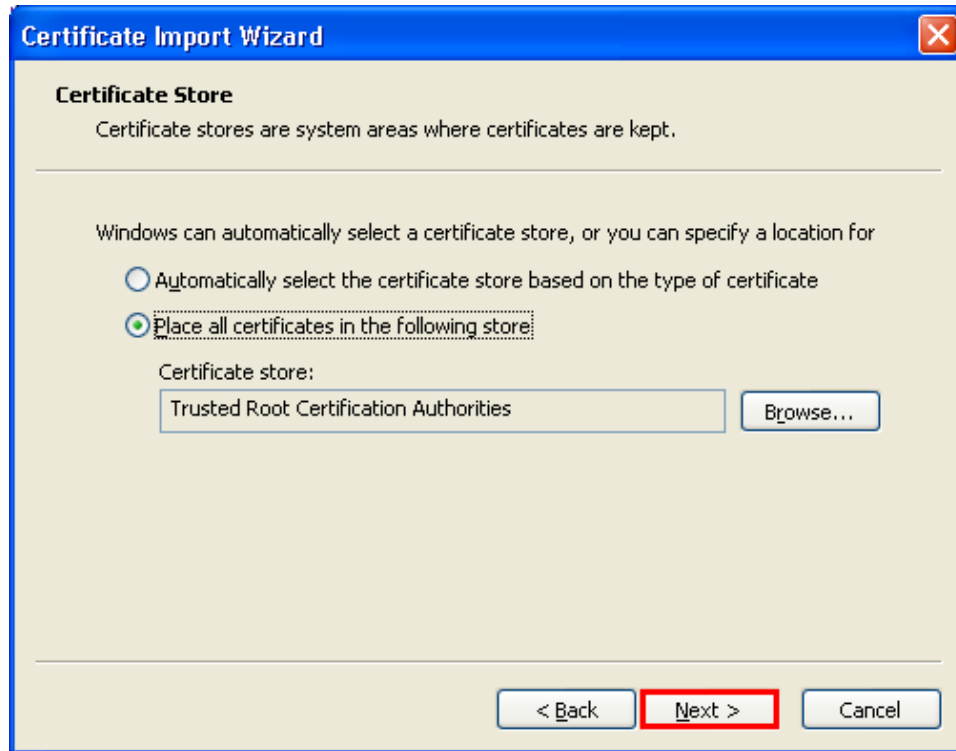


Figure 38: Certificate store

10. Click **Next**. The following window is displayed:

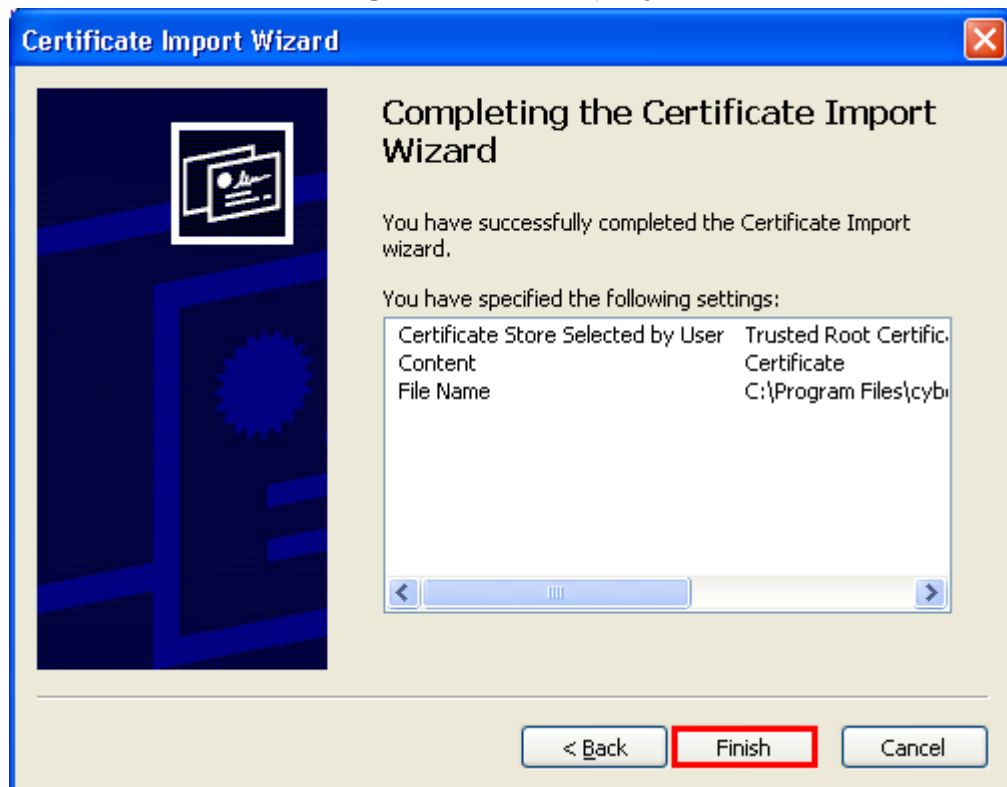


Figure 39: Completing the wizard

11. Click **Finish** to start the import process. After successful import, the following message is displayed:



Figure 40: Successful import

12. Click **OK** to close the wizard.

Installing the Client Certificate

1. Go to the certificate console like you did for the Cisco certificate.

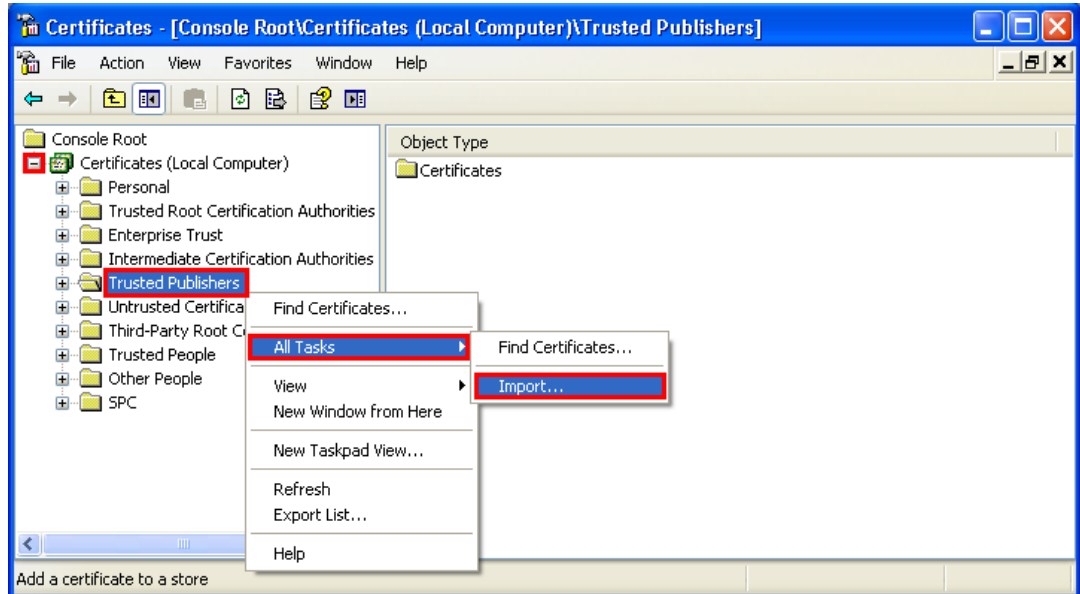


Figure 41: Certificate Console

2. Expand the entry **Certificates (Local Computer)**.
3. Right-click the entry **Trusted Publishers**.
4. In the context menu that appears, click the subsequent entries **All Tasks > Import...** The *Certificate Import Wizard* opens as follows:



Figure 42: Certificate Import Wizard

- Click **Next**. The window *File to Import* is displayed:

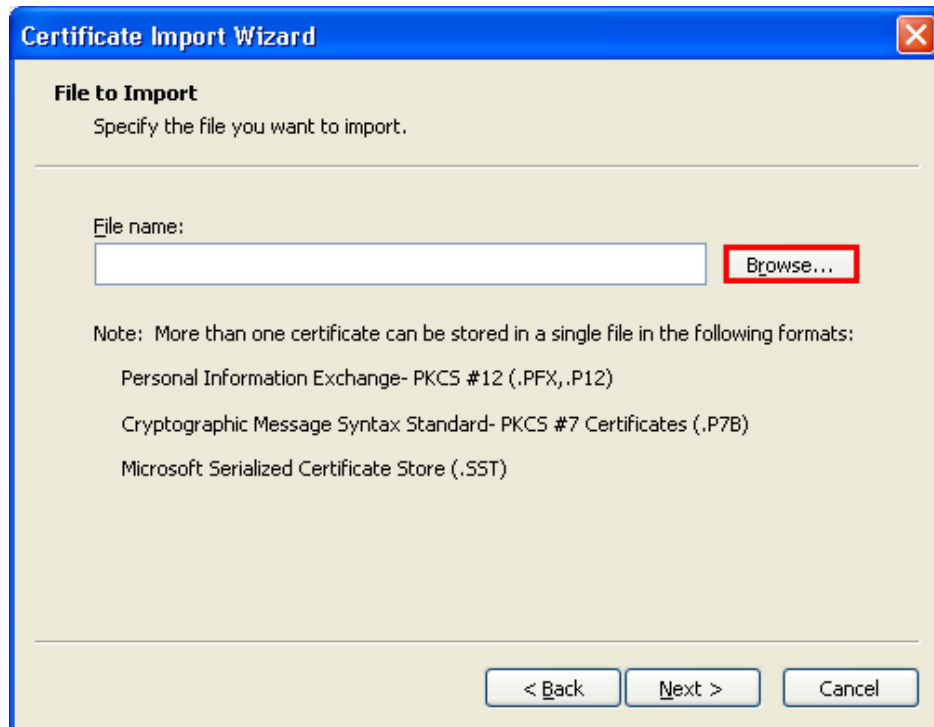


Figure 43: File to import

- Click **Browse**, and browse to the security folder of the Sip Server.
- In the drop down box next to the field **Files of type:**, select the file type "Personal Information Exchange (*.pfx, *.p12)":

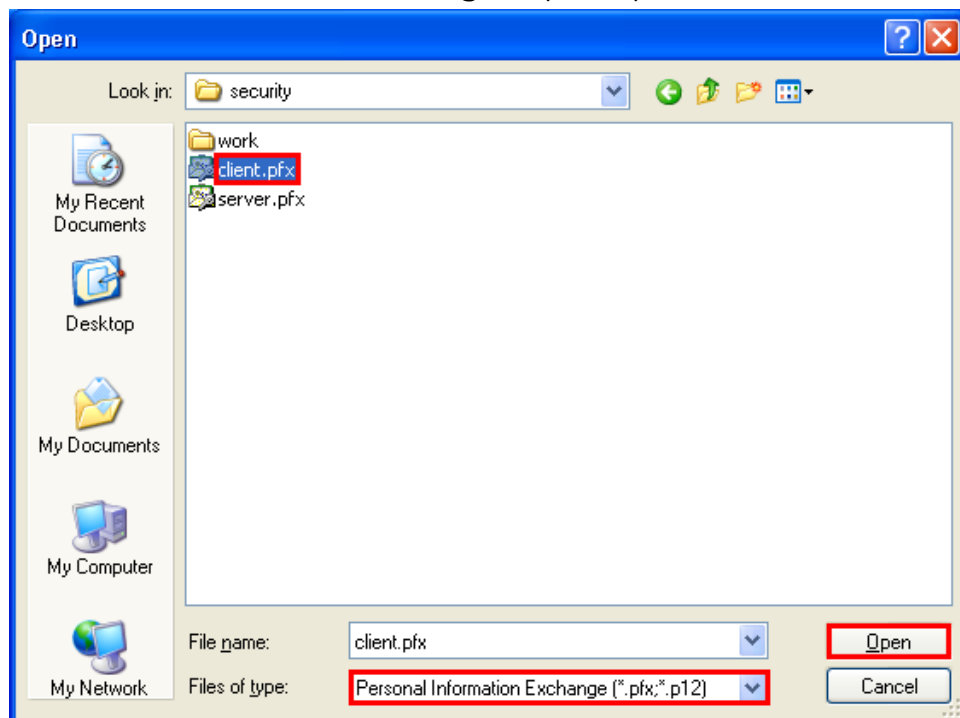


Figure 44: PFX files in Security folder

- Select the client certificate 'Client.pfx' and click **Open**. The name of the certificate file is displayed in the **File name** field.

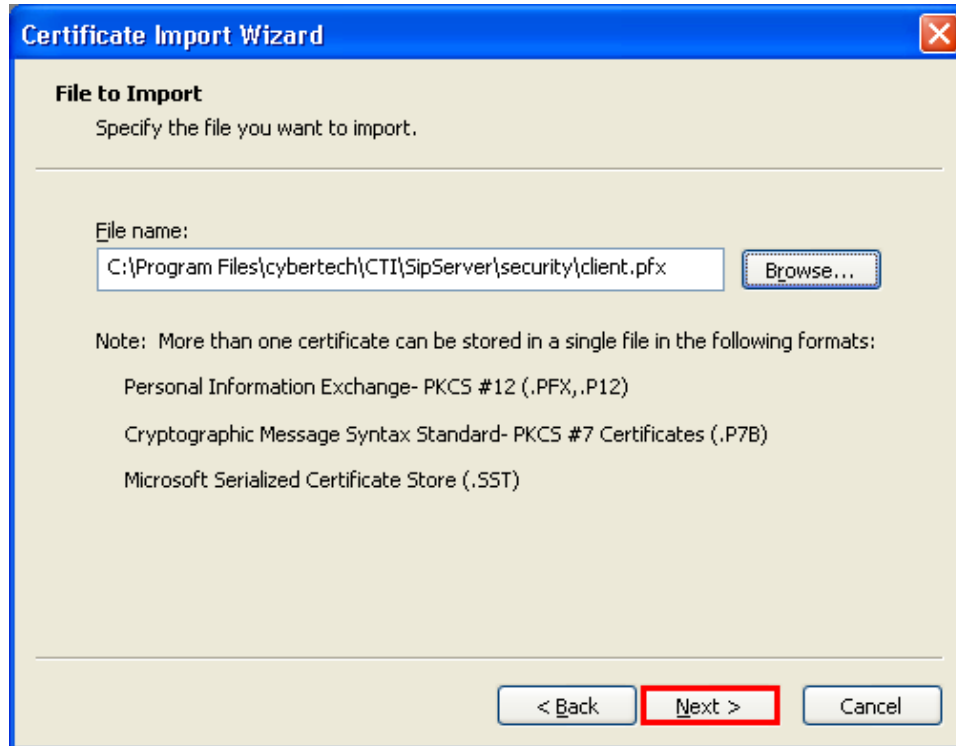


Figure 45: Client certificate

- Click **Next**. The *Password* window opens:

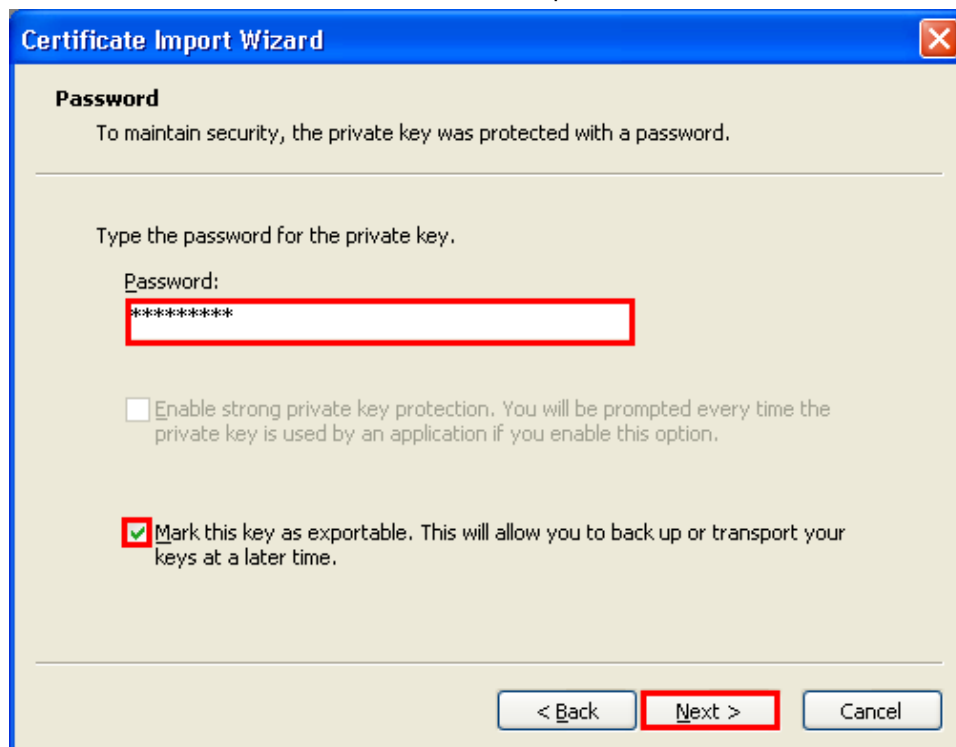


Figure 46: Password

10. Enter the same password that you used when generating the certificates (see section 6.3.2 'Generate Certificates').
11. Select the checkbox **Mark this key as exportable**. This allows you to back up or transport your keys at a later time.
12. Click **Next**. The *Certificate Store* window is displayed:

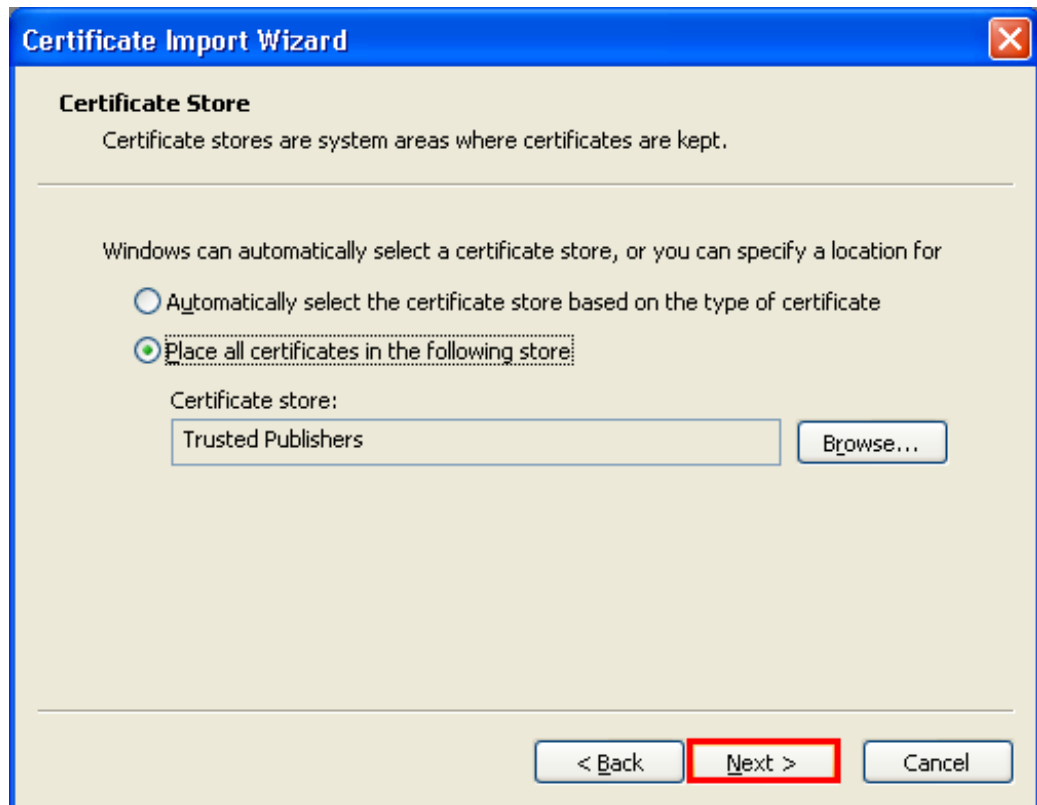


Figure 47: Certificate store

13. The correct destination should already be selected, so click **Next**. The following window is displayed:

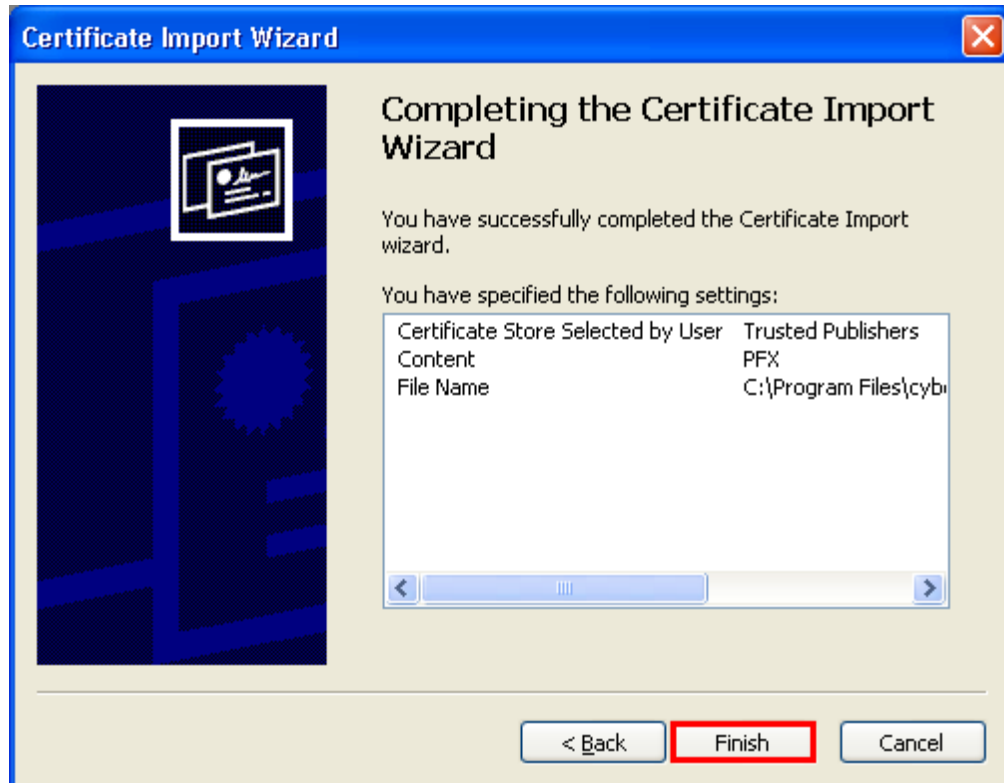


Figure 48: Completing the wizard

- Click **Finish** to start the import process. After successful import, the following message is displayed:



Figure 49: Successful import

- Click **OK** to close the wizard.

Installing the Server Certificate

Execute the same steps as described for the Client Certificate. In the **File name** field, you now select the file 'server.pfx' (instead of 'client.pfx').

6.3.5 Configuring the SIP Server

1. Log on to the CyberTech Web GUI.
2. Select the respective tabs **cti integration** > **devices**:

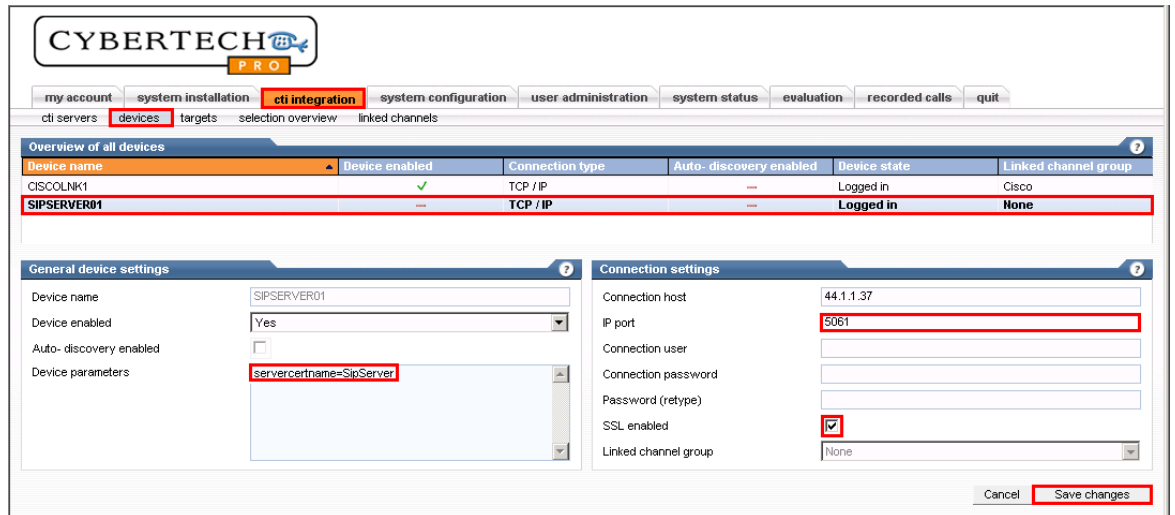


Figure 50: Device overview

3. Click on the device representing the SIP Server ("SIPSERVER01" in the example above) to modify its settings.
4. In the *General device settings*, add the device parameter "servercertname=SipServer". This means that the SIP Server will use the CN (common name) of the SIP Server certificate ("SipServer") that you previously installed.

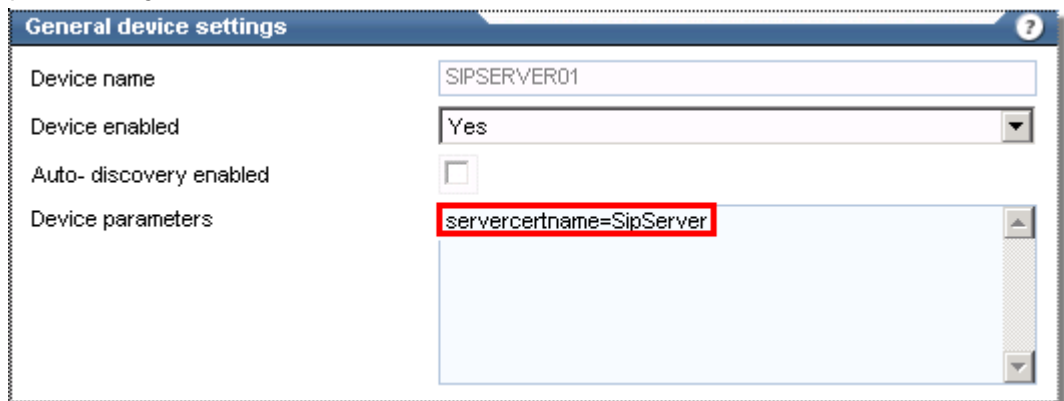
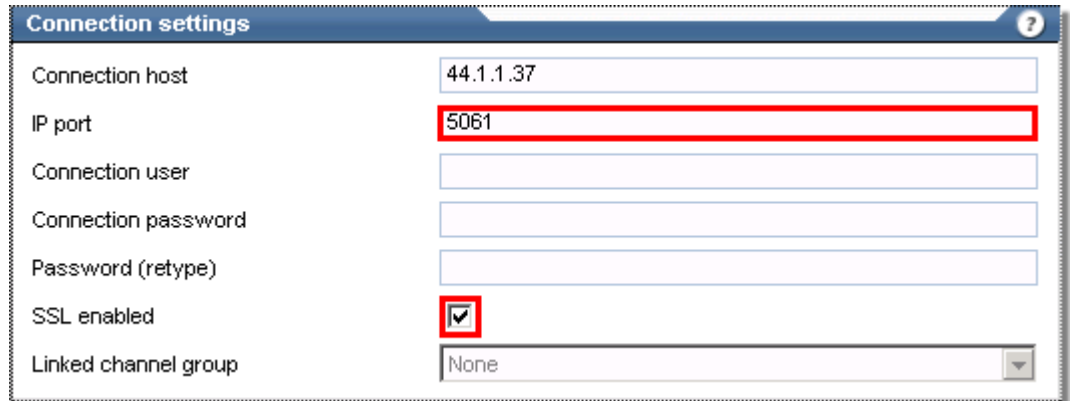


Figure 51: General device settings

5. In the *Connection settings*, do the following:
 - a. Set the **IP port** value to "5061".
 - b. Select the **SSL enabled** check box so that the SIP Server accepts secure connections.



Connection settings	
Connection host	44.1.1.37
IP port	5081
Connection user	
Connection password	
Password (retype)	
SSL enabled	<input checked="" type="checkbox"/>
Linked channel group	None

Figure 52: Connection settings

- Click the **Save changes** button.

6.3.6 Configure the CUCM



This step must be executed by a Cisco-certified engineer and is not described in this manual.

<BLANK PAGE>

7 Configuration

This chapter describes the necessary steps to configure the Cisco/CTI recording solution.

The following topics are covered:

- Linking Targets to Users
- Logging On to the CT Web GUI
- Defining Channel Groups
- Configuring the Cisco Link Controller
- Defining Targets
- Specifying Cisco Call Data



Before starting with the configuration, verify that the CTI Receiver is enabled on the Core Server.

7.1 Linking Targets to Users

Recorded calls for targets can be linked automatically to users. This way, full user management is available for defined recording targets.



Consult the CTI Manual for details about the necessary steps to link targets to users.

7.2 Logging On to the CT Web GUI

To configure and operate the CT recording system, you use the CT Web GUI. This is a web interface in the standard browser window, in which you can configure and monitor CTI-based recording solutions.

The CT Web GUI contains various options (grouped into tabbed menus, or 'tabs' for short) to configure and use the Cisco/CTI recording solution.



In the configuration examples, the Web GUI of CyberTech PRO version 5.3 is used. The Web GUI of CyberTech MYRACLE is similar.

Instructions

1. In the browser window's address bar, type the IP address of the recorder or – when accessing from the recorder itself – type 'http://localhost'.

The login page of the web interface is displayed:

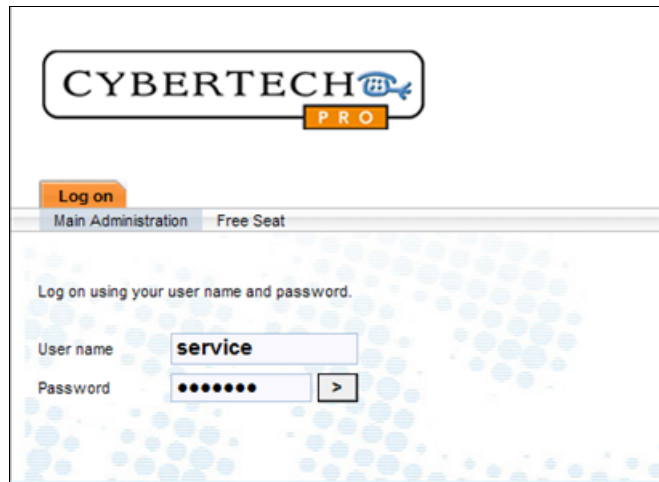


Figure 53: Web GUI – logon

2. Type the user name and password. (Both with *Administrator* rights.)
3. Click the > button to the right of the **Password** field. The main window of the Web GUI appears.

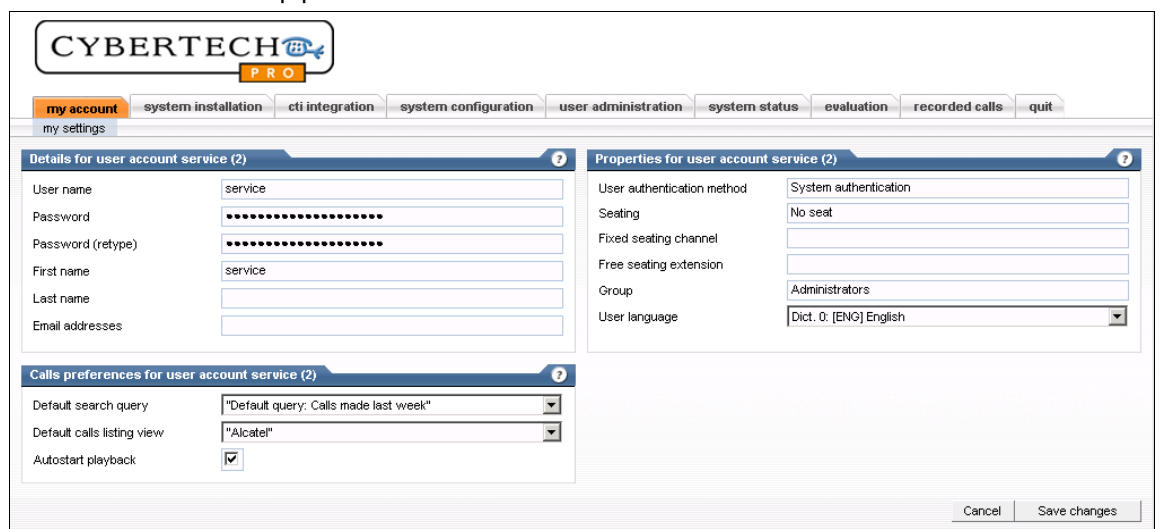


Figure 54: Web GUI – Main window

7.3 Defining Channel Groups

The procedure below describes the necessary steps to create a channel group for the Cisco/CTI Recording Solution.

Instructions

1. In the Web GUI, click the tabs **system configuration** > **channel groups**. The window *Overview of all channel groups* appears:



Figure 55: Channel group overview

2. Click the **+** button to define a new Cisco channel group.

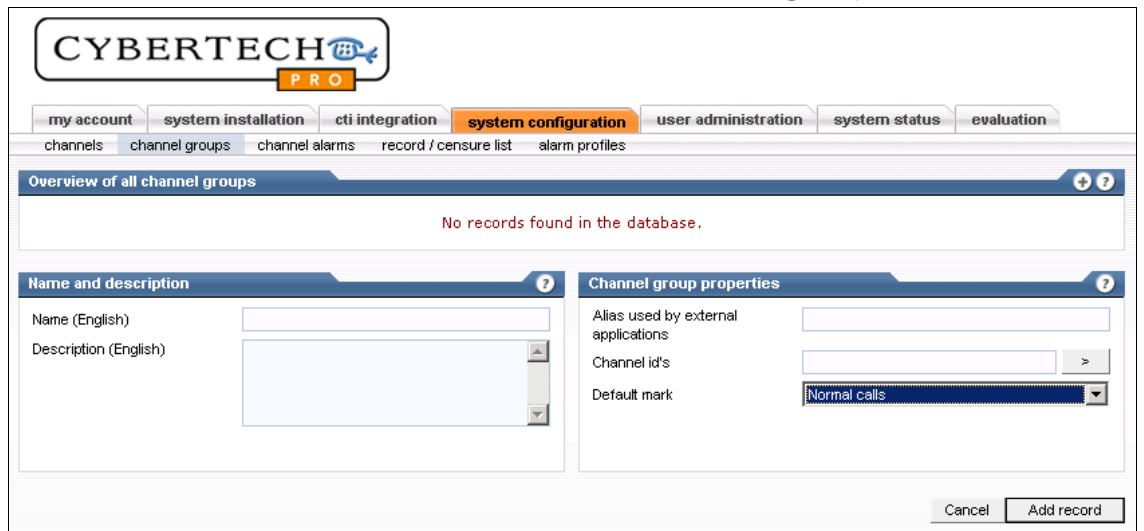


Figure 56: New channel group

3. Enter the following data in the **Name and description** group:

Figure 57: Name and description

- a. **Name:** The name of the channel group.
 - b. **Description:** Text to describe the channel.
4. Enter the following data in the **Channel group properties** group:

Figure 58: Channel group properties

- a. **Alias used by external applications:** Short name to reference the channel group (optional).
- b. **Channel id's:** Reserved channel numbers in the group or "-" to reserve all channels.*
- c. **Default mark:** Select "Normal calls" from the list (if not selected).



- * **When using more than one PBX system, specify the channel numbers you want to include in the group. Otherwise, include all channels.**
- 5. Click the **Add record** button to save the channel group and close the entry window.
 - 6. Note that the newly created channel group is added to the list:

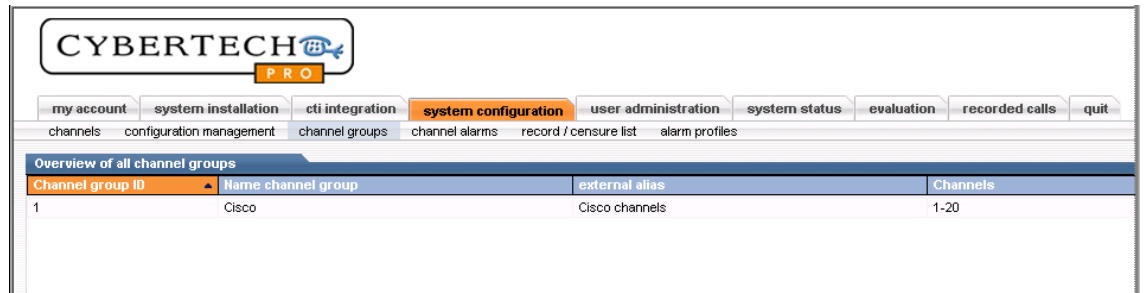


Figure 59: Cisco channel group added

7.4 Configuring the Cisco Link Controllers

The procedure below describes the necessary steps to configure the Cisco Link Controllers by defining properties like name, connection host, and IP port.

Instructions

1. Click the **cti integration** > **devices** tabs to display a list of all currently installed link controllers:

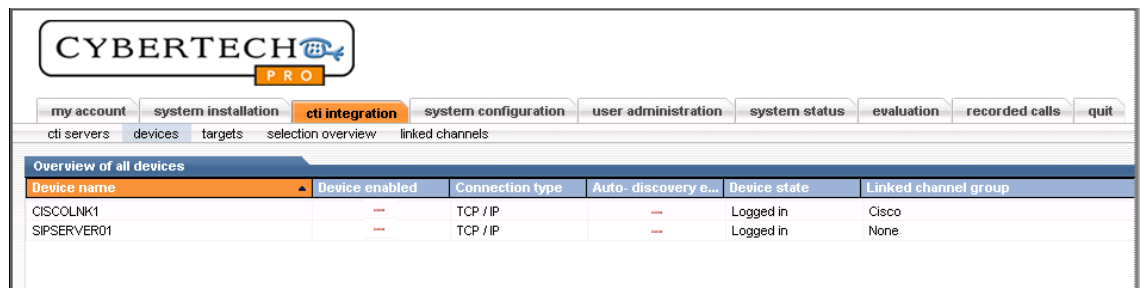


Figure 60: Device overview

2. Verify that the names of the Cisco link controller and SIP Server link controller are displayed in the device overview.
3. Click the Cisco link controller. A window with corresponding device and connection settings appears:

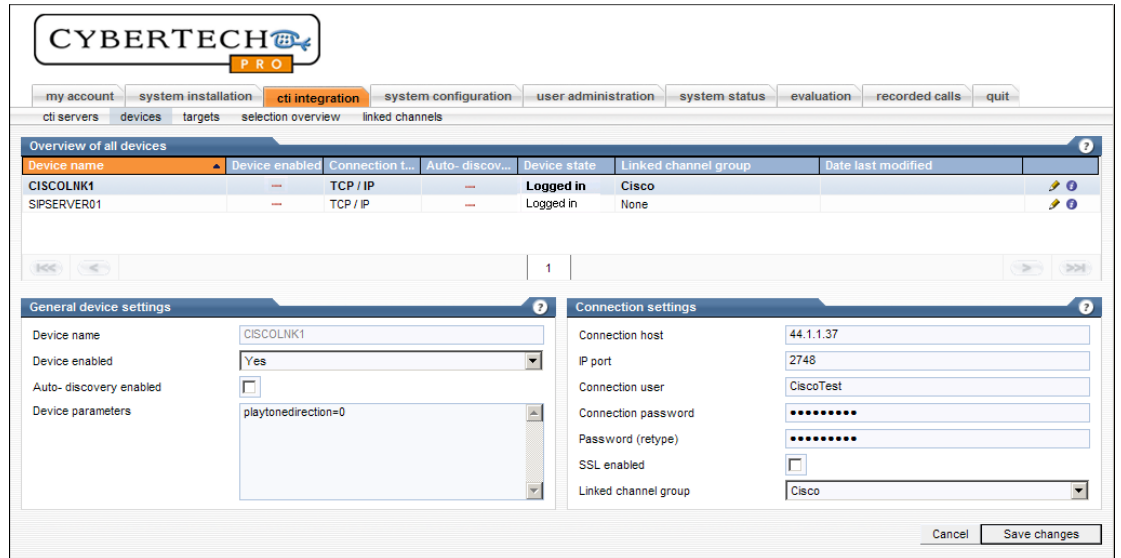


Figure 61: Cisco device and connection settings

4. Add the following settings in the *General device settings* group:

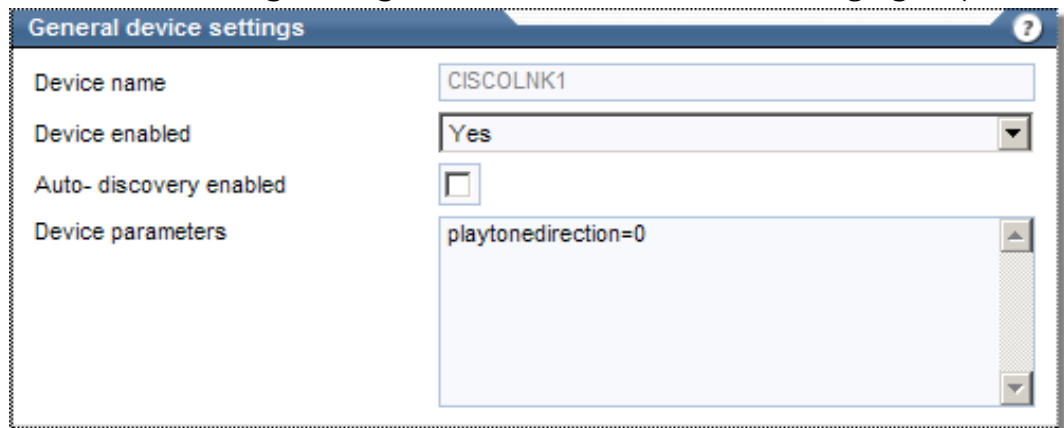


Figure 62: Cisco general device settings

- a. **Device name:** Name of the Cisco link controller
- b. **Device enabled:** Indication that the Cisco link controller is activated. The value of this field must be "Yes" (be sure to set it accordingly).
- c. **Device parameter** PlayToneDirection (optional): Warning tone that is played on handsets when recording is started. Possible values are:
 - 0: Recording warning tone on target extension only (PLAYTONE_LOCALONLY=0)
 - 1: Recording warning tone on non-target extension (PLAYTONE_REMOTEONLY=1)
 - 2: Recording warning tone on both target and non-target extensions (PLAYTONE_BOTHLOCALANDREMOTE=2)

- 3: No recording warning tone (= default setting when left empty) (PLAYTONE_NOLOCAL_OR_REMOTE=3)

5. Add the following settings in the *Connection settings* group:

Figure 63: Cisco connection settings

- Connection host:** IP address of the CUCM.
- IP port:** Reserved port number "2748".
- Connection user:** User name of the CUCM application user.
- Connection password:** Password of the CUCM application user (see section 5.2 'Cisco Prerequisites').
- Linked channel group:** Name of previously created Cisco channel group.

The **SSL enabled** checkbox remains unchecked.

6. Click the **Save changes** button to return to the *Device overview*. Note that the Cisco link controller is now enabled.

Device name	Device enabled	Connection type	Auto-discovery e...	Device state	Linked channel group
CISCOLNK1	✓	TCP / IP	---	Logged in	Cisco
SIPSERVER01	---	TCP / IP	---	Logged in	None

Figure 64: Cisco device settings – enabled

7. Click the SIP Server link controller. A window with corresponding device and connection settings appears:

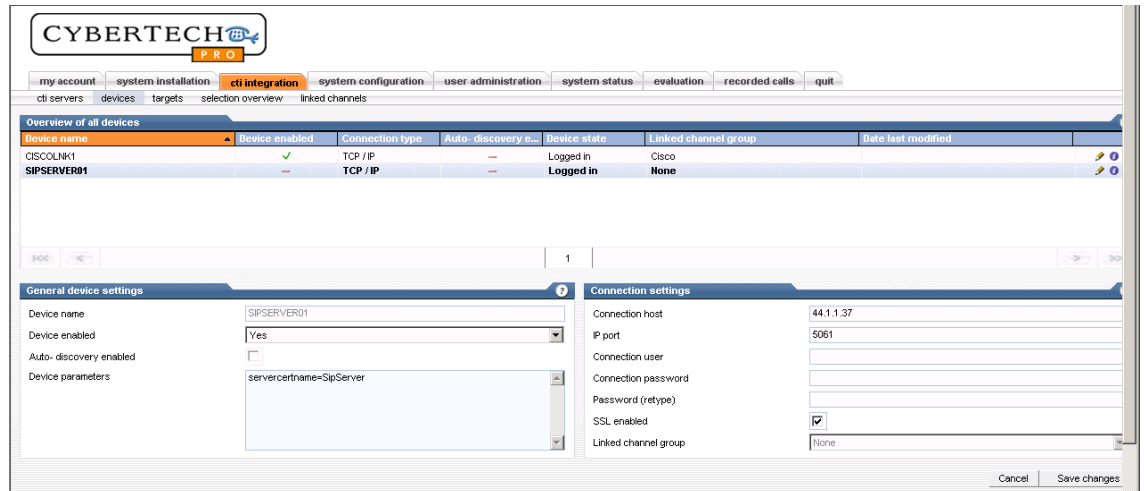


Figure 65: SIP Server device and connection settings

8. Add the following settings in the *General device settings* group:



Figure 66: SIP Server general device settings

- a. **Device name:** Name of the SIP Server link controller
 - b. **Device enabled:** Indication that the SIP Server link controller is activated. The value of this field must be "Yes" (be sure to set it accordingly).
 - c. **Device parameter:** servercertname (optional): name of the server certificate that is used for Secure SIP Trunk (consult section 6.3 'Setting Up the Secure SIP Trunk for details). Set this value to "SipServer".
9. Add the following settings in the *Connection settings* group:

Figure 67: SIP Server connection settings

- a. **Connection host:** IP address of the CUCM.
 - b. **IP port:** Reserved port number. Use one of the following values:
 - "5061" when you use Secure SIP Trunk
 - "5060" otherwise
10. If you use Secure SIP Trunk, select the checkbox **SSL enabled**. The other fields remain empty.
 11. Click the **Save changes** button to return to the *Device overview*. Note that the SIP Server link controller is enabled as well.

Device name	Device enabled	Connection type	Auto- discovery e...	Device state	Linked chan
CISCOLNK1	✓	TCP / IP	--	Logged in	Cisco
SIPSERVER01	✓	TCP / IP	--	Logged in	None

Figure 68: Both devices enabled

7.5 Defining Targets

This section describes the steps to do the following:

- Add new targets
- Monitor target states

7.5.1 Adding a New Target

This section describes the steps to add a target type "Extension" for both the Cisco and SIP Server link controller.



The target registration speed is approximately 10 targets per second.

Instructions

1. Click the **cti integration** > **targets** tabs to display a list of all currently defined targets (if any).

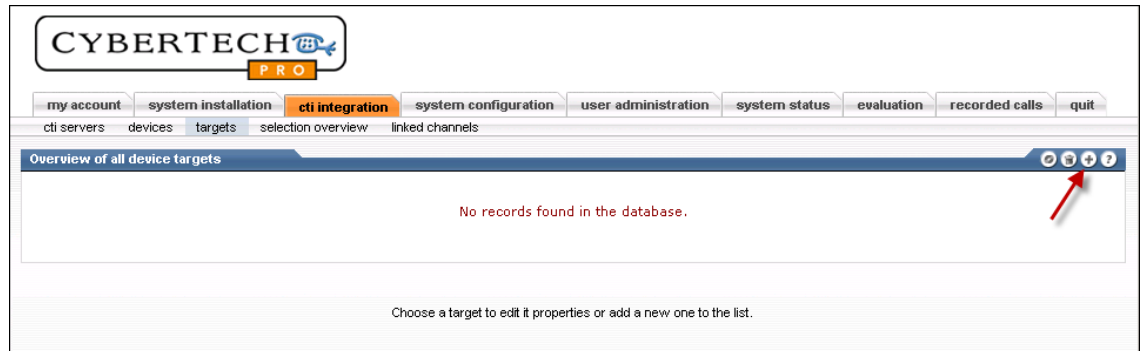


Figure 69: Target overview - empty

2. Click the **+** button to add a new target in the *Add target* window.

Figure 70: Add target for Cisco link controller

3. Add one or more targets of type "Extension" by specifying the following information:
 - a. **Target name(s)**: Name of the target (free text field)
 - b. **Device**: Select the name of the Cisco link controller from the dropdown list
 - c. **Target type(s)**: Type of the target (select "Extension" from the dropdown list)
 - d. **Target value range start**: Number of the target type
 - e. **Target value range end**: Leave empty for single target
 - f. **Target selection**: Select this check box to activate usage of this target

4. Click the **OK** button to save the new target. The target input window closes and you return to the *Target overview* window.
5. Repeat these steps for each extension you want to define for the Cisco link controller.
6. When finished, perform the same overall procedure for the SIP Server link controller.
7. As a result, the targets are added to the target list. The following image contains an example of defined targets:

Target name	Target Selection	Device name	Target type	Target value	Date last modified
1004	---	CISCOLNK1	EXTENSION	1004	2009-11-30
1005	✓	CISCOLNK1	EXTENSION	1005	2009-11-27
1006	✓	CISCOLNK1	EXTENSION	1006	2009-11-30
1007	---	CISCOLNK1	EXTENSION	1007	2009-11-30
1008	---	CISCOLNK1	EXTENSION	1008	2009-11-30
1050	✓	CISCOLNK1	EXTENSION	1050	2009-11-30
3001	---	CISCOLNK1	EXTENSION	3001	2009-11-27

Figure 71: Added Cisco targets

7.5.2 Monitoring Target States

1. From the main window, click the **cti integration > selection overview** tabs. The *selection overview window* opens, with the targets :

Target name	Device name	Target type	Target value	Target state
1005	CISCOLNK1	EXTENSION	1005	Selected
1006	CISCOLNK1	EXTENSION	1006	Selected
1050	CISCOLNK1	EXTENSION	1050	Selected

Figure 72: Selection overview

2. Select the value "All" in both fields **Devices** and **Target types**.
3. Verify that the actual monitoring state for the newly created targets is shown in the **Target state** column (see red rectangle in the figure above).

The applicable target state values have the following meanings:

- **None:** The target has not (yet) been passed to the link controller.
- **Selecting:** The link controller is registering the target at the PBX.
- **Selected:** The target is registered and monitored.

- **Removing:** The target is being removed and will be deleted from the list.
- **Recording:** The target is being recorded.

7.6 Specifying Cisco Call Data

The specific Cisco call data are specified in the file 'extrafields.ini' which you have copied in the preparatory steps as described in section 5.3.2 'Preparatory Steps'.

The file 'extrafields.ini' is located in the folder 'C:\Program Files\cybertech\INI_Files' and looks like the following:

```
[FILTERS]
RawData = 0x00F
Display = 0x00FF

[Fields]
#Reserved Base Numbertypes
3, LastCause,           CVSLCS #
3, AllParties,         CVSAPS # List of all parties that were ever in the call
3, TargetId,           CVSTRG # Recorded target id: Extension
3, PBXCallID,         CVSPCI # Call ID used in PBX system
3, RecordingState,    CVSRST #
#Base numbertypes
3, Extension,         CVSPHN # Called party information (Phone number)
3, CallingParty,      CVSCIP # Calling party information
3, CalledParty,       CVSCEP # The number that was dialed
3, ConferenceParties, CVSCPS # List of parties in conference
```

Figure 73: ExtraFields.ini

In the Web GUI, you specify which call data you want to use in your recordings.

Instructions

1. From the main window, click the **recorded calls** > **column selection** tabs. The *selection overview* window opens:

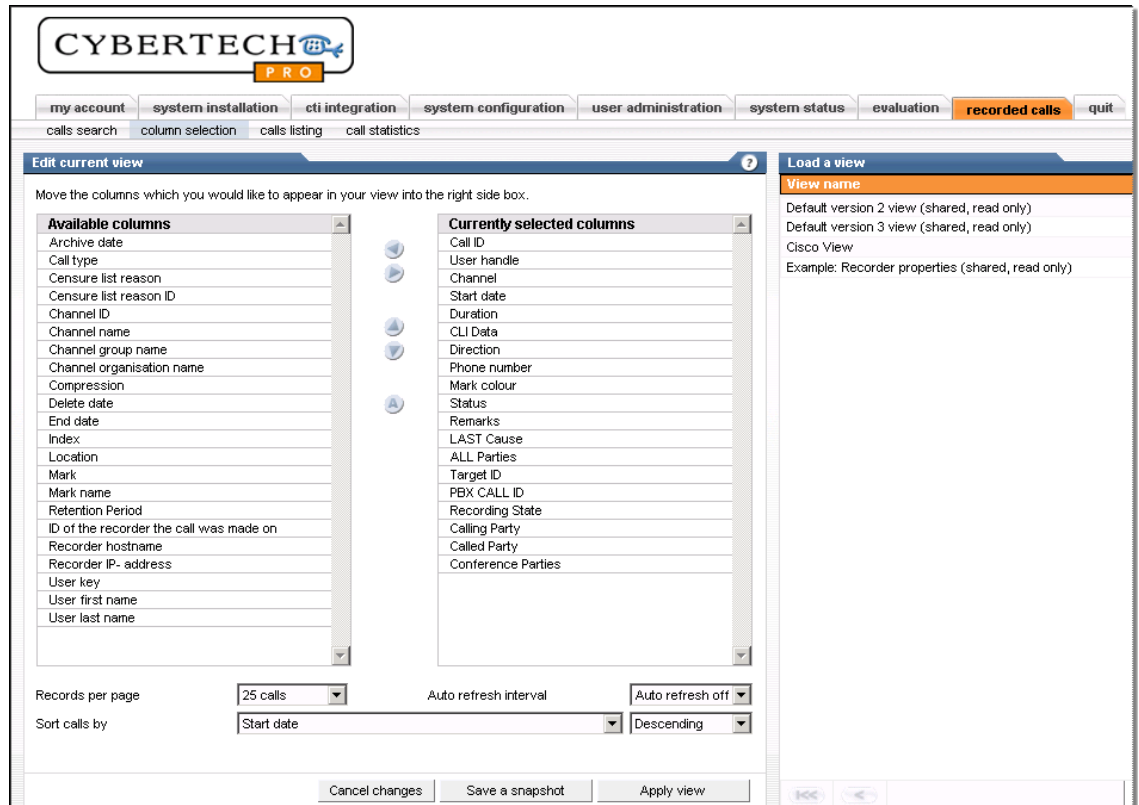


Figure 74: Selection overview

The column **Available columns** display the complete list of available call data. The column **Currently selected columns** represent the call data that are currently in use.

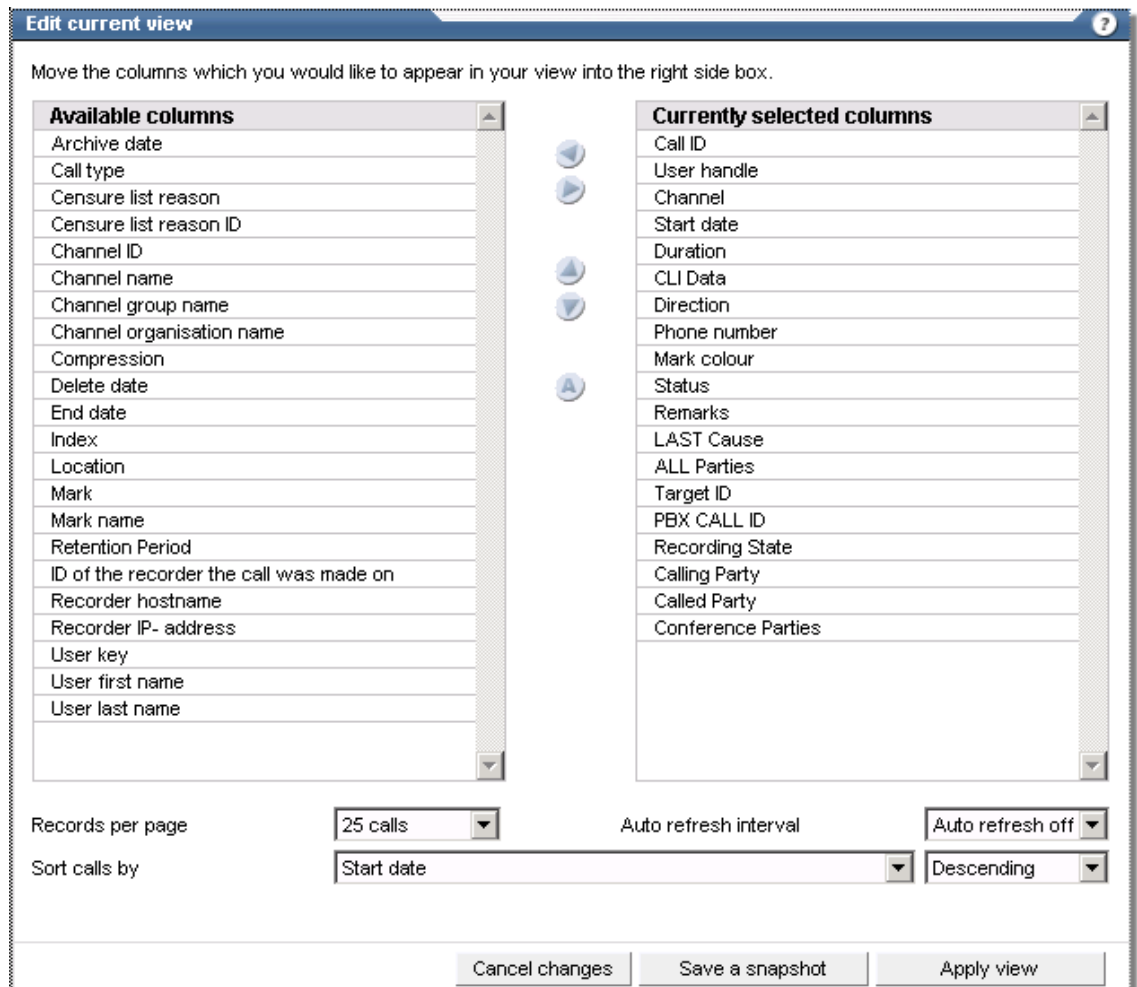


Figure 75: Selection overview: Columns

2. Add a field to be used in recordings by double-clicking it in the left column (or single-clicking it and use the <right> arrow).
3. Delete a field by double-clicking it in the right column (or single-clicking it and use the <left> arrow).
4. Save your view under the name "Cisco View".
5. Click **Apply view** to apply your settings.
6. When you select the subsequent tabs **my account** > **my settings**, you simply select this view to use the call preferences you just specified:

The screenshot displays the CyberTech PRO web interface. At the top, there is a navigation menu with tabs for 'my account', 'system installation', 'cti integration', 'system configuration', 'user administration', and 'sys'. The 'my account' tab is selected, and a sub-tab 'my settings' is also visible. Below the navigation, there are two main sections:

Details for user account service (2)

User name	service
Password
Password (retype)
First name	service
Last name	
Email addresses	

Calls preferences for user account service (2)

Default search query	"Default query: Calls made last week"
Default calls listing view	"Cisco View"
Auto start playback	Remember last used view "Default version 2 view" "Default version 3 view" "Cisco View" "Example: Recorder properties"

Figure 76: Call preferences

<BLANK PAGE>

Appendix A Abbreviations and Terms

This appendix contains an overview of relevant abbreviations and terms used in this manual.

A.1 Abbreviations

Item	Description
BIB	Built-in-Bridge
CCLC	Call Controller Link Controller protocol
CN	Common Name
CSTA	Computer Supported Telephony Applications. Standardised link protocol, used to transfer CTI information
CTI	Computer Telephony Integration
CTRS	CyberTech Recording System
DLU	Device License Unit
DSC	Digital Selective Calling
ESD	Electrostatic Discharges
GUI	Graphical User Interface. A user interface based on graphics (icons and pictures and menus) instead of text.
IP	Internet Protocol
JTAPI	Java Telephony Application Interface
PBX	Private Branch eXchange. Telephone system in an organisation.
PSTN	Public Switched Telephone Network
SCCP	Skinny Client Control Protocol (Cisco proprietary protocol)
SIP	Session Initiation protocol
SRST	Survivable Remote Site Telephony
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol

Table 11: Abbreviations

A.2 Terminology

Item	Description
Agent	Call-centre employee who can log on to an extension.
Agent ID	Identification of an agent who is involved in a call (logged in on a phone).
Answering party	Party who answers a call.
Call Controller	A service linking to the recorder database which reads configuration details for installed CTI Devices. The Call Controller processes all CTI Device messages to determine when to start and stop recording for a specific recording target.
Call ID	Call identification used in a PBX system. Each call is assigned a unique call id by the PBX. It is not unique across multiple PBX systems.
Call ID multi PBX	Unique Call ID for multiple linked PBX.
Called Party	Party that receives a call (called DDI).
Calling Party	Party that initiates a call (called DNIS/CLI).
Conferencing Parties	List of parties involved in a transfer or conference.
Device (target type)	Recordable analogue or digital phone.
Extension (target type)	Recordable line number.
Last Cause	Last cause for a CTI event (On hook, Transfer complete, etcetera).
Last Party	Last party in a call (transferring party) who initiated the transfer or conference to a target.
Link Controller	Interface between CT Call Controller and Cisco call controller.
Monitor Tool	CT Recording Solution Monitor.
Ringling Party	Party a call was ringing on.
Target	Recordable unit (device, agent).
Trunk ID	Identification of a trunk.

Table 12: Terminology

Appendix B Quick Install Reference

This appendix contains an overview for the installation engineer. It contains the main steps for installing, configuring, and testing the Cisco/CTI Recording Solution.

Each step refers to the associated section in this manual where you can find additional information.



Consult section 1.6 'Reference Manuals' for a complete overview of other reference manuals.

The CyberTech contact person must make sure that the CyberTech installation engineer has a copy of the required installation or upgrade data on a CD.

No	Step	Section
Installation		
1.	Install Parrot-DSC Cards	5.3
2.	Install Parrot-DSC firmware	5.4
3.	Load license information	5.5
4.	Add Cisco-specific call data	5.6
5.	Update CTI_Receiver .exe	5.7
6.	Install CT Cisco CTI Integration Software	6.1
7.	Perform post-installation copying	6.2
8.	Setting up Secure SIP Trunk	6.3
Configuration		
9.	Link users to targets	7.1
10.	Define a channel group in the recorder	7.3
11.	Configure the Cisco Link Controllers	7.4
12.	Define targets	7.5

Table 13: Quick Install Reference

<BLANK PAGE>

Appendix C Cisco Configuration Settings

This appendix contains checklists that the Cisco-certified engineer can use to verify that all client-specific preconditions are met for successful connectivity.

It contains the following checklists:

- CUCM Configuration checklist
- Open Port Configuration

C.1 CUCM Configuration Checklist

This checklist contains a CUCM configuration checklist for advanced users.

It comprises the following parts:

- Generic steps (first part)
- Specific steps that depend on how the SUP Trunk link to the CyberTech SIP Server Link Controller is used:
 - Normal use
 - Use with secure SIP
- Generic steps (second part)

C.1.1 Generic Steps (part 1)

1. Enable the **Cisco CTI Manager** service on the CUCM.
2. Create an application user for CUCM access for JTAPI.
3. Write down the username and password for this user.
4. Put all Devices for recording in the **Controlled Devices** list for this user.
5. Add *at least* the following **Roles** for the permissions for this user:
 - "Standard CTI Enabled"
 - "Standard CTI Allow Call Recording"

C.1.2 Normal Use of the SIP Trunk Link

1. Alter or create a SIP trunk Security profile.
2. Set the settings to: "Non Secure" and put the **Outgoing Transport Type** to "TCP" (default) or "UDP" (depending on Cybertech SIP trunk configuration settings).
3. Leave the value of **Incoming Port** at "5060".
4. Select all checkboxes starting with **Accept**.
5. Save the Security Profile.

6. Create a new SIP trunk that points to the IP address of the Cybertech SIP server.
7. Set **Calling Line ID Presentation** to "Allowed".
8. Set **Calling Party Selection** to "Allowed".
9. Use port 5060.
10. Select the **SIP Trunk Security Profile** you just created/alterd.
11. Select the SIP profile. If you did not change the system default settings, you can select the standard SIP profile.

C.1.3 Use with Secure SIP

1. Create a new SIP trunk Security profile.
2. Set the **Device Security Mode** to "Encrypted". The **Incoming Transport Type & Outgoing Transport Type** will be set to "TLS" automatically.
3. For **X.509 Subject Name** enter the **Name** of the server certificate used for encryption. (The default value is "SipServer" when using the CyberTech certificate generator.)
4. Set the **Incoming Port** to "5061".
5. Select all checkboxes starting with **Accept**.
6. Save the Security Profile.
7. Create a new SIP trunk that points to the IP address of the Cybertech SIP server.
8. Set **Calling Line ID Presentation** to "Allowed".
9. Set **Calling Party Selection** to "Allowed".
10. Use port 5061.
11. Select the secure **SIP Trunk Security Profile** you just created.
12. Select the SIP profile. If not changed from system defaults, the standard SIP profile can be selected.

C.1.4 Generic Steps (part 2)

1. Create a new **Route Group** for the Cybertech SIP trunk.
2. Create a new **Route List** for the new Route Group.
3. Create a new **Route Pattern** for the new Route List, with a new extension (such as "4101").
4. Use "OnNet" for **Call Classification**.
5. Disable all checkboxes directly below **Call Classification**.
6. Allow all **Connected Party Transformations**.
7. Create a recording profile for the Cybertech SIP server Link Controller (SIP trunk) that points to the number created in the route pattern.
8. Enable the **Built In Bridge** on the devices that need to be recorded.

9. Be sure the **Device** only uses G711, G729, or G722 by selecting/creating the correct **Regions** and **Device Pools**.
10. In the **Directory Number Information**, edit the **Line Appearance** for each device. Do this for every DN that needs to be recorded.
11. Change the **Recording Option** to "Application Invoked Call Recording Enabled".
12. For the **Recording Profile**, select the newly created recording profile that points to the Cybertech SIP server.

C.2 Open Port Configuration

This checklist describes the open port configuration for the Cisco Link Controller, the Call Controller and the SIP Server.

The arrow symbols in the table have the following meanings:

- Outgoing
- ← Incoming
- ← → Incoming / Outgoing

No	Description	Ports to open	Protocol	YES/NO	Remarks
Cisco Link Controller					
1.	JTAPI →	2748	TCP		
2.	JTAPI ←	2789	TCP		
3.	Communication with the call controller ← →	4246	TCP		
Call Controller (v3 or higher)					
4.	Communication with the CTI receiver ← →	4245	TCP		
5.	Communication with the link controller and the SIP Server ← →	4246	TCP		
6.	Communication with the database ← →	3306	TCP		
SIP Server					
7.	SIP ← →	5060	UDP/TCP		
8.	Secure SIP	5061	TCP		
9.	Trunk	10501	TCP		
10.	Trunk	10502	TCP		

No	Description	Ports to open	Protocol	YES/NO	Remarks
11.	Communication with the call controller ← →	4246	TCP		

Table 14: Open Port Configuration



Consult the 'CTI OS Hardening Manual' for details about port configuration.

Appendix D Troubleshooting

Error messages

Consult the document 'CT Recording Solutions R5 - CTI Manual' for an overview of error messages.

FAQs

Consult www.cybertech-int.com for an overview of frequently asked questions.

Contact information

When encountering any problems during system installation/configuration and/or testing, please refer to:

1. Your local installation partner
2. CyberTech International – Global Support:
globalsupport@cybertech-int.com or +44 203 147 4997

Version history

Date	Version	Remark
11-06-2009	1.0.5-4	Initial release
16-12-2009	2.0	<ul style="list-style-type: none"> • Redesigned & restructured to reflect new standard layout • Upgraded to CUCM 7 • Upgraded to CTRS 5.4 • Upgraded to Cisco Active IP installer kit 3.2 • Added: Setting Up Secure SIP Trunk • Added/modified: Appendixes

Table 15: Version History