

Verint® Enterprise Recording™

Recorder Configuration and Administration Guide

Document Revision 1.75

VERINT.

© 1992–2025 Verint Systems Inc. All Rights Reserved Worldwide.
Confidential and Proprietary Information of Verint Systems Inc.

All materials (regardless of form and including, without limitation, software applications, documentation, and any other information relating to Verint Systems, its products, or services) are the exclusive property of Verint Systems Inc.

This document contains confidential and proprietary information of Verint Systems Inc. and may not be distributed to persons or organizations for which it is not intended. Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Verint Systems Inc. is strictly prohibited. By providing this document, Verint Systems Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice. Features listed in this document are subject to change. Contact your Verint representative for current product features and specifications.

Any third party technology that may be appropriate or necessary for use with the Verint Product is licensed to you only for use with the Verint Product under the terms of the third party license agreement specified in the Documentation, the Software or as provided online at <https://www.verint.com/third-party-license/>. You may not take any action that would separate the third party technology from the Verint Product. Unless otherwise permitted under the terms of the third party license agreement, you agree to only use the third party technology in conjunction with the Verint Product.

The Verint Systems Inc. products are protected by one or more U.S., European or International Patents and other U.S. and International Patents and Patents Pending.

All marks referenced herein with the ® or ™ symbol are registered trademarks or trademarks of Verint Systems Inc. or its subsidiaries. All rights reserved. All other marks are trademarks of their respective owners.

Visit our website at www.verint.com/intellectualpropertynotice for updated information on Verint Intellectual Property.

ITS, ITSNETRIX, BT Netrix and BT Unified Trading are registered trademarks of BT, plc.

IPC, the IPC name and IPC logo are trademarks of IPC Systems, Inc.

Document Revision 1.75
Published June 20, 2025

Customer Engagement Solutions™

Contents

About this guide	15
Getting started with recorders	26
Overview for the Recorder	27
Configuration and administration	29
Enterprise Manager features	29
Recorder Manager features	30
Recording configuration workflows	32
Trader recording	32
Workflow: IP-based voice and video recording	33
Voice recording	35
Workflow: Station-side TDM recording	36
Trunk-side TDM recording	36
Workflow: Mixed TDM trunks and IP trunks recording with service observe	36
Workflow: Screen recording	38
Workflow: Integrate Dialer integration	39
Shared screens for recording configuration	40
Install and configure Archive	41
Configure recording	42
Deployment overview	43
Configure the recording environment	44
Switches and third-party devices	44
Set up Recorder roles and associations	44
Associate a server role with a Recorder	45
Associate a Recorder with the Integration Service	46
Configure the Integration Service role	48
Set up voice and video recording	49
Create a phone data source	49
Create a collection data source for gateway recording	61
Create and edit member groups and extensions	63
Create a member group	66
Compliance station extension member group settings for TDM	67
Compliance trunk span member group settings for TDM	68
IP extension pool member group settings	71
Trunk span recording resource member group settings	75

Extension recording resource member group settings	75
Selective extension pool member group settings	77
Dedicated extension pool member group settings	78
Multiple registration extension pool member group settings	79
DMCC recording group member group settings	81
Gateway side correlation pool member group settings	83
Device Location member group Settings	89
Amazon Connect member group settings	90
Microsoft Teams Group member group settings	90
AudioHook Recording member group settings	92
Streaming Media Capture Pool member group settings	93
Stream Recording member group settings	97
Skype Recording member group settings	98
Skype Interaction Capture member group settings	100
Configuring Media Proxy member groups to support high availability and load balancing	102
Example: Geographical routing and failover with Skype member groups	103
Set up screen recording	106
Create a LAN data source	107
Set up workstations and workstation groups	109
Create workstation groups	110
Define workstations	112
Create a workstation group and assign workstations	113
Assign workstations to workstation groups	113
Unassign workstations	114
Create subnets	114
Set up a dialer integration	116
Create a dialer data source	116
Create and edit phones for dialers	123
Create member groups for dialers	123
Set up phones and extensions	124
Create and edit phones/extensions	125
Set a default recording mode	129
Map workstations to phones	130
Edit multiple extensions	130
Create a range of extensions	131
Generate extension numbers or trunk group members	133
Delete extensions	134
Assign a range of IP extensions	134
Edit IP extensions	136
Batch edit IP extensions	137

Unassign IP extensions	138
Unassign a range of extensions	139
Create and import large numbers of extensions	140
IP recorder extensions	141
Recorder extensions	141
View IP recorder extensions	142
View TDM recorder extensions	142
Create employees and add employee IDs	143
Create an employee	143
Import employee from an existing source	145
Map employees to data sources	145
Add employee mappings	146
Edit employee mappings	147
Create a recording profile	149
Edit a recording profile	151
Create data source groups	154
Create and edit data source groups	154
Upload data source group information	156
Set up data sources, member groups, and devices for radio recording	158
Create a Radio data source	158
Create a Devices Pool member group for a Radio data source	162
Devices Pool member group settings	162
Set up devices for radio recording	164
Create or edit devices for radio recording	164
Delete devices for radio recording	167
Create a range of devices for radio recording	168
Assign radio devices to a member group	170
Create and assign a range of radio devices to a member group	175
Unassign individual radio devices from a member group	177
Unassign a range of radio devices from a member group	178
Set up for Ingestion Recording	180
Set up individual Recorders	181
Recorder configuration workflow	182
Launch Recorder Manager	183
Initial setup	183
Recorder setup	184
Standardize server name references	184
Configure Recorder settings	184
Call buffer setup	187
Relocate the call buffer	187

Create a new call buffer location	188
Configure compression	188
Disk manager setup	191
Configure disk manager	191
Monitor disk drives	192
Configure database settings	194
View database settings	194
Edit a contact database or text analytics database	195
Reprocess call date ranges	196
TDM recording setup	198
Supported voice cards	198
Configure DP voice cards	201
Modify DP voice card properties	201
Update DP voice card channels	202
Modify the trunk protocol on a T1 voice card	204
Modify the trunk protocol on an E1 voice card	204
Configure PCM32 voice cards	205
Modify PCM32 voice card properties	205
Update PCM32 voice card channels	206
Configure DT voice cards	208
Modify DT voice card properties	209
Update DT voice card channels	211
Configure NGX voice cards	213
Modify NGX voice card properties	213
Update NGX voice card channels	215
Configure LD voice cards	217
Modify LD voice card properties	217
Update LD voice card channels	217
TDM voice card reference	219
TDM voice card properties reference	219
TDM voice card channel properties reference	225
T1 trunk protocols reference	228
E1 trunk protocols reference	229
Voice cards and channels	230
Manage voice cards	230
View voice cards	230
Copy voice card configuration	232
Identify a voice card	233
Delete a voice card	233
Add a new voice card	234
Replace a voice card	234

Modify an existing voice card	235
Manage voice card channels	236
View voice card channels	236
Configure voice card channels	236
Edit voice card channels	237
Copy voice card configuration from the Channels screen	237
Revert channel settings	238
Edit tags for voice card channels	238
IP Recorder and IP Recorder Video configuration	240
Update BIOS settings for Windows 2012 R2	240
Configure network interface cards	240
Configure capture settings for NICs	241
NIC settings for interception recording	242
Configure network cards and filters	243
Configure network protocols	247
Configure IP recording settings	249
IP Analyzer configuration	254
View Analyzer	254
Manage Analyzer	255
Analyzer setup	256
Configure Call Control	257
View Call Control information	258
Create a Call Control Recorder Group	259
Edit a Call Control Recorder Group	260
Backup and recover for recorder configuration	262
Back up the Recorder configuration	262
Recover the Recorder configuration	263
Start and stop Recorder components	265
Start and stop components	265
Edit component start and stop settings	266
Restart web services	268
Set up attributes, tagging, and recording rules	269
Attributes configuration workflow	270
Attributes	271
Standard attributes	272
Create, edit or delete an attribute	278
CTI tagging	282
Identify CTI data	282
Create Custom Data fields	291
Map Custom Data to an attribute	292

Map attributes to an adapter	294
Attribute external name syntax	295
Concatenate field values into an attribute	301
Limitations of attribute mapping	302
Recording rules	303
Set up recording rules	303
Recording rules configuration workflow	303
Configure server-level settings for recording rules	304
Create a recording rule	305
Conditions in a rule	310
Create conditions for a recording rule	311
Create a schedule for recording rules	312
Validate regular expressions	313
Delete a rule	319
Configure CTI adapters	320
About CTI adapters	321
Configure a CTI adapter	322
Create an adapter	322
Edit an adapter	324
Delete an adapter	324
Start, stop, or restart an adapter	325
Recover calls for an Amazon Connect adapter	325
Configure adapter custom attributes	326
Adapter behavior and troubleshooting	330
Configure Secure Communication	331
Enable secure communication between the RIS and remote recorders	333
Configure high availability	334
High availability	335
Recorder Redundancy	335
Integration Service Redundancy	335
Choosing a Location for your Main Integration Service in N+M	335
Screen recorder failure	336
Backup servers	336
Recorder redundancy	338
N+N	338
Supported environments	339
Full Duplicate Recording	340
Load balancing in N+N	341
Configure N+N Recorder redundancy	341
Promote backup calls	344

Disable recording-based failover marking	346
N+M	347
Load Balancing in N+M All Shared	348
Real-time Monitoring	349
Configure N+M redundancy	349
N+N and N+M redundancy with IP Analyzer	358
Configure redundancy for IP Analyzer for N+N	359
Configure redundancy for IP Analyzer for N+M	360
Integration Service redundancy	361
1+1	361
Configure Integration Service 1+1 redundancy	363
Recorder Integration Service failover from main to back up	364
N+1 redundancy with SIP trunk recording	365
Troubleshooting	366
Gateway recording	366
Recording and RTM loss in Recorder Integration Service failover	366
Scaling for SIP and SIPREC traffic with RAPS	367
Scaling solution for SIP and SIPREC environments	368
Site architecture	369
Security	370
Message flows with RAPS	371
RAPS configuration	373
Enable RAPS roles	373
Configure Data Sources and Member Groups	374
Configure adapters	374
Resilience and Redundancy	376
Failure Modes	377
Advanced configuration	379
Configure pause recording on hold	380
Configure RTP detection	381
Record terminal sessions	382
To record terminal sessions	382
Limitations (screen capture of multiple sessions and Published Applications)	383
System Tools	385
Launch System Tools	385
Configure the Interaction Capture Control API (eQuality Connect V6) Adapter	386
Device aliasing	391
Registration and device failures	392
Configure Recorder generated comfort noise	393
Configure SIP Interception	394

Overview	395
Configure the Recorder	396
Custom SIP tagging	398
Change the default SIP signaling port number	399
Add additional SIP signaling port numbers	401
Use the Configuration Checker	405
Configuration Checker	406
Select your recording environment	407
Check configurations	408
View Configuration Checker details	409
Reference	412
Archive	414
Audio quality statistics events (AQS)	415
Enable AQS	418
Conditional Custom Data	420
Conditions	421
CTI-based Recorder selection	423
Custom Data	424
Data sources	425
Delivery	426
Dialers	427
Extension recording modes	429
Extensions	430
Fallback modes	431
Hunt group	432
Integration Service	433
Interception	435
IP recording	438
Member groups	441
Multiple Recorders and high availability	444
NIC teaming	445
Limitations of NIC teaming	445
Phones	447
Queues	448
Real-Time Monitor	449
Recorder control types	450
Recording resources	452
Roles	453
RTP detection	454
Screen Recording	455

Seating arrangements	458
Selective extension pools	459
Shared screen Recorders	460
Shared lines	461
SIP trunk recording	462
Subnets and subnet masks	464
TDM recording	465
Trunk span groups	467
Video stitching of separate recordings	468
Workstations and workstation groups	469
Administration	470
Administer the Recorder	471
Manage Workstations	471
Edit and Batch Update Workstations	471
Edit Multiple Workstations	472
Batch Update Workstations	472
Create View Filters	474
Create and Edit Employee Filters	474
Create and Edit Phone Filters	475
Filter the Workstations View	476
Export and Import Data Source Settings	478
Export Data Source Settings	478
Import Data Source Settings	479
Review the Status of Data Source Imports	480
Delete a Data Source	482
System status, logs, and alarms	483
Recorder and component status screens	484
View a Recorder's status summary	484
Edit status summary thresholds	487
View System Monitor status	489
View capture status	489
View Recorder capture status	490
View channel status (TDM capture)	493
View extension status (IP capture)	495
View workstation status	498
View Integration Service status	499
Query Integration Service status	506
View the status of other components	509
System logs	511
System log manager	511

View system logs	513
Customize the log viewer display	514
Alarms	515
View active alarms	515
Clear alarm history	516
Recorder troubleshooting	517
Troubleshooting Recorder issues	518
General issues	518
Discrepancy in displayed call duration or percentage recorded	519
No employee ID tagged	519
Workstation not recording	519
Workstation recorded does not appear to match voice recording	519
Recordings occur when none are required	520
Integration Service not tagging	520
Cisco DMS not recording	520
All Cisco recordings are “noise”	520
Long calls	520
Missing recordings	520
Connect API events not being processed	520
Recorder fails to update components	520
Interaction playback between two employees, when one is on hold, has replay issues during hold times	521
One or more of the media files that are part of the interaction are not found	521
Software issues	522
Unable to delete workstation	523
Find lost calls	523
Activity auditing	523
Short IP call segments are not being recorded	525
TDM recording issues with NGX cards	525
Reset channel mechanisms for NGX cards	541
Checksum mismatches	542
Network Interface Card (NIC) name displays symbols	545
Hardware issues	545
Voice cards	545
Wiring	547
Channel assignment	548
Configuration reports	551
Log Manager utility	552
Use Log Manager	552
Import formats for data sources	556

General guidelines for importing data sources	557
Use the data source import utility	559
Import into a data source	559
Schedule a data source import	559
Delete existing data source members while importing	560
Data source import formats	561
Data source group import/export formats	564
Application data source import formats	565
Sample Application data source import formats	571
Phone and Trader data source import formats	573
Create/Update Phone data source import formats	573
Create/update IP Extension Pool member group	576
Create/update IP Extension Pool phones/extensions	577
Create/update Station-side Extension member group	578
Create/update Station-side extensions	579
Create/update Extension Trunk Span	580
Create/update Extension Trunk Span members	581
Create/update Trunk Group Trunk Span	582
Create/update Trunk Group Trunk Span members	583
Create/update Multiple Registration Extension Pool group members	584
Trader data source import formats	584
Switch-specific data source import formats	586
Create/update Alcatel Trunk Span	586
Create/update Alcatel Trunk Span members	588
Create/update Aspect Trunk Span	588
Create/update Aspect Trunk Span members	590
Create/update Generic Trunk Span	590
Create/update Generic Trunk Span members	592
Create/update Avaya NES Trunk Span	592
Create/update Avaya NES Trunk Span members	593
Switch-specific import working examples	594
LAN data source import formats	600
Importing workstation groups	600
Importing workstations	601
LAN-specific import working examples	602
System maintenance	604
Perform system maintenance	605
Perform routine maintenance	605
Follow a preventative maintenance schedule	606
Daily tasks	606

Weekly tasks	607
Monthly tasks	607
Perform hardware maintenance	608
Change voice cards/NICs	608
Replace a hard drive	609
Duplicate and combine Recorders	611
Recorder maintenance mode	612
Put a server in or out of maintenance mode	614
Maintenance mode reference	615
Recovery procedures for a site Recorder	617
Back up existing settings and data	618
Install software and restore data on the new server	619
Test the new Recorder	621

About this guide

This guide describes how to set up and administer recording, at both the enterprise and recorder levels. In describing the process for configuring adapters and completing recording integrations, this guide provides instructions that are independent of specific switch and vendor considerations.

Additional *Integration Guides* document integrations for specific switch-computer telephony integration (CTI) combinations—check with your Verint Systems representative to obtain the latest guides.



Any references in this guide to a “multi-tenancy” or “multi-tenant” environment are only relevant for a Cloud/SaaS deployment of the product.

Intended audience for this guide

The *Verint® Enterprise Recording™ Recorder Configuration and Administration Guide* is intended for the following readers:

- Enterprise administrators and system integrators
- IT staff responsible for system maintenance
- Verint Systems Field Services, partners, and support personnel

Where to begin

To determine the sequence of tasks that you need to complete to configure your particular recording environment, go to [Recording configuration workflows \(page 32\)](#). If your environment includes a particular Verint-supported CTI combination, you need the associated *Integration Guide* as well (contact Verint Field Services).



This guide focuses on tasks related to recording configuration and administration. Links to the next task to complete and to related reference material are provided at the end of most procedures.

Documentation feedback

We strive to produce the highest-quality documentation products and welcome your feedback. If you have comments or suggestions about our guides or help, you can email us. With your feedback, include the following information:

- Document name and revision number or title of help topic and product version
- Your suggestion for correcting or improving the documentation

Send your messages to userguides@verint.com.

The email address is only for documentation feedback. If you have a technical question, contact Technical Support.

Technical support

Our goal at Verint Systems is to provide you with the best products backed by a high-quality support network with various resource options. Verint Systems Technical Support services include email and telephone support.

To learn more about the support options that best suit your needs, visit us at [Customer Engagement Support](#).

Verint Learning

In addition to documentation, help, and support services, Verint also offers both instructor-led and self-paced learning options to suit your specific needs.

To learn more about available training options from Verint, visit us at connect.verint.com/learn.

Document revision history

Revision	Description of changes
1.75	<p>Application data sources can now be exported and imported.</p> <ul style="list-style-type: none">• Updated all topics related to importing and exporting data sources to include supported types: Phone, Application, LAN (Screen), Radio, and Trader.• Added "Application data source import formats"• Added "Sample Application data source import formats"• Renamed "Importing data sources" to "General guidelines for importing data sources"• Renamed the chapter "Data source import formats" to "Import formats for data sources"• In "Data Source import formats" and "Create/update Phone data source import formats", added fields "Time zone", "Local time tagging mode" and "Associated role" to the table.

Revision	Description of changes
1.74	Modified the N+N Dual Forking section of the Resilience and Redundancy topic.
1.73	Added Redaction and Morphing options in <i>Create a recording rule</i> .
1.72	In <i>Configure compression</i> , updated information that the Inline Compression option must always be enabled.
1.71	In <i>Streaming Media Capture Pool member group settings</i> , added the Participant Configuration setting to support capturing the agent segment of consultations, transfers, and conferences.
1.70	<ul style="list-style-type: none"> • In <i>Configure Interaction Capture Control API (eQuality Connect V6) Adapter</i>: <ul style="list-style-type: none"> ▪ Renamed Recorder Integrations API to Interaction Capture Control API ▪ Added the Response timeout (milliseconds) field • In <i>Streaming Media Capture Pool member group settings</i>, added the "Associated Recording Profile" section, which allows multiple profiles in the same member group for capturing the agent segment of consultations, transfers and conferences.
1.69	In <i>Identifying CTI Data</i> , added the section " <i>Example 2: CTI events in unknown array index</i> " to describe how to map CTI event data when it is contained in an unknown array index.
1.68	Updated the procedure in <i>Enable AQS</i> .
1.67	In <i>Configure network cards and filters</i> , provided additional guidance when configuring the UDP port range used for delivery recording.
1.66	<p>In <i>Create a Phone Data Source</i>, updated the Keep Duplicate Recording option. Updated Audit Viewer topics to describe the change in behavior for Time of Event field (date range is required and cannot exceed 6 months). Updated <i>IP extension pool member group settings</i> to include NEC NEAX for the Full Delivery option of the Recorder Control Type setting. In "<i>Resilience and Redundancy</i>", added the first note about SIP traffic load balancing on a RAPS node.</p>
1.65	Added content about viewing Audio Quality Statistics results in Automated Verification and updated the Audio Quality Statistics event score ranges in <i>Audio quality statistics events (AQS)</i> .
1.64	In <i>Set up Recorder roles and associations</i> , noted that you must enable the <i>Streaming Service</i> role on all servers that have the <i>Content Server</i> server role enabled.

Revision	Description of changes
1.63	<p>Added new data source options for redaction and morphing to the following topics:</p> <ul style="list-style-type: none"> • <i>Create a phone data source</i> • <i>Create a dialer data source</i> • <i>Create a Radio data source</i>
1.62	<ul style="list-style-type: none"> • In <i>Multiple registration extension pool member group settings</i>, added the "Station Monitoring" option. • In <i>Stream Recording member group settings</i>, removed the "WebSocket Target URL" option, which is now available in the Twilio data source.
1.61	<ul style="list-style-type: none"> • Added Streaming Media Capture Pool member group settings. • Added an Advanced Parameters section to all member groups settings. • Added the DMCC UI control to Multiple Registration Extension Pool member group topic. • Added the "Recording Beep Tone" option to the following member groups: <ul style="list-style-type: none"> ▪ DMCC recording group member group settings ▪ Multiple registration extension pool member group settings ▪ Extension recording resource member group settings
1.60	Added Stream Recording Member group settings.
1.59	In <i>Recorder troubleshooting</i> , in "Hardware issues," under "Voice Cards," added a note that the "Secure Boot" BIOS option needs to be disabled.
1.58	In "Multiple registration extension pool member group settings," added DMCC Control Type.
1.57	<ul style="list-style-type: none"> • Under <i>Advanced configuration</i>, changed the name of the <i>Configure the Connect Adapter</i> section to <i>Configure the Interaction Capture Control API Adapter</i>, and updated the section. • Under <i>Recorder Redundancy</i>, updated the <i>Load Balancing in N+M All Shared</i> section.
1.56	Incorporated BT content into Verint-branded version of the guide.

Revision	Description of changes
1.55	<ul style="list-style-type: none"> Under "Identify CTI data," in the SIPREC event example, corrected the white space in the example. In "Standard attributes," updated the descriptions of the Number of Holds and Time on Hold (seconds) attributes. Updated the descriptions of delete behavior options in "Configure server-level settings for recording rules."
1.54	<ul style="list-style-type: none"> Removed note about Capture Verification limitation around Avaya phone data sources with back-office contact policy type in <i>Create a phone data source</i>. Minor changes.
1.53	Clarified in "Call buffer setup" that the call buffer cannot be located a remote SAN or on a remote server.
1.52	Altered the text in the "Recorder Integration Server failover from main to backup" topic.
1.51	<ul style="list-style-type: none"> Removed sentence indicating number of configured phones must not exceed the number of recording resources from the "Selected extension pool member group settings" topic. Added this sentence to the "Dedicated extension pool member group settings" topic. Modified "Minimum Session Length" description in the following topics: Create a collection data source for gateway recording, Create a dialer data source, Create a LAN data source, Create a radio data source, and Create a phone data source. Fixed a typo in the "Configure roles" topic.
1.50	<ul style="list-style-type: none"> Added documentation for AudioHook member group Added documentation for new recording profile settings: Record/Do Not Record Chat, Email, and Social Media
1.49	Added note about Capture Verification limitation around Avaya phone data sources with back-office contact policy type in <i>Create a phone data source</i> . Minor changes.
1.48	Added a topic titled "Recover calls for an Amazon Connect adapter" to the "Configure a CTI adapter" section.
1.47	<ul style="list-style-type: none"> Added requirement to install screen capture on desktops in "Set up screen recording." Added technical overview and diagram to <i>Recorder Maintenance Mode</i>.
1.46	In the <i>System maintenance</i> chapter, added information about SIP/SIPREC maintenance mode for the RAPS server role. The following topics were updated: <i>Recorder maintenance mode</i> , <i>Maintenance mode reference</i> , and <i>Put a server in or out of maintenance mode</i> .

Revision	Description of changes
1.45	In the "Create conditions for a recording rule" topic, added a subtopic titled "Usability issue with the In List and Not In List condition settings."
1.44	In the "Create a phone data source" topic and the "Create a dialer data source topic, added documentation for the "Maximum Allowed Extensions" setting.
1.43	Changed Checksumutil directory from %IMPACT360SOFTWARE%\ContactStore to %IMPACT360SOFTWARE%\ContactStore\Tools.
1.42	<p>Added "Create a recording profile" and "Edit a recording profile" to the "Configure recording" chapter.</p> <p>Added registry location to the "Allow Grow based on free space" field description in the "Use Log Manager" topic.</p>
1.41	Clarified how recording rules work across the midnight boundary in the "Time to schedule" field in the "Create a schedule for recording rules" topic.
1.40	In the "Associate a server role with a Recorder" topic, added clarifications to the note about associating data sources to Recorder Integration Service servers.
1.39	Added a note to the "About this guide" section regarding usage of the terms "multi-tenancy" or "multi-tenant" in this documentation.
1.38	Revised description of recorder maintenance mode.
1.37	<ul style="list-style-type: none"> • Deleted unneeded sentence in the "Security" topic in the "Scaling for SIP and SIPREC with RAPS" chapter. • Revised the "Selective recording flow" text and diagram in the "Message flows with RAPS" topic in the "Scaling for SIP and SIPREC with RAPS" chapter. • Clarified third-party SIP device forking for the primary and secondary RAPS nodes in the "Resilience and Redundancy" topic in the "Scaling for SIP and SIPREC with RAPS" chapter. • Added "Limitations" to the Real Time Monitor" topic. • Revised description of recorder maintenance mode.
1.36	<ul style="list-style-type: none"> • Added new chapter on scaling for SIP and SIPREC traffic with RAPS. • Removed duplicate topic named "Gateway side correlation pool member group settings." • Minor edits.
1.35	Added the topics "Create a recording profile" and Edit a recording profile."

Revision	Description of changes
1.34	<p>Updates for V15.2 2021R1:</p> <ul style="list-style-type: none"> • Added details for enabling Audio Quality Statistics. • Added new chapter on scaling for SIP and SIPREC traffic with RAPS. • Added new topic titled "DMCC recording group member group settings."
1.33	<p>In the "Create Custom Data fields topic, corrected steps, and updated related information reference.</p>
1.32	<ul style="list-style-type: none"> • In the "Create a phone data source" topic, added a note that overlay settings only apply to station/line side recordings. • In the "Use Log Manager" topic, clarified the "Allow Grow based on free space" option. • In the "Real-time Monitor" topic, added RTM limitation for TDM calls.
1.31	<ul style="list-style-type: none"> • Added details for the Default Employee section on the Data Source definition page for Phone, LAN, and Dialer data sources. • Added content to the "Create workstation groups," "Create subnets," and "Subnets and subnet masks" topics to provide context for the configurations. • Added details to the "Audio quality statistics" topic. • Added a note to the description of the threshold in "Configure disk manager" topic explaining the change in recommendation from V15.1 to V15.2.
1.30	<p>In the "Export and Import Data Source Settings" topic, removed a sentence indicating you could use a command line to run imports of extensions or replay restrictions using a CSV file.</p>
1.29	<p>Updated "Log Manager utility" and "Use Log Manager" to reflect UI and option changes made available in a 2020R1 update.</p>
1.28	<p>The following changes are new with 2020R1:</p> <ul style="list-style-type: none"> • Added a chapter for "Configure Secure Communication." • Changed custom data fields to 300 in the "Custom data" topic. • Added a topic for the Amazon Connect member group.
1.27	<ul style="list-style-type: none"> • Removed duplicated steps in "Create a phone data source." • Added requirements to "Set up for Ingestion Recording."
1.26	<p>Added 100-character limitation to recorder selection expression setting.</p>
1.25	<p>Updated the steps in "Create a Dialer Data Source" to match the work flow.</p>

Revision	Description of changes
1.24	<p>Revised description around unidentified values when concatenating multiple field values into a single attribute. If none of the dynamic references contain any data, then nothing is tagged.</p> <p>Revised recorder selection expression setting to specify that it applies only to Avaya DMCC SSC/SO or Shared Interception.</p>
1.23	Updated description of Session Auditing Policy.
1.22	In the "Multiple registration extension pool member group settings" topic, add "Never (application)" as a supported Recorder Fallback Type.
1.21	<ul style="list-style-type: none"> • In "Gateway side correlation pool member group settings" topic, added additional information about expressions and recording of internal calls using DMCC with SIPREC solutions. • Added the "Audio quality statistics events" topic. • In "Configure the Integration Service role" and the "Configure server-level settings for recording rules" topics, updated the descriptions for "Delete all future recordings in a contact" and "Delete all future recordings in currently active sessions."
1.20	<p>The following changes are new with V15.2 HFR7:</p> <ul style="list-style-type: none"> • In "Multiple registration extension pool member group settings" topic, added that multiple registration of devices is increased from 3 to 10 in Aura 8.0.1. • In "Create/update Multiple Registration Extension Pool group members" topic, deleted "Abandon CTI Calls" field and removed "RETAIN" from the sample line in CSV. • For screen recordings, modified the "Maximum Record Time (Seconds)" field in the "Configure Recorder settings" topic.
1.19	<p>The following changes are new with HFR6:</p> <ul style="list-style-type: none"> • Documented a new "Enable Stereo Recording" option for the Multiple Registration Extension Pool member group. • Noted that the maximum password length for the "Interactive Intelligence" adapter is 1024 characters. • Added "Setup for Ingestion Recording" topic. • Removed "Abandoned CTI Calls" setting and description from "Multiple registration extension pool member group settings" topic.
1.18	Modified "Minimum Session Length" description in the following topics: Create a collection data source for gateway recording, Create a dialer data source, Create a LAN data source, Create a radio data source, and Create a phone data source.

Revision	Description of changes
1.17	<ul style="list-style-type: none"> • Modified Session Auditing Policy description in the "Create a phone data source" and the "Create a dialer data source" topics. • Added a note to the "Screen recording" topic that Recorders cannot be shared across multiple Recorder Integration Service servers. • Added in "N+M" topic that load balancing within shared recorders in a DMCC delivery environment follows the N+M All Shared algorithm. • Added a topic named "Load balancing in N+M All Shared."
1.16	<p>Changed Product Central to the portal in Switches and third-party devices.</p> <p>Corrected Enterprise Manager Configuration and Administration Guide name.</p>
1.15	<p>Modified the N+N note in the general considerations section of the N+N topic.</p>
1.14	<p>Fujitsu integrations are no longer supported.</p>
1.13	<p>Added "Configure recorder generated comfort noise" topic.</p>
1.12	<p>The following changes are new with V15.2 HFR4:</p> <ul style="list-style-type: none"> • In Configure network cards and filters, for the Recording type field, added a note that the field does not need to be configured for Skype environments. • In Configure network cards and filters, for the RTP Proxy option in the Recording type field, added that the option is for V15.2 HFR3 and lower Lync environments.
1.11	<p>Clarified the Persist Agent State on Shut Down field description in the "Create a phone data source" topic.</p> <p>Added the SIP Call Tracking setting to the "Create a phone data source" topic.</p> <p>Changed session to interaction, where applicable.</p>

Revision	Description of changes
1.10	<p>The following changes are new with V15.2 HFR3:</p> <ul style="list-style-type: none"> • Throughout the guide, made the following changes: <ul style="list-style-type: none"> ▪ Changed "External Controlled" to "Full Delivery (External Controlled)" ▪ Changed "Duplicate Streamed" to "Selective Delivery (Duplicate Streamed)" • Added section titled "Recorder maintenance mode" to the System maintenance appendix. • Added note to the "Configuration and Administration" topic to remind users to check the Alarm Dashboard after changing a recorder. • Throughout the guide, made the following changes: <ul style="list-style-type: none"> ▪ changed "Enable N+N Double Consolidation" to "Keep Duplicate Recording" ▪ Changed "N+N Master Recording" to "N+N Primary Recording" ▪ changed "N+N Primary Recording" to "N+N Main Recording" ▪ Changed "Enable Return to Primary after Recover" to "Enable Return Primary Control to Main after Recovery" ▪ changed "Dual marking master recording" to "Dual marking primary recording" ▪ Changed "Dual marking primary recording" to "dual marking main recording" ▪ Changed master (recording) to primary ▪ Changed slave (recording) to secondary ▪ Changed primary (server) to main ▪ Changed secondary (server) to backup ▪ Changed mastership to primary control • Updated with new document template. • Added a topic named "Reset channel mechanisms for NTX cards." • Added note to "Create subnets" topic about creating subnets for workstations behind a NAT.
1.09	Added Full Duplicate Recording topic in the "Configure high availability" chapter.
1.08	<p>Removed Custom Data Planner reference. In N+N, adding IP video limitation. In "Standard attributes" and "Configure adapter custom attributes", changed "Source QM Database Server" fields description to Not applicable since QM 7.x is no longer supported.</p>

Revision	Description of changes
1.07	In Set up attributes, tagging, and recording rules > CTI tagging > Map attributes to an adapter > Limitations, changed plus sign syntax to {+}.
1.06	In Configuring Recording > Gateway side correlation pool member group settings, added notes to the Correlation Key setting.
1.05	Corrected cross-references in "Set up phones and extensions" topic.
1.04	In Configure CTI adapters > Configure a CTI adapter, clarified that a single data source needs to be assigned only one "primary" CTI adapter.
1.03	In Recorder Reference > Screen Recording, added Selective Screen Application Recording.
1.02	<p>In Recorder Redundancy > N+N, added a note about mastership on the Recorders when the IP Capture Service is restarted.</p> <p>In Set up attributes, tagging, and recording rules > CTI tagging > Identify CTI data, revised topic.</p>
1.01	In "Configure compression," added G.711 channel limitation.
1.00	<p>The following changes have been made for this release:</p> <ul style="list-style-type: none"> • "Recording configuration workflows" clearly identify what to do next, completion of major steps in the workflow, identification of major procedures in the workflow, and references to supporting guides you can use to supplement the workflow. • Support for recording video (omnichannel recording). The following areas were updated: <ul style="list-style-type: none"> ▪ IP-based voice and video recording ▪ Set up voice and video recording ▪ IP Recorder and IP Recorder Video configuration ▪ Video stitching ▪ Configure Recorder settings • The "High-availability" chapter has been updated with enhancements for the Full Duplicate Recording feature. • The Integration Service redundancy > 1+1 has been updated with N+M and N+N information.

Getting started with recorders

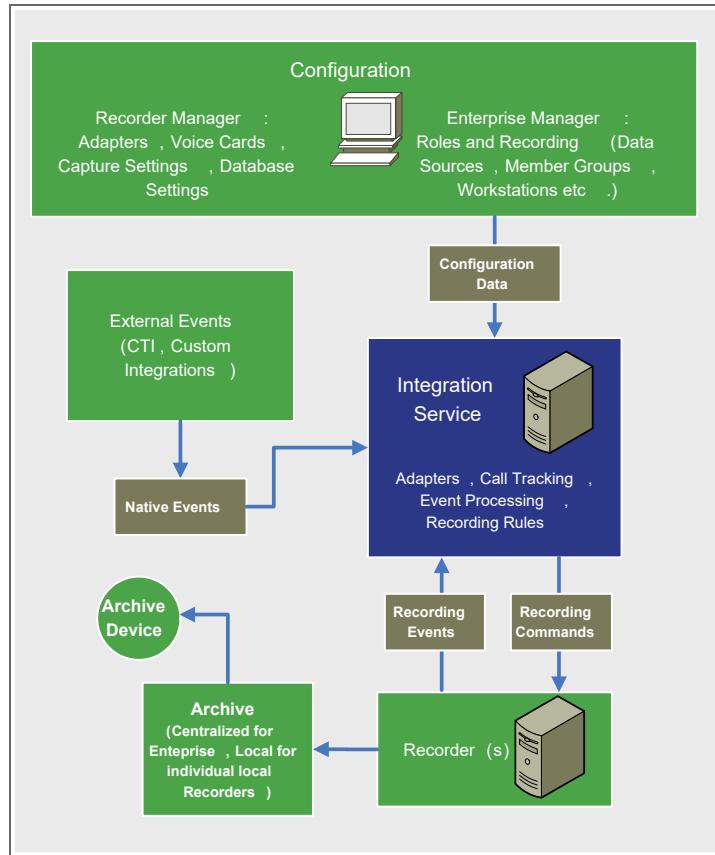
This section introduces the Recorder configuration user interface, and outlines the high-level steps required to implement different types of recording.

Topics

Overview for the Recorder	27
Configuration and administration	29
Recording configuration workflows	32

Overview for the Recorder

The Recorder can record both voice and screen data in your front- and back-office, in TDM, IP, and mixed telephony environments. The Integration Service handles output from the switch and other data sources, controls recording, and manages recording rules, as illustrated in the following diagram.



Ensuring that a call is recorded and stored reliably in accordance with the needs of the business depends on careful administration, on-going checks, and for mission critical deployments, redundant configurations.

It is important to read and follow the advice given in this manual and in others such as the *Archive Administration Guide*, and to understand the importance of robust recorder and archive deployment, configuration and management.

As with any system, external system changes, equipment failure, errors within the system, errors in the system configuration, and human error can result in the system either not keeping the calls you want or recording a call that you are not supposed to record. It is recommended to protect against critical system failure that redundant recording and CTI solutions are deployed, and in all cases that careful monitoring of alarms and systems is routinely undertaken. To protect against human error or unexpected behavior from any

configured recording or archive rules, checks should be made to ensure that the system is recording and archiving, and that only the required calls are recorded and archived. Failure to do so may result in data loss, data corruption, or recording of unintended calls.

Related topics

[Configuration and administration \(page 29\)](#)

[Recording configuration workflows \(page 32\)](#)

Configuration and administration

The two applications you can use to configure your Recorder: the **Enterprise Manager** and **Recorder Manager**. Each allows you to set up different aspects of your recording system.



After making changes to the recorders, remember to check the System Monitoring > Alarm Dashboard. Some changes may require additional, manual corrective actions to reconcile.

Related topics

[Enterprise Manager features \(page 29\)](#)

[Recorder Manager features \(page 30\)](#)

Enterprise Manager features

Use Enterprise Manager to configure system-wide features.

Features

- recorder installations across sites in the enterprise
- recorder roles, which define the functionality of servers
- data sources, which include phones (or PBX/ACDs) and local area network (LAN) workstations (for screen recording), and require the configuration of phones and extensions, member groups, workstations and workstation groups
- conditional custom data (CCD) and custom data (CD), used for tagging and recording rules
- Central Archive functionality (see the *Archive Administration Guide*)

The screenshot shows the 'SYSTEM MANAGEMENT' interface. At the top, there are navigation links: 'ENTERPRISE | LICENSING MANAGEMENT | GENERAL SETTINGS | CALL LOCK'. Below these are sub-links: 'Settings • Enterprise Settings • Security • Version • Configuration Status • Topology Report'. On the left, a sidebar titled 'View: All' and 'Find:' contains a tree view under 'Installations': 'Enterprise' (selected), 'Site Group', 'Site', and 'ATL'. On the right, the main panel displays details for 'Enterprise: Enterprise'. The table includes fields: 'Name' (Enterprise), 'EM Server Name' (atl), 'Port Number' (80), 'Description' (Installations across the enterprise), and 'Master Enterprise Manager Server' (ATL-1). At the bottom right are buttons: 'More Actions', 'Reports', 'Create Site', 'Create Site Group', 'Save', and 'Revert'.

Related topics

[Configuration and administration \(page 29\)](#)

[Recorder Manager features \(page 30\)](#)

Recorder Manager features

Use the Recorder Manager to control specific behavior for each Recorder.

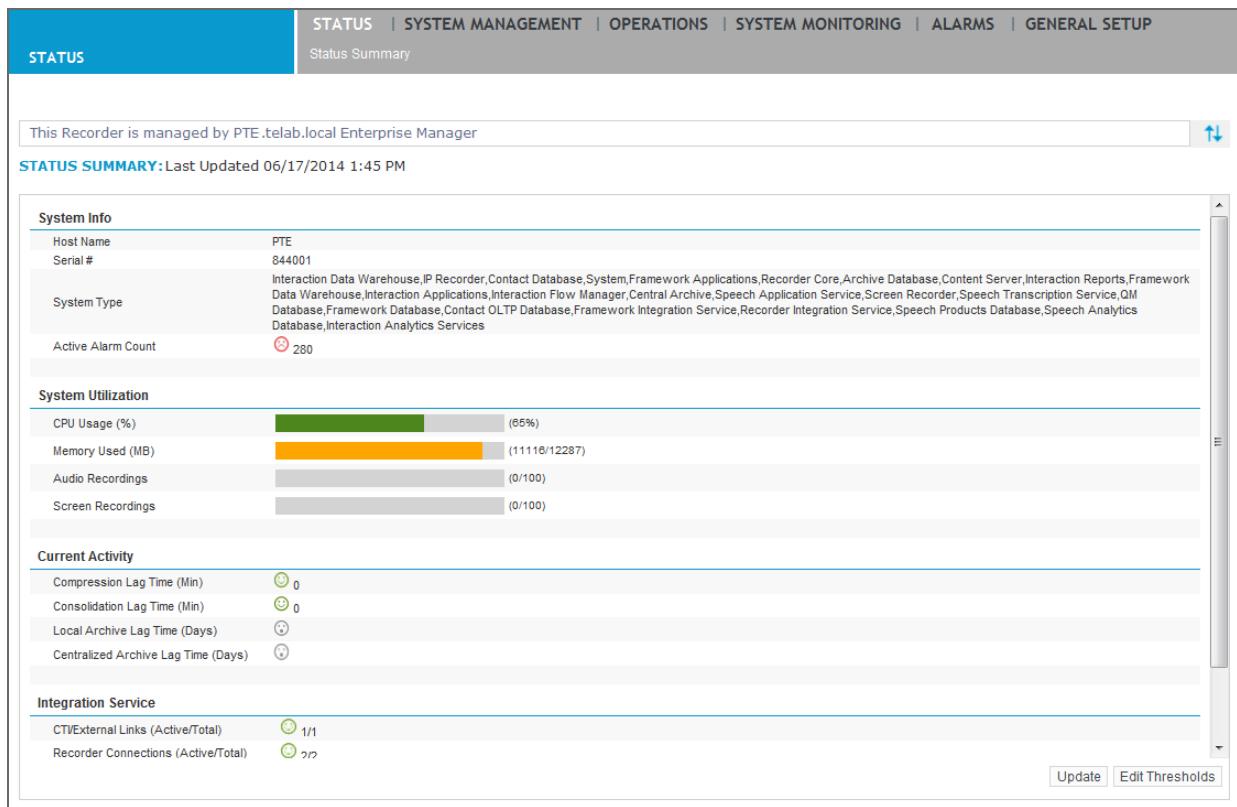
Access Recorder Manager

1. In Enterprise Manager, select a recorder.
2. Go to **System Management**. Under **Enterprise**, select **Settings**.
3. Select the **Launch** button.

Features

- check the status of the recorder
- configure voice cards or NICs
- back up your configuration
- configure and manage local drives on the recorder

- create a Calls folder on the local drive, in which to store recorded audio files before they are archived
- configure local Archive functionality (see the *Archive Administration Guide*)



Configuring adapters

Recorder Manager is also the place where you can configure the adapters for CTI integrations. Adapters connect to and receive events from third-party systems—identified in Enterprise Manager as a data source—translating the event data into key-value pairs that are then sent to the Integration Service. Adapters notify the Integration Service of any serious errors in the third-party system, or in the communication with that system.

Related topics

[Configuration and administration \(page 29\)](#)

[Enterprise Manager features \(page 29\)](#)

Recording configuration workflows

The steps you need to complete to configure your recorder and CTI integrations depend on the type of recording you require. You can set up each of the following scenarios by following the associated workflow through the procedures in this guide.

Workflows

- Workflow: IP-based voice and video recording (page 33)
- Voice recording (page 35)
 - Workflow: Station-side TDM recording (page 36)
 - Trunk-side TDM recording (page 36)
 - Workflow: Mixed TDM trunks and IP trunks recording with service observe (page 36)
- Workflow: Screen recording (page 38)
- Workflow: Integrate Dialer integration (page 39)
- Shared screens for recording configuration (page 40)
- Redundancy—refer to the *Integration Guide* for redundancy workflows

About the workflows

Each workflow outlines the specific procedures that you need to complete, including links to the procedures within this guide. Notes are provided at key configuration points where the settings described are critical to implementing the type of recording you require.



This section outlines common scenarios, including some that apply to multiple switch types. It does not include scenarios that are exclusive to specific switches. If the recording deployment you require does not appear here, consult the *Integration Guide* for your particular switch.

Trader recording

See the appropriate Trading *Integration Guide* for complete workflow and details on how to create a Trader data source.

Related topics

[Recording configuration workflows \(page 32\)](#)

Workflow: IP-based voice and video recording

The tasks required for IP-based voice and video recording include setting up the recorders and mapping the employees to the extensions.

Before you begin: Limitation on RTP detection

RTP detection is not supported when the RTP payload type is in the dynamic payload range of 96-127 (such as video) and for any encrypted media streams (such as Lync). Therefore, RTP detection is not supported for video recording and Lync recording.

Workflow

1. [Associate a Recorder with the Integration Service \(page 46\)](#)

If both components are on the same server, it is possible the association was completed during installation.

Create an association between the recorder and the Integration Service.

2. [Create a phone data source \(page 49\)](#)

Define where the calls to be recorded are coming from.

3. Referring to [IP extension pool member group settings \(page 71\)](#), create an IP Extension Pool Member Group.

Set the **Recorder Control Type** to **Recorder Controlled** or **CTI Controlled**.

4. [Create and edit phones/extensions \(page 125\)](#)

This step enables you to configure the actual extensions in use in your system and associate them with the data source. You also set the Recording Mode, which defines whether recording occurs for any given extension, and if so, how recording is triggered.

[Create employees and add employee IDs \(page 143\)](#)

5. .

Maps employees to extensions and data sources, and specifies the type of employee seating arrangement.

Optional, depending on your requirements.

6. Following the [Recorder configuration workflow \(page 182\)](#), set up individual recorders.

Set up the local recorder machine, in particular the voice card or NIC, database settings, call buffer, and compression.

7. Optional: [Set up attributes, tagging, and recording rules \(page 269\)](#)

Use the [Attributes configuration workflow \(page 270\)](#) for implementation of recording and tagging based on a business logic that reflects the goals of your enterprise.

8. [Install and configure Archive \(page 41\)](#)

Set up the central or local archiving mechanisms as required.

Related topics

[Recording configuration workflows \(page 32\)](#)

[Configure RTP detection \(page 381\)](#)

Related information

Setup procedures (*Archive Administration Guide*)

Voice recording

The following workflow outlines the tasks required for voice recording.

Workflow

[Associate a Recorder with the Integration Service \(page 46\)](#)

1. Create an association between the recorder and the Integration Service.
If both components are on the same server, the association may have already been completed during installation.
2. [Create a phone data source \(page 49\)](#)
Define where the calls to be recorded are coming from.
3. [Create a collection data source for gateway recording \(page 61\)](#)
A member group represents groups/pools of extensions, or channels. The type of member group you set up—along with the Recorder Control Type—will define the particular type of recording that needs to happen in your environment (for example, Recorder Controlled Trunk Side TDM).
4. [Set up phones and extensions \(page 124\)](#)
Configure the actual extensions in use in your system and associate them with the data source. You also set the Recording Mode, which defines whether recording should occur for any given extension, and if so, how recording is triggered.
5. [Create employees and add employee IDs \(page 143\)](#)
Map employees to extensions and data sources and specify the type of employee seating arrangement.
Optional depending on your requirements.
6. Following the [Recorder configuration workflow \(page 182\)](#), set up individual recorders.
Set up the local recorder machine, in particular the voice card or NIC, database settings, call buffer, and compression.
7. Optional: [Set up attributes, tagging, and recording rules \(page 269\)](#)
Use the "Attributes configuration workflow" for implementation of recording and tagging based on a business logic that reflects the goals of your enterprise.
8. [Install and configure Archive \(page 41\)](#)
Set up the central or local archiving mechanisms as required.

Related topics

[Attributes configuration workflow \(page 270\)](#)

Related information

Setup procedures (*Archive Administration Guide*)

Workflow: Station-side TDM recording

The workflow outlines the tasks required for station-side TDM voice recording.

Workflow

1. Set up [Voice recording \(page 35\)](#)
2. Create a Compliance Station Extension Member Group.
Set the **Recorder Control Type** to **Recorder Controlled** or **CTI Controlled**.

Related topics

[Workflow: IP-based voice and video recording \(page 33\)](#)

Trunk-side TDM recording

The following table outlines the tasks required for trunks-side TDM voice recording.

Configuration workflow:		Trunk-side TDM recording
Complete the procedures under Workflow: IP-based voice and video recording (page 33) , using the settings below when creating member groups.		
Create a Compliance Trunk Span Member Group.	1.	See Compliance trunk span member group settings for TDM (page 68) . Set the Recorder Control Type to Recorder Controlled or CTI Controlled .

Related topics

[Workflow: IP-based voice and video recording \(page 33\)](#)

Workflow: Mixed TDM trunks and IP trunks recording with service observe

The following tasks are required to set up mixed TDM trunks and IP trunks recording with Service Observe (SO).



Service Observe does not apply to Trading calls.

Workflow

1. Follow [Workflow: IP-based voice and video recording \(page 33\)](#)
2. Set up a trunk span recording resource member group and associate it with one recorder.
A Trunk Span Recording Resource represents T1 or E1 lines on TDM switches with recording capabilities such as Service Observe (SO). Set the **Recorder Control Type** to **Recorder Controlled** or **CTI Controlled**.
3. Set up an extension recording resource member group and associate it with the other recorder.

An Extension Recording Resource represents extensions used on IP switches with selective recording capabilities like SO. Recording Resource extensions can be assigned to only one member group. Set the Recorder Control Type **Service Observe**.

Related topics

[Extension recording resource member group settings \(page 75\)](#)

[Trunk span recording resource member group settings \(page 75\)](#)

Workflow: Screen recording

The following workflow outlines the tasks required to configure the system to record employee screen activity.



To use screen recording you must associate phones and extensions with workstations, or LAN employee IDs with phone employee IDs in the Employee Mapping section under **Recording Management > Data Sources > Employees**.

Workflow

1. Associate a Recorder with the Integration Service (page 46)

Assign the Screen Recorder role to a Recorder and associate it with the Integration Service. Note that in Screen-only recording, in order to archive calls you must also enable an IP Recorder or TDM Recorder role, in addition to a Screen Recorder role.



Recorders cannot be shared across multiple Recorder Integration Service servers.

2. Create a LAN data source (page 107)

Create a LAN data source and assign it to the Integration Service(s) that will be triggering Screen Recording of the workstations created on this LAN data source.

[Define workstations \(page 112\)](#)

3. and Create workstation groups (page 110)

Identify the computers or groups of computers on which you want to perform screen recording. You can also configure subnets to represent the range of computers that match the subnet criteria.

For static workspaces, workstations can be assigned to an extension and vice versa. For dynamic workspaces, assign the Windows Logon ID of a workstation to an employee, and build the relationship with Extensions.

[Create employees and add employee IDs \(page 143\)](#)

4.

Map Employees to extensions/workstations. Assign the phone extension or phone logon ID and workstation, or workstation logon ID to employee, depending on the respective data source seating arrangement type.

5. Following the Recorder configuration workflow (page 182), set up individual recorders.

Set up the local recorder machine, in particular the voice card or NIC, database settings, call buffer, and compression.

6. Optional: Set up attributes, tagging, and recording rules (page 269)

Use the [Attributes configuration workflow \(page 270\)](#) for implementation of recording and tagging based on a business logic that reflects the goals of your enterprise.

7. Install and configure Archive (page 41)

Set up the central or local archiving mechanisms as required.

Related topics

[Recording configuration workflows \(page 32\)](#)

[Map employees to data sources \(page 145\)](#)

Related information

Setup procedures (*Archive Administration Guide*)

Workflow: Integrate Dialer integration

The following workflow outlines how to configure integration with a dialer.

Workflow

1. [Create a phone data source \(page 49\)](#)

When employees log in to a dialer, typically a call is placed from the dialer to the employee through the PBX and a connection is established and maintained for their entire dialer login session. This call is typically called a "nailup call." In trunk-side recording deployments, you must tap the trunks that are between the dialer and the PBXs that are used to establish these nailup calls to record the voice for dialer calls. You configure this by creating a Phone data source with a Trunk Side Member Group for the dialer trunks.

2. [Create a member group \(page 66\)](#)

The member group represents groups/pools of extensions, or channels. For dialer integration, use the Compliance trunk span member group settings for TDM.

3. [Create a dialer data source \(page 116\)](#)

Define where the dialer data is coming from. Be sure to link the dialer data source with the Phone data source created in step 1.

4. [Create employees and add employee IDs \(page 143\)](#)

Map employees to extensions and data sources, and specify the type of employee seating arrangement. May be optional depending on your requirements.

5. [Add employee mappings \(page 146\)](#)

Associate employees with data sources, and specify a fixed, free, or hybrid seating arrangement. May be optional depending on your requirements.

6. [Set up individual Recorders \(page 181\)](#)

Following the appropriate workflow for your recorder type, set up the local recorder machine, in particular the voice card or NIC, database settings, call buffer, and compression.

7. [Install and configure Archive \(page 41\)](#)

Set up a central archive or local archive server.

Related topics

[Recording configuration workflows \(page 32\)](#)

[Compliance trunk span member group settings for TDM \(page 68\)](#)

Related information

(*Archive Administration Guide*)

Shared screens for recording configuration

Shared Screens functionality is supported in all environments as long as the system is configured with two Integration Service servers. See [Shared screen Recorders \(page 460\)](#) for more information.

Related topics

[Recording configuration workflows \(page 32\)](#)

Install and configure Archive

Workflow sequence

- Workflow: IP-based voice and video recording ([page 33](#)): Task 8 of 8
- Workflow: Screen recording ([page 38](#)): Task 7 of 7
- Workflow: Integrate Dialer integration ([page 39](#)): Task 7 of 7

Before you begin

Detailed guidance for setting up and configuring Archive is found in the related information section.

Procedure

1. For enterprise-level Archive, enable the **Central Archive** role, either on the Recorder server or on a separate server.
For local Archive, the Local Archive role is enabled by default during installation.
2. Set up the Archive server to Recorder associations.
3. Configure Archive.

Related topics

[Recording configuration workflows \(page 32\)](#)

Related information

Archive Administration Guide

Configure recording

The following sections describe how to configure the Recorder.

Topics

Deployment overview	43
Configure the recording environment	44
Set up voice and video recording	49
Set up screen recording	106
Set up a dialer integration	116
Set up phones and extensions	124
Create employees and add employee IDs	143
Create a recording profile	149
Create data source groups	154
Set up data sources, member groups, and devices for radio recording	158
Set up for Ingestion Recording	180

Deployment overview

By this point you have already planned your setup and installed the recorder. However, it may be useful to revisit some key concepts before proceeding.

Key concepts

- Deployment of components occurs in one of two types of zones: data center and satellite. Typically the data center is at a customer's headquarters, while a satellite zone is located at a branch or remote site, but these two types of zones may also be physically co-located.
- The Recorder (including the Integration Service) is considered a satellite component, while its database is part of the data center. Since the Integration Service often supports Recorders across satellite site boundaries, it may need to be co-located with the data center, depending on the locations of the call center's voice switches, CTI servers, and network storage.
- Servers are governed by Server Roles that define functionality (for example, "Integration Service").

Using the Enterprise Manager and Recorder Manager

You will configure recording using Enterprise Manager to set up data sources and seating arrangements, and the Recorder Manager to set up hardware and other aspects of individual recorders.

Finding additional information about concepts

The following chapters focus primarily on the tasks you need to complete. For information about any of the concepts used, please refer to the related topics section below.



To determine which tasks from the following sections are relevant to the type of recording you want to perform in your particular environment (for example, CTI/Recorder-Controlled Trunk Side TDM), and the order in which to complete those tasks, see the workflow topic.



All "Configure recording" procedures take place in Enterprise Manager, unless otherwise stated.

Related topics

[Reference \(page 412\)](#)

[Recording configuration workflows \(page 32\)](#)

Configure the recording environment

Before you begin the recorder configuration, configure switches and third-party devices and set up recorder roles and associations.

Related topics

[Switches and third-party devices \(page 44\)](#)

[Set up Recorder roles and associations \(page 44\)](#)

Switches and third-party devices

Switches and other third-party devices in use within your system will require configuration in order to set up an integration. This information is covered in a series of Guides, available on the Recorder software, the Portal, and the Partner Extranet.

Related topics

[Configure the recording environment \(page 44\)](#)

Set up Recorder roles and associations

To configure your Recorder, first create an Enterprise Site and add recorders to that site. Next, if you did not do so during installation, assign the appropriate roles to your Recorder and Integration Service. See the *Enterprise Manager Configuration and Administration Guide* for comprehensive coverage of sites and roles, including configuration of the roles themselves.



After making any changes to a server role, you must restart the system.

Role configuration notes

- The Streaming Service server role supports audio streaming for real-time and recorded playback. Enable this server role on all servers that have the Content Server server role enabled.
- To improve scalability in deployments with SIP/SIPREC, consider making use of the RAPS role to offload traffic from RIS nodes.

Related topics

[Associate a server role with a Recorder \(page 45\)](#)

[Associate a Recorder with the Integration Service \(page 46\)](#)

[Configure the Integration Service role \(page 48\)](#)

[Recording configuration workflows \(page 32\)](#)

[Scaling for SIP and SIPREC traffic with RAPS \(page 367\)](#)

Related information

Server Role Configuration and Administration (*Enterprise Manager Configuration and Administration Guide*)

Associate a server role with a Recorder

Procedure

1. In Enterprise Manager, click **System Management > Settings**.
2. Select a Recorder from the left-hand pane.
3. Click **Server Roles**.

Active	Role Name	Version
<input type="checkbox"/>	Analytics Framework	11200
<input checked="" type="checkbox"/>	Archive Database	11101
<input type="checkbox"/>	Biometrics Database	11200
<input type="checkbox"/>	Biometrics Engine	11208
<input checked="" type="checkbox"/>	Central Archive	11200
<input checked="" type="checkbox"/>	Contact Database	11200
<input checked="" type="checkbox"/>	Contact OLTP Database	11200
<input checked="" type="checkbox"/>	Content Server	11200
<input type="checkbox"/>	Framework Applications	11100
<input type="checkbox"/>	Framework Data Warehouse	11243
<input type="checkbox"/>	Framework Database	11200
<input type="checkbox"/>	Framework Integration Services	11205
<input type="checkbox"/>	Interaction Analytics Service	11100
<input type="checkbox"/>	Interaction Applications	11202
<input type="checkbox"/>	Interaction Data Warehouse	11101
<input type="checkbox"/>	Interaction Flow Manager	
<input type="checkbox"/>	Interaction Reports	

4. Select the check box beside the name of the appropriate recording-related role (IP Recorder, TDM Recorder, or Screen Recorder). To allow a Recorder to be controlled by a CTI adapter, associate it with an *Integration Service* role.



A data source may only be associated with at most one Recorder Integration Service server (or one redundant pair of Recorder Integration Service servers). All of the Recorders associated to that data source must also be associated to the Recorder Integration Service for that data source. TDM and screen recorder roles may only be associated with at most one Recorder Integration Service server (or one redundant pair of Recorder Integration Service servers). IP recorder roles may be associated with at most two Recorder Integration Service servers (or two redundant pairs of Recorder Integration Service servers), but only one association is recommended.



Note that in Screen-only recording, in order to archive calls you must also enable an IP Recorder or TDM Recorder role, in addition to a Screen Recorder role.

5. Click **Save**.

6. Restart the Recorder:

- a. Select the Recorder, then click **Settings**.
- b. Click **Launch** to start Recorder Manager.
- c. In Recorder Manager, click **Operations > Start and Stop**.
- d. Click **Reboot**.



You can view and edit all nodes associated with a role by selecting a role node (from under any recorder) on the left-hand side, then clicking Associations. (Only nodes to which that role can be applied are available for selection.)

Related topics

[Associate a Recorder with the Integration Service \(page 46\)](#)

[Configure the Integration Service role \(page 48\)](#)

[Set up Recorder roles and associations \(page 44\)](#)

Associate a Recorder with the Integration Service

A Recorder is automatically associated with an Integration Service during installation if they are both on the same server. You can associate Recorders with an Integration Service at any time thereafter using the procedure below.



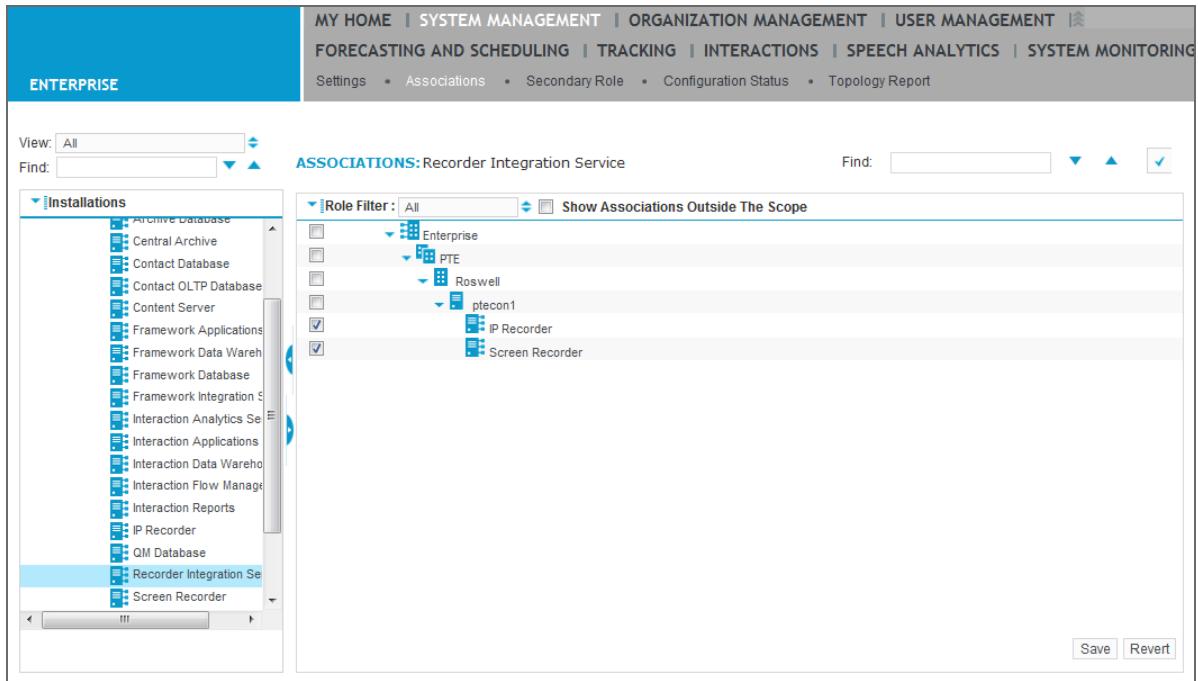
A data source may only be associated to a single Recorder Integration Service server (or pair in the case of redundant Recorder Integration Service servers). All of the Recorders associated to that data source must also be associated to the Recorder Integration Service for that data source.

Workflow sequence

- [Workflow: IP-based voice and video recording \(page 33\)](#): Task 1 of 8
- [Workflow: Screen recording \(page 38\)](#): Task 1 of 7

Procedure

1. Click **System Management > Settings**.
2. Locate a Recorder server with the Recorder Integration Service role by clicking the arrow button beside the name of the Recorder.
3. Click the Recorder Integration Service role, then **Associations**.



4. In the right-hand pane, select the Recorder server(s) you want to associate with the Integration Service.
5. Click **Save**.

What to do next

- Voice recording: [Create a phone data source \(page 49\)](#)
- Screen recording: [Create a LAN data source \(page 107\)](#)

Related topics

[Associate a server role with a Recorder \(page 45\)](#)

[Configure the Integration Service role \(page 48\)](#)

[Set up Recorder roles and associations \(page 44\)](#)

Configure the Integration Service role

Procedure

1. In Enterprise Manager, navigate to **System Management > Settings**.
2. Locate one of the Integration Servers under **Installations** and click the triangle beside it to show the list of associated roles.
3. Select the **Recorder Integration Service** role.
4. Configure the **Delete/Block Behavior**. This setting controls how the Recorder Integration Service deletes recordings when they are blocked by any of the Delete-on-Demand feature (on a phone), a recording rule, AIM, or a block command from a Recorder Integration Service API integration.
Select one of the following:
 - **Delete entire contact completely:** All recordings (past, present, and future) in a contact are deleted.
 - **Delete active sessions completely:** All recordings (past, present, and future) for all active interactions at the time of the block are deleted. Past interactions in the contact are not affected. Future interactions in the contact are not affected.
 - **Delete all future recordings in a contact:** All current and future interactions in a contact are affected. Any active recording is segmented at the time that the block is processed. Any recording prior to the block for the current interaction is not affected and is kept or discarded according to its current state. Any recording after the block and future interactions in the contact are deleted. Past interactions in the contact are not affected.
 - **Delete all future recordings in currently active sessions:** All future recordings for all active interactions at the time of the block are deleted. Any active recording is segmented at the time that the block is processed. Any recording prior to the block for the current interaction is not affected and is kept or discarded according to its current state. Any recording after the block are deleted for the affected interactions. Past interactions in the contact are not affected. Future interactions in the contact are not affected.
5. Specify the portion of a contact or session/interaction to which rules should apply using the **Process Business Rule on** setting. Options are to run the rules against each,
 - **Contact, then apply action to every session**— Evaluates rules on the contact level (and will only fire once per contact) and the action will affect all sessions/interactions in that contact.
 - **Session, then apply action to that session only**— Evaluates rules on the session/interaction level and the action will only affect that session/interaction.
6. Select **Enable Return Primary Control to Main After Recovery** to enable the system, in fallback scenarios, to attempt to return primary control to the main Integration Service after a period of stability has been achieved and both systems are fully functional.
7. Click **Save**.

Related topics

[Associate a server role with a Recorder \(page 45\)](#)

[Associate a Recorder with the Integration Service \(page 46\)](#)

[Set up Recorder roles and associations \(page 44\)](#)

Set up voice and video recording

To set up voice and video recording, several basic tasks must be completed.

Tasks

- [Create a phone data source \(page 49\)](#)
- [Create a collection data source for gateway recording \(page 61\)](#)
- [Set up phones and extensions \(page 124\)](#)
- [Create employees and add employee IDs \(page 143\)](#)



Video recording is supported only for IP recording environments.

The particular workflow you need to follow depends on your environment—see [Recording configuration workflows \(page 32\)](#) for a complete list.

Related topics

[Workflow: IP-based voice and video recording \(page 33\)](#)

Create a phone data source

Phone data sources are for capturing *voice calls* from a computer telephony integration (CTI) middleware server. A phone data source encapsulates information related to the target to be recorded, specifically the switch type, and the seating arrangement of agents using the phones within the call center.

Before you begin

Phone integration: [Associate a Recorder with the Integration Service \(page 46\)](#)

Dialer integration: [Create a member group \(page 66\)](#)

Procedure

1. In the Enterprise Manager, click **Recording Management**.
2. Under **Data Sources**, click **Settings**.
3. Click **Create Data Source**.
4. In the **Data Source Type** dialog box, select **Phone** as the **Type**, and select your switch from the **Switch/Sub Type** list.



The data source types available to you depend on licensing. Similarly, some of the following options are only applicable if you are using a specific switch, and therefore they do not appear in all cases.

5. Click **Select**.
6. Type a **Name** for the phone data source, and a Description (optional).

7. Select a **Time Zone** from the drop-down list (the recorder relies on the time zone for recording start and end times). You can specify whether tagging is based on this time zone or that of the organization below.



The time zone must always be correct on each server.

8. Specify a **Data Source Parent** in either of these scenarios:
 - You are creating a collection data source for gateway recording. Refer to [Create a collection data source for gateway recording \(page 61\)](#).
 - You are configuring a Genesys Business Continuity environment.
In this environment, you can specify a data source to act as a parent to multiple child data sources. In this scenario, you use a parent data source to configure extensions that the child data sources share. Each child data source represents a different switch (or site) where the sites are paired together to support failover. The child data source and parent data source must be of the same Phone data source subtype.
9. Under **Recorder Settings**, do the following:
 - a. Specify a **Seating Arrangement**—*Fixed*, *Free*, or *Hybrid*.
 - **Fixed** seating indicates that an employee has a permanently assigned workstation and is associated with a specific extension.
 - **Free** seating, the default, indicates that employees do not have permanently assigned workstations. They are assigned an Employee ID and can log in from any location in the call center. Extensions are assigned dynamically when the employee logs in.
 - **Hybrid** seating refers to a mixed arrangement that contains both Free and Fixed seating for employees.
 - b. In a multi-tenant enabled (cloud) environment, if the Seating Arrangement is Fixed or Hybrid, the Service Provider Administrator (SPA) can specify a **Maximum Allowed Extensions** value for this data source. The Maximum Allowed Extensions setting limits the number of extensions a Tenant Administrator can create for the data source. This setting allows a SPA to prevent tenants from creating more extensions than their assigned capture capacity supports.

If this setting is not set and the data source currently has no extensions associated with it, this setting defaults to 1000 at the time a Tenant Administrator creates the first extension.

In an upgrade scenario, a data source may already have extensions assigned to it. In this scenario, when a Tenant Administrator adds extensions, the system updates this setting to 120% of the existing number of extensions or 1000, whichever is higher. For example, if 2000 extensions are associated with the data source at the time of the upgrade, this setting defaults to 2400 when a Tenant Administrator adds extensions.

This setting does not limit the number of extensions a SPA can create. For example, if the setting is 1000, a SPA can create more than 1000 extensions. If the SPA creates more extensions than this setting specifies, the Tenant Administrator cannot create any extensions.

If a Tenant Administrator configures the maximum number of allowed extensions, the SPA can increase this number to allow the Tenant Administrator to create additional extensions. Before increasing this setting, the SPA should verify that the tenant's environment has the resources necessary to handle the increased load.

- c. To save the last employee settings after the computer is shut down, select the **Persist Agent State on Shut Down (minutes)** check box.

Specify the amount of time in minutes for which you want to save the employee data login state information. The default threshold is 600 minutes (10 hours). If the service restarts, state information within the threshold is reloaded from startup. State information beyond the threshold is not loaded. Reloading this state information can be useful if the CTI link does not provide a snapshot capability so the recorder can learn about all the logged in states on startup. It is expected that the CTI feed supplements any state information loaded on startup. Data from within this period is not loaded, while data from after this duration has passed is loaded.

If the CTI adapter is down, the following occurs:

- If unselected, all agents on the data source are logged out right away.
- If selected, all agents on the data source are logged out once the persistence period has elapsed.

- d. To prevent the retention of very short calls, specify a **Minimum Session Length (seconds)**. Active calls (from connected to closed) that are shorter than the specified value will be deleted automatically. If set to zero (0), this feature is disabled and no calls will be deleted based on this setting. The maximum value is 3600 (or one hour). This setting applies to the active duration of CTI Sessions or the entire duration of VOX Sessions. Inactive CTI Sessions can be retained using the Session Auditing Policy.

- e. If you are working with a system that uses Performance Mode (set in the IP Extension Pool member group) or N+N redundancy, enable the **Rollback Period (minutes)**.

The Rollback Period ensures that an amount of extra overlapping audio is kept for a time, so that in the event of a disconnection it is possible to retrieve it. The default value is 15 minutes, and the maximum value is 60 minutes.



A rollback period is applicable only to Performance Mode (set in the IP Extension Pool member group) and N+N redundancy.

- f. If you are working with a system that uses Performance and Liability fallback modes, enable RTP detection to prevent audio loss. Coordination between the Integration Service and RTP, using the following settings, ensures that there is only one recording for a given call:

- **Start Overlay (milliseconds)**—This threshold indicates the longest amount of audio (from before CTI starts) that is associated to that CTI call. Anything over this threshold is treated as VOX. The default is 5000 milliseconds (5 seconds).
- **End Overlay (milliseconds)**—This threshold indicates the longest amount of audio (after CTI ends) that is associated to that CTI call. Anything over this threshold is treated as VOX. The default is 6000 milliseconds (6 seconds).



The overlays only apply to station/line side recordings and not to trunk/correlation recordings.

- g. **Long Call Duration (minutes)**—This setting allows you to specify the length of a call, in minutes, after which the system triggers an alarm. The system also stops tracking the call from

a CTI perspective, so in CTI-controlled application or performance mode environments, this may cause loss of recording. Enter any number between 1 and 1440 (24 hours)—an alarm is raised in the cases where calls exceed this number of minutes. The default is 120.



The Integration Service runs maintenance checks every five minutes to close calls that last for more than the length of time specified as the **Long Call Duration**. An alarm indicated that a call was closed because it was too long. These maintenance checks are not run more frequently to avoid imposing an extra load on the system. Therefore it can take up to five minutes to close a long call after it has passed the defined **Long Call Duration** threshold.

- h. **Long Hold Duration (minutes)**— This setting allows you to specify the maximum duration of a single hold in minutes. Any holds over this duration raise an alarm. Enter any number between 1 and 3000, representing the number of minutes. The default is 30.
- i. **Recording Resource Allocation Behavior**—This setting is for duplicate streaming solutions, which allow you to distribute recordings across multiple recorders.



To use the CTI-based recorder selection feature available for Shared Interception and Avaya DMCC environments, you must select either **LineFirst** or **LineExclusive**. For Shared Interception, see [IP extension pool member group settings \(page 71\)](#). For Avaya DMCC environments, see [Extension recording resource member group settings \(page 75\)](#).

- **IgnoreLine**—Records the next recording on the least-utilized recorder connected to the Integration Service, regardless of data source, member group, and extension list settings.
- **LineFirst**—First attempts to record on the least-utilized recorder that contains the extension being recorded in a member group associated with the recorder. If the Integration Service cannot find an associated recorder, it attempts to find any connected recorder with the capacity (whether the extension is associated with the recorder). LineFirst provides a way to keep recorders local to the extensions/site. The Integration Service fails over to another set of recorders if a call cannot be recorded locally. If you do not want to fail over to another set of recorders, use 'LineExclusive', described below. This is the default.
- **LineExclusive**—First attempts to allocate the recording to the least-utilized recorder that contains the extension being recorded in a member group associated to the recorder. If the Integration Service fails to find a recorder associated with the line to be recorded, it does not record the call. By recording calls on a recorder co-located with the PBX for agents taking calls on a remote site, the use of this setting has the advantage of reduced WAN traffic.

The “least-utilized” recorder is the one with the most unused capacity. For example, if one recorder has 300 licenses and 50 calls are currently being recorded, and another recorder has with 100 licenses and 10 calls currently being recorded, the capacity left on the recorders are 250 and 90 respectively. The system attempts to record the next duplicate streamed call on the first recorder.

- j. **Always Report Extension as Primary Extension**—If enabled, the extension field of the session/interaction is always the primary extension on a telephone. If disabled, the extension field contains the DN/extension that first answered the call. This option only affects multiline phones. Enabled by default.

- k. **Contact Policy Type**—This setting allows you to set the call stitching method.
- **Follow the call**—When follow the call is enabled, there is one contact that includes all audio from the beginning of the call to the end. This option is the default.
 - **Backoffice - Contact per call**—Enables the “Back office” style of stitching, which creates sessions/interactions based on CTI calls. If one employee is on two calls at the same time (for example, a customer call and a consultation call), the system creates two sessions/interactions. This option is used more often in trading environments rather than contact center environments.
- l. **Raise Alarm for Out Of Service Devices**—If enabled, the Integration Service raises alarms for any devices that go out of service. This option is only available for Cisco JTAPI and Genesys adapters.
- m. **Alarm - Device Not Recorded Call Count**—The number of calls for a configured device that must fail to record before triggering the DeviceNotRecording alarm. The default is 1.
- n. **Alarm - Device Not Recorded (milliseconds)**—Failed call durations under this threshold do not count against the Device Not Recorded Call Count. The default is 15 seconds.
- o. **Service Observe Fail Count Threshold**—The number of consecutive recording failures that must occur before the Integration Service attempts to reset the Service Observe connection. The default is 3.
- p. **Session Auditing Policy**—Defines the type of session/interaction that is marked and kept in the system. “Disabled” (the default) only marks sessions/interactions with some kind of content. Two options create a basic entry in the database for calls that occurred but were not recorded: “Missed Recordings” marks calls that should have been recorded, but were not, while “Full Switch” marks all sessions/interactions for which we receive CTI without recording (for example, calls that were blocked, or interception calls that were met with a busy tone or unanswered ringtone). You may then search for these types of interactions in the Portal. The Recorder Integration Service selects a viable recorder associated with any device within the Session workspace to audit the interaction. If no viable recorder could be located at the time of the audit, the audit is lost. Recorded employee segments marked by means of auditing appear in playback once all sessions/interactions in the related Contact are closed, after a delay of up to five minutes.



Recorded employee segments marked by means of auditing will appear in playback once all interactions in the related Contact are closed, after a delay of up to five minutes.

q. **Keep Duplicate Recording**—

For an N+N recording environment, select one of the following options:

- Select the **Keep Duplicate Recording** option when a customer's compliance recording policies require them to archive duplicate recordings of every call. To support this configuration, you must double the size of the Contact Database, the Archive Database, and the archive storage media.
- Clear the **Keep Duplicate Recording** option (default) so that the system deletes the secondary interaction after determining which copy to keep.



When N+N recording is configured, the system evaluates the interactions captured by both Recorders. It marks one as primary and the other as secondary based on several criteria, including call quality. For details, refer to *Selective Recording Configuration*.

Archive campaigns provide alternative methods for managing recordings in N+N environments. Set the N + N Dual Marking options to turn off the double-archiving of recordings, which keeps a single copy. For details, refer to *Campaign conditions*.

- r. **Recorder Allocation Based On Audio Location**—Use this setting in a SIP-based VoIP delivery environment to control how Recorders are selected to record calls, and ensure that each call is recorded by a Recorder local to the media gateway at which the call arrives. This setting is designed primarily for environments where recording occurs at multiple sites and each site has its own gateway.

This setting must be used with either a Gateway Side Correlation Pool member group or an IP Extension Pool member group configured for the data source. Within these member groups, you must specify the IP addresses or host names of the phones associated with the member group in the IP Network Region configuration.

The Recorder Allocation Based on Audio Location setting instructs the system to examine the IP address in a SIP message and compare this address to the addresses listed in the IP Network Region settings of the Gateway Side Correlation Pool or IP Extension Pool member group associated with the data source.

If an address in the SIP message matches one of those specified in the member group IP Network Region settings, the system routes the call to a Recorder associated with that member group.

The options for this setting are:

- **Inactive**—The system attempts to record the call, but does not use an address found in a SIP message to route the call to a particular Recorder. This option is the default setting.
- **From Signaling**—The system examines the SIP header section of the SIP Invite. The system compares the address found in a SIP header field (such as From, Contact, Via, or Socket) to the addresses configured in the member group IP Network Region settings. If there is a match, the system routes the call to a Recorder associated with that member group. If the system does not find a match, the **Recording Resource Allocation Behavior** setting determines how the call is recorded.
- **From Media**—The system examines the SDP message attached to a SIP Invite. The system compares the IP addresses found in the SDP message to those addresses configured in the member group IP Network Region settings. If there is a match, it routes the call to a Recorder associated with that member group. If the system does not find a match, the **Recording Resource Allocation Behavior** setting determines how the call is recorded. This option does not work if SIP operates in Delayed-Offer mode.

This setting works with the **Recording Resource Allocation Behavior** setting to determine recording behavior. If the **Recording Resource Allocation Behavior** setting specifies:

- **IgnoreLine**—The system acts as if the Inactive setting is selected for this setting. If either the From Signaling or From Media is selected, those settings are ignored. In this case, any Recorder associated with the data source can record the call.
 - **LineFirst**—The system makes two attempts to record the call using the address obtained from the SIP message. If the system cannot successfully route the call to a Recorder using the SIP message address, any Recorder associated with the data source can record the call.
 - **LineExclusive**—If the system cannot successfully route the call to a Recorder using the address from the SIP message, the call is not recorded. In this case, the system raises an alarm.
- s. **Video Recording Mode** — Select one of the following options:
- **Start On Trigger** - Do not record video calls for the extensions associated with this data source until a recording rule is triggered or an external API command starts recording. Video recording starts whenever the call starts, but video before the recording trigger is deleted.
 - **Application Controlled** - Record every video call for every extension associated with this data source, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the video call. If the call is kept, the recording includes all video from the start to the end of the call.
 - **Do Not Record** - Do not record video calls for extensions associated with this data source. Recording rules are ignored and cannot trigger the recording of video calls.
 - **Record** - Record all video calls for all extensions associated with this data source. Only a block recording rule, AIM command, or external API command can prevent calls from being recorded.
- t. **Require Replay Audio Redaction** - When redaction is enabled for the system, select whether redaction occurs for interactions that the data source captures. Redaction obscures sensitive customer information in captured audio and transcriptions. Select from the following for interactions that the data source captures:
- **Disabled**: No information in the interaction is obscured. *Disabled* is the default setting.
 - **Always**: Sensitive customer information is obscured.
 - **In Fallback**: Sensitive customer information is obscured, but only in the event of CTI or recorder disconnection from the Integration Service.
- u. **Require Replay Audio Morphing** - When morphing is enabled for the system, select whether replay of interactions captured by the data source requires morphing. Morphing changes the voice heard during replay such that the speaker remains anonymous and the audio remains intelligible. Select from the following options for interactions that the data source captures:
- **Disabled**: The original voice of the agent and the customer are heard during interaction replay. *Disabled* is the default setting.
 - **Always**: The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting.
 - **In Fallback**: The voice of the selected channel or channels is morphed during interaction

replay, as configured by the **Audio Morphing Channel** setting, but only in the event of CTI or recorder disconnection from the Integration Service.

- v. **Audio Morphing Channel** - Enabled when **Require Replay Audio Morphing** is set to **Always** or **In Fallback**, choose the audio channel or channels that use morphing. Select from:
 - **Agent**: Only the voice of the agent channel is morphed during interaction replay. The voice on the customer channel is the original captured voice. *Agent* is the default setting.
 - **Agent and Customer**: The voice of the agent channel and the customer channel are morphed during interaction replay.
10. In the **Default Employee** section, specify the employee to be associated to a recording that has no employee associated to it.

There are situations where recordings do not have employees associated to them. Examples include:

 - IVR recordings where there is no employee or phone device
 - Back office environments where phones are shared and not associated to a specific employee

Assigning a **Default Employee for Interactions** to a data source provides a way to provide replay access to recordings that do not include a specific employee. When a **Default Employee for Interactions** is assigned to a data source, any recording that is not assigned to a specific employee will be associated to the **Default Employee for Interactions**.

To capture recordings for a default employee, select the **Organization** to which the **Default Employee for Interactions** belongs, and then select one employee as the **Default Employee for Interactions**.

The default employee must not have a configured end date. Also, do not select an employee who will soon move or transfer to a different organization.

Once an employee is selected as the **Default Employee for Interactions**, an error message is displayed on the data source screen if the employee has been deleted, terminated, or changed to a different organization since the last time the data source was saved.

 11. If you selected **Generic** as the switch subtype, expand the **Specific Switch Type** area and, in the **Specific Switch Type** field, specify the type of switch. Consult with our engineers for a list of supported switch types.
 12. If you are using the TDM Recorder and selected the **Generic** or **Avaya** switch types, expand the **Recorder TDM Settings** area, then enter values in the following fields:
 - **Off Hook Delay (milliseconds)**—For Service Observe and Single Step Conference only, type the amount of time in milliseconds that the recorder will wait after taking a channel off-hook. Maximum of 6 characters, representing a total time of not more than 15 seconds.
 - **On Hook Delay (milliseconds)**—For Service Observe only, type the amount of time in milliseconds that the recorder will wait after putting a channel on-hook. Maximum of 6 characters, representing a total time of not more than 15 seconds. (The default is 2 seconds.)
 - **Service Observe String**—Service Observe is a type of three-way conference that allows the monitoring of employees on an extension. Type the dial string used to invoke the Service Observe feature on a switch. Use the characters 0–9, #, or *, to a maximum of 16 characters. (The default is 116.)
 - **Inter Digit Delay (milliseconds)**—Type the amount of time in milliseconds that the recorder waits between dialing digits on a channel. Maximum of 6 characters, representing a total time of

- not more than 15 seconds. (The default is 150 milliseconds.)
- **Period Between Service Observe (milliseconds)**—Type a value in milliseconds, between 0 and 10000, to indicate the minimum allowable time between sessions of Service Observe. This setting is for Dedicated Service Observe deployments only and prevents overloading the system with simultaneous requests. The default is 250 milliseconds.
 - **Record Extensions for Internal Calls**—This setting applies to trunk side environments (such as the Avaya switch in trunk-side environment), and hybrid systems where the same data source is used for TDM recording and IP recording (one data source and two member groups). To allow the recording of internal calls on selective recording resources, select this option. If you configure a Gateway Side Correlation Pool member group and an Extension Recording Resource member group, internal calls are recorded regardless of this setting.
 - **Record IP Trunks**—To record all other non-SIP calls using selective DMCC resources when there is no match between CTI events and configured member groups, enable this setting. If you configure a Gateway Side Correlation Pool member group and an Extension Recording Resource member group, all other non-SIP trunk calls are recorded regardless of this setting.
13. If your recorder is part of a package that includes WFM, expand the **WFM Settings** area and configure the following values:
- Specify whether you want to **Use ACD Staffing**.
 - Type an **External Name**.
 - If applicable, from the **Organization** drop-down list, select the organization to which you want to associate this data source.
- i** For this feature, note the following:

 - The Organization selection feature is only visible if you have the Org Scoped Data Sources license.
 - By default, organizations are selected in the drop-down list in one of the following ways:
 - If no organization is configured for a data source, the selected organization is the default root organization.
 - When creating a data source, the selected organization is the user's current organization assignment.
 - The **Organization** drop-down list is not restricted by the user scope, and displays all existing organizations.
 - Child organizations inherit the parent organization association with a data source.
- Select a **Data Source Parent**.
14. Expand the **TimeZone Settings** area, and select one of the **Local Time Tagging Mode** options from the drop-down list:

- **Organization**—to base tagging on the organization. This option is useful in scenarios where employees are working in different regions, allowing you to unify tagging across multiple time zones.



If you select **Organization**, it is still necessary to specify the correct time zone for the data source as described in step 5, where you selected a time zone from the **Time Zone** drop-down list.

Time zone is used in fallback selection for monitored extensions without an associated Employee or Profile (that is, extensions that do not belong to an employee).

- **Data Source**—to base tagging on the time-zone specified in step 5, where you selected a time zone from the **Time Zone** drop-down list.

15. Specify the **Device IP Configuration**.

Select the appropriate **Server Type** (see below), and then select an **Address Type** of either IP Address or Host Name. In the Address field, enter the IP address or host name of the selected server type.

The two **Server Types** are:

- **PBX Side-Near End**—The **PBX Side-Near End** is the server used to send/receive the control messages to/from the extensions. If you have the same extensions in multiple data sources, you must specify the IP address or host name for the signaling interface server. Otherwise, it is not mandatory, but recommended.

The Recorder uses the source or destination address (either the IP address or the host name) of the signaling messages to identify the particular data source with which a call is associated. It does not use any data inside the signaling itself to make this determination. For this reason, the source/destination of the IP packets presented to the Recorder *must be different for each duplicate extension*. Make sure that your network is set up in such a way as to allow for this.

Example:

A proxy server in front of separate PBXes using duplicate extensions can cause IP packets to appear as though they are using the same address (even though the SIP signaling would indicate otherwise). This prevents the correct recording of duplicate extensions.

For more information, see "Recording Duplicate Extensions" under [Extensions \(page 430\)](#).

- **PSTN Side-Far End**—If you are using SIP Trunk Recording, set **PSTN Side-Far End** as the **Server Type** and specify the server address (either the IP address or the host name). This setting is mandatory if you use a Gateway Side Correlation Pool member group with this data source. (See [SIP trunk recording \(page 462\)](#) for more information.)

16. If Scorecards is part of your package, expand the **Scorecards Settings** area and type the **Contact Viewer Server Name**, **Contact Viewer Server Port**, **Contact Viewer URL**. For more details, refer to your Scorecards documentation.
17. Configure **SIP Call Tracking** to achieve session tracking and recording of signaling only calls (non-CTI), typically seen with Interactive Voice Response (IVR).

- **Track Signaling Calls** - Select this setting to enable session tracking for signaling only calls (non-CTI). To disable session tracking for signaling only calls, clear the check mark from this setting. (If you disable the setting, neither of the settings below is applicable). This setting is disabled by default.
- **Separate CTI and Signaling API Commands** - If you select this setting, API commands sent during a signaling or CTI session are applicable only within that session. If a command is sent during an IVR call, and the call then transitions to an agent, the command is cleared. If a command is sent during an agent call, and then the call transitions to IVR, the command is also cleared. If the agent performs operations such as consult, transfer, or conference, any command sent within the agent portion is still applicable to all the portions of the agent call within the contact.

If you clear the check mark from this setting, API commands apply to the entire contact, including any agent calls.
- **Signaling Recording Mode** - Defines the behavior applied to the correlation line on a tracked signaling call. This setting also exists in the Recorder configuration and in that context controls the baseline behavior. Use this setting to control the signaling portion of the call specifically. For example, to capture all signaling recordings, select **Record** as the value. Set to one of the following:
 - **Start On Trigger** —Do not record calls for the extensions associated with this data source until a recording rule is triggered or an external API command starts recording. Recording starts whenever the call starts, but data before the recording trigger is deleted.
 - **Application Controlled**—Record every call for every extension associated with this data source, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the call. If the call is kept, the recording includes all data from the start to the end of the call.
 - **Do Not Record**—Do not record calls for extensions associated with this data source. Recording rules are ignored and cannot trigger recording.
 - **Record**—Record all calls for all extensions associated with this data source. Only a block recording rule, AIM command, or external API command can prevent calls from being recorded.

18. If applicable, expand the **Associated Integration Service Installations** area and select the server that is providing Integration Services for the recorder for which you are configuring this data source.
19. Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system. Do this only in consultation with our field engineers.
20. Click **Save**.

What to do next

- Phone integration: [Create a collection data source for gateway recording \(page 61\)](#)
- Dialer integration: [Create a member group \(page 66\)](#) using [Compliance trunk span member group settings for TDM \(page 68\)](#)

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Workflow: IP-based voice and video recording \(page 33\)](#): Task 2 of 8

[Workflow: Integrate Dialer integration \(page 39\)](#): Task 1 of 7

Create a collection data source for gateway recording

A collection data source is a type of Phone data source. It represents shared gateway resources used by multiple, independent PBX sources. The collection data source holds the gateway member group of associated Recorders, and acts as a “parent” data source to multiple “child” data sources. These child data sources represent the multiple PBXs that may place or receive calls through the recorded gateway(s).



You can add up to 50 child data sources to any given parent Collection data source.

Workflow sequence

[Workflow: IP-based voice and video recording \(page 33\)](#): Task 3 of 8

Procedure

1. In Enterprise Manager, click **Recording Management > Data Sources > Settings**.
2. Click **Create Data Source**.
3. In the Data Source Type dialog box: in the **Type** list, select **Phone**; in the **Switch/Sub Type** list, select **Collection**.
4. Click **Select**.
5. Enter a **Name** for the Phone data source, and a **Description** (optional).
6. Select a **Time Zone** from the list.

The Recorder requires the time zone for accurate recording start and end times.
The time zone selected for the Collection data source applies to all child data sources.
7. In **Recorder Settings**, do the following:
 - a. To prevent the retention of very short calls, specify a **Minimum Session Length (seconds)**.
Active calls (from connected to closed) that are shorter than the specified value will be deleted automatically. If set to zero (0), this feature is disabled and no calls will be deleted based on this setting. The maximum value is 3600 (or one hour). This setting applies to the active duration of CTI Sessions or the entire duration of VOX Sessions. Inactive CTI Sessions can be retained using the Session Auditing Policy.
 - b. If your system uses Performance Mode, which was set in the IP Extension Pool member group, or N+N redundancy, enable the **Rollback Period (minutes)** to ensure that an amount of additional overlapping audio is kept for a period, so that if there is a disconnection, it is possible to retrieve the audio. The default value is 15 minutes, and the maximum value is 60 minutes.
8. Under **Associated Integration Service Installations**, select the server that provides Integration Services for this Recorder. The Integration Service associated with the Collection data source applies to all child data sources.
9. For SIPREC only, associate a SIPREC adapter to the parent Collection data source. This adapter handles INVITE messages from the SBC.
10. Under **Device IP Configuration**:

- a. In **Server Type**, select **PSTN Side - Far End**.
 - b. Enter the **IP Address** or **Host Name** of the PSTN Side - Far End server.
11. Click **Save**.
 12. In the Collection data source, create a **Gateway Side Correlation Pool** member group and associate it to the relevant IP Recorders.
 13. Click **Save**.
 14. Create and configure a Phone data source for each contact center system (PBX).
 - a. Create a child data source that has the same subtype as the other children data sources. For example, you may not have a combination of Cisco and Avaya sources.
 - b. Associate the data source to the same Integration Service as the parent Collection Data Source.
 - c. Make the data source a child: in the **Data Source Parent** field, select the name of the Collection data source created previously.
 - d. For all scenarios, including SIPREC, associate a CTI adapter to each child data source.
 - e. If required for your system to deploy possible member group(s) on the child data sources, refer to the relevant integration guide for instruction.
 - f. Set the Long Call Duration.
The maximum Long Call Duration value from among all those specified in child data sources is used.

What to do next

Voice recording: [Create and edit phones/extensions \(page 125\)](#)

Related topics

[Gateway side correlation pool member group settings \(page 83\)](#)

Create and edit member groups and extensions

You set up the particular type of recording you require (trunk-side, station-side, and so on) by creating member groups. Member groups tie channels to Recorders, and define different groupings and their associations to Recorders, such as TDM extensions, TDM trunk spans and IP extension pools.



When you create a member group you will assign a Recorder Control Type and Fallback Type. The Integration Service uses these and other settings to determine what should be recorded and when—see “Recording Decisions” in the *Technical Overview* for more information about how these settings impact one another.



Each member group requires assignment to a recorder, which automatically assigns any Integration Service associated with the member group to the Recorder. View the relationships on the Associations page.

The types of member groups available to you depend on your specific recording configuration.

Type	Description	Settings
Compliance Station Extension Group	Used to set up extensions for TDM station side recording.	Compliance station extension member group settings for TDM (page 67)
Compliance Trunk Span	Used to simplify the management of multiple phone lines from T1 (up to 24) or E1 (up to 30) trunk spans. Trunk group members are the actual channels derived from the T1 or E1 trunk span.	Compliance trunk span member group settings for TDM (page 68)
IP Extension Pool	Used to group extensions in the IP switch or a hybrid switch that supports both IP and TDM. These groups of extensions are assigned to Recorders. Use this type of member group for DMS and for IP Interception.	IP extension pool member group settings (page 71)
Trunk Span Recording Resource	Used to represent T1 or E1 lines on TDM switches with selective recording capabilities like SO.	Trunk span recording resource member group settings (page 75)

Type	Description	Settings
Extension Recording Resource	Used to represent a list of extensions used on IP switches with selective recording capabilities like SO and SSC (for example, these extensions are used on Avaya as softphone extensions).	Extension recording resource member group settings (page 75)
Selective Extension Pool	A selective extension pool is a list of extensions to be recorded, and at least one recording resource (described above) should be associated with it (the recording resources define and perform the actual recording).	Selective extension pool member group settings (page 77)
Dedicated Extension Pool	Used with the Avaya switch for Dedicated SO (either with DMCC [IP] or TDM). Specific extensions to be recorded are statically assigned to channels (for TDM) or softphones (for DMCC/IP) and the channels or softphones will remain service observed onto the recorded extensions. A dedication extension pool must be associated with a recording resource.	Dedicated extension pool member group settings (page 78)
Multiple Registration Extension Pool	Used in Avaya DMCC environments to support multiple device registration (including support for N+N redundancy).	Multiple registration extension pool member group settings (page 79)
DMCC Recording	Used in Avaya DMCC environments to support Avaya on demand recording. Specific extensions to be recorded are statically assigned to softphones.	DMCC recording group member group settings (page 81)
Gateway Side Correlation Pool	Use this member group to record traffic at a Session Interface Protocol (SIP) Trunk. This includes environments in which SIP trunk sessions are replicated by an edge device such as Acme Packet SBC to the Recorder.	Gateway side correlation pool member group settings (page 83)
Amazon Connect	Used for recording with Amazon Connect data sources.	Amazon Connect member group settings (page 90)

Type	Description	Settings
Microsoft Teams Group	Used for recording with Microsoft Teams data sources.	Microsoft Teams Group member group settings (page 90)
AudioHook Recording	Used for recording with Genesys PureCloud data sources.	AudioHook Recording member group settings (page 92)
Streaming Media Capture Pool	Used to record real-time traffic from a Streaming Media Capture server in Avaya.	Streaming Media Capture Pool member group settings (page 93)
Stream Recording	Used for recording real-time interactions from a cloud contact center that has a real-time streaming API that uses WebHooks for delivering interactions to the Verint system. Used by Twilio Flex and Zoom Contact Center data sources.	Stream Recording member group settings (page 97)

Learn more

The type of member group you create depends on the type of Recorder configuration in use. TDM station-side and TDM trunk-side member groups are used for TDM Recorders, and IP Member Groups are used for IP Recorders. Member groups also define the mechanism used to record the element groups defined within them. Examples of recording mechanisms are CTI Controlled, Recorder Controlled, or Duplicate Streamed, among others.

Trunk Span Recording Resources and Extension Recording Resources are member groups representing resources on a switch that are capable of selectively recording extensions. For example, this could be a TDM E1/T1 line capable of Service Observe or Single Step Conference in the case of a Trunk Span Recording Resource, and IP softphones/Virtual Extensions in the case of an Extension Recording Resource.

A Selective Extension Pool is the list of extensions to be recorded, and you associate them with Trunk Span Recording Resources and Extension Recording Resource member groups to perform the recording. The number of configured phones (among primary extensions only) must not exceed the number of recording resources.

Each member group consists of:

- general properties that depend on the Member Group type
- recorder control type (see [Recorder control types \(page 450\)](#))
- the associated channels (trunks for TDM trunk-side, extensions for TDM station-side and IP)
- an association to a Recorder

Related topics

[Create a member group \(page 66\)](#)

Create a member group

Workflow sequence

[Workflow: Integrate Dialer integration \(page 39\)](#): Task 2 of 7

Before you begin

For a dialer integration, use the settings defined in [Compliance trunk span member group settings for TDM \(page 68\)](#).

Procedure

1. Click **Recording Management > Data Sources > Settings**.
2. Select a data source and then click **Member Groups**.

In a multi-tenant enabled environment, the tenant to which the selected data source is associated displays in parentheses in the screen heading. An organization belongs to a tenant. When a data source is associated to an organization, the screen heading displays the tenant to which the organization belongs. The data source can be associated to a particular tenant or have the **Shared** status. A data source associated to a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

3. Click **Create**.

The **Group Type** dialog box lists the types available to you.



The types of member groups available to you depend on your specific recording configuration.

4. Select the member group type you are creating.
5. Complete the member group settings. See the related topics section for details about settings for each member group type.
6. Click **Save**.

What to do next

Dialer integration: [Create a dialer data source \(page 116\)](#)

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

Compliance station extension member group settings for TDM

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for this extension group (optional).
Port Count	Specify the number of channels (phone extensions) available on the voice card.
Recorder Fallback Type	Select one of the following: <ul style="list-style-type: none"> • Never (Application)—If CTI is disconnected, no audio or screen recording will occur. If CTI is up, CTI segments will be retained. • On CTI Disconnection (Performance)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, only CTI segments with recorded audio are retained; if we receive CTI for a call but no audio (for any reason), recording will not occur. VOX segments (not associated to CTI calls) will be discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings will be held. • Always (Liability)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, both CTI- and VOX- detected segments will be retained. (If a signalling protocol is configured, it will be used before VOX to record the call.)
Shared Recorders	Select one or more Recorders to associate with this Member Group.
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Member groups \(page 441\)](#)

Compliance trunk span member group settings for TDM

Setting	Description
Type	<p>Select a trunk type—the way in which the switch identifies the trunk will determine the type you choose:</p> <ul style="list-style-type: none"> Select Extensions if trunks are configured on the switch as a set of extensions or a signalling group. In a set of extensions, the first channel may be identified by 3000 (the extension) to 3029 (the last channel). See also Associate port numbers with extensions for Extension Compliance Trunk Span Member Groups (page 70). Select Trunk Group if trunks are configured as a trunk group, with each channel identified by 2 numbers (a trunk group and a member). In a signalling group each channel is identified by a common trunk group number and a unique member number. Please refer to the switch configuration documentation for more information. <p>Other available options will depend on the switch type you selected in the associated data source (you should refer to the associated <i>Integration Guide</i> for the most up-to-date information):</p> <ul style="list-style-type: none"> Alcatel 4400—Extension, Alcatel <ul style="list-style-type: none"> i Alcatel uses 3 numbers (crystal, coupler and time slot) to uniquely identify the trunks. These identifiers depend on the voice card in use. Aspect—Extension, Aspect Avaya—Extension, Generic, Trunk Group Generic—I3, TrunkSpan, TrunkGroup, NortelLoop, Generic, Extension, Aspect, Alcatel InteractiveIntelligence—Extension, I3 Nortel CS1000 or Nortel CS2100—Extension, NortelLoop <ul style="list-style-type: none"> i For Nortel a loop number is used to uniquely identify trunk lines. Trader—PCM32 Intecom—Intecom <ul style="list-style-type: none"> i Intecom uses five numbers to uniquely identify the trunks: group, cabinet, shelf, cardslot, and circuit. These identifiers depend on the voice card in use.
Name	Type a unique name for the member group.
Description	Type a description for this extension group (optional).

Setting	Description
Port Count	Specify the number of channels (phone extensions) available on the voice card.
Associated Dialer Data Source	Select an existing Dialer data source from the drop down list. This setting allows trunks to be configured between the switch and dialer for the purpose of nailup call identification.
Recorder Fallback Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Never (Application)—If CTI is disconnected, no audio or screen recording will occur. If CTI is up, CTI segments will be retained. • On CTI Disconnection (Performance)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, only CTI segments with recorded audio are retained; if we receive CTI for a call but no audio (for any reason), recording will not occur. VOX segments (not associated to CTI calls) will be discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings will be held. • Always (Liability)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, both CTI- and VOX- detected segments will be retained. (If a signalling protocol is configured, it will be used before VOX to record the call.)
Shared Recorders	Select one or more Recorders to associate with this Member Group.
Group Members	<p>Group Members are the actual channels on a TDM cable (30 on E1, 23/24 on T1). Do one of the following.</p> <ul style="list-style-type: none"> • For Extension trunk types, type the extension numbers in the fields, or click Generate Extensions, type a Starting Port Number, Number of Ports, and Starting Extension Number, then click Assign. • For Trunk Groups, type in the Trunk Group and Trunk Member numbers, or click the Generate Group/Member button and specify the Trunk Group Number, the Starting Port Number, total Number of Ports, the number of the Starting Trunk Member, and the Trunk Member Prefix. If your data source is Avaya with E1 (30 channels) you can also enter a Trunk Member to Skip (may be required for ISDN type E1 trunks). Click Assign when you are finished.
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.



Additional fields may appear, depending on your switch type. Refer to the associated *Integration Guide* for details.



You can generate trunk members automatically to create phone extensions from PCM32, Extension, Generic, and Trunk Group trunk spans after clicking the **Generate Extensions** or **Generate Members** button. Type the starting extension number in the Starting Extension Number field. For example, with a Compliance Trunk Span Member Group, 24 extensions are created default. So if you type 1250 as the Starting Device Number, the final extension would be 1250 plus 24 (1274).

Associate port numbers with extensions for Extension Compliance Trunk Span Member Groups

For TDM trunk spans, the configuration you set for the recorder must match the configuration of the trunk in the existing environment, so that the CTI messages can be associated with the trunk channels for recording. The PBX administrator on site can advise whether the trunks are configured as extensions or not. Typically trunks from the Service Provider will not be extensions. Trunks on dialers or IVRs are sometimes configured as extensions.

Under **Group Members**, you can associate port numbers with extensions by doing one of the following:

- type an extension number (for example, 3344) in each field, then click **Save**.
- or
- automatically assign extensions by clicking **Generate Extensions**, type the **Starting Port Number**, the total **Number of Ports**, and the **Starting Extension Number**, then click **Assign**.

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Member groups \(page 441\)](#)

IP extension pool member group settings

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for this extension group (optional).
Recorder Control Type	Select one of the following: <ul style="list-style-type: none">• Recorder Controlled—The Recorder controls recording of the extensions or trunks, and implements the default recording modes. In this case the Integration Service is used for segmentation, stitching, and tagging purposes.• Full Delivery (External Controlled)—Recording is used in compliance delivery recording and is controlled by a 3rd party application, which redirects audio to the Recorder. For use with Cisco DMS (where the Recording Option of the line has been set to Automatic Call Recording), Genesys SIP full Delivery, and NEC NEAX.• CTI Controlled—Used in environments with interception recording, where the Integration Service will tell the Recorder when to start and stop recording.• Selective Delivery (Duplicate Streamed)—Used in selective delivery recording. Specifically, in environments where the Integration Service issues requests to start recording to a 3rd party application. For use with SAP switches, and Avaya DMCC, Avaya NES DMS, and Cisco Call Recording, where the Recording Option of the line is set to Application Invoked Call Recording.

Setting	Description
Recorder Load Balancing Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • None—A single recorder records all calls and no load balancing will occur. • Media Only—Multiple recorders are used to record the calls and all recorders will be aware of signaling (both call control and media control messages) for all calls. Only one of the recorders will be aware of the audio. Example deployments are: <ul style="list-style-type: none"> ▪ Using a load balancing device or link protector to manage the traffic. ▪ Using IP Analyzer to control a group of recorders. • Media with Signaling—Multiple recorders are used to record the calls. Use only in Recorder Controlled environments where one of the recorders will be aware of the call (that is, call control and media control messages + audio), while other recorders are not aware of this call. Do not use this option in CTI controlled environments. An example deployment would be the use of Acme Packet SBC to load balance the traffic. • Shared Interception—Multiple recorders are used to record the calls. All recorders will be aware of all the calls (that is, call control and media control messages + audio). The Integration Service load balances call recording by enabling and disabling available resources. Use this for deployments in which multiple recorders have the same network SPAN. • Dedicated Interception—Available only if the Recorder Control Type is Recorder Controlled. Multiple recorders are used to record the calls and all recorders will be aware of all the calls (that is, call control and media control messages + audio). Enterprise Manager controls load balancing of call recording by distributing the extension list to all recorders with which this Member Group is associated.
	<p>i There are two ways that load balancing can be applied to extensions: automatic and manual. Automatic will occur only if the recorders are over capacity. If you select Dedicated Interception as the Load Balancing Type, you can perform manual rebalancing by clicking Rebalance Extensions, and rebalancing will occur regardless of whether the recorders are at capacity.</p>

Setting	Description
Recorder Fallback Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Never (Application)—If CTI is disconnected, no audio or screen recording will occur. If CTI is up, CTI segments will be retained. • On CTI Disconnection (Performance)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, only CTI segments with recorded audio are retained; if we receive CTI for a call but no audio (for any reason), recording will not occur. VOX segments (not associated to CTI calls) will be discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings will be held. • Always (Liability)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, both CTI- and VOX-detected segments will be retained. (If a signalling protocol is configured, it will be used before VOX to record the call.)
Recorder Selection Expression	<p>You can use this setting only in Avaya DMCC SSC/SO or Shared Interception environments.</p> <p>This setting allows individual calls to be directed to the recorder associated with this member group based on specific call data (for example, the call's trunk group).</p> <p>Select an Attribute from the dropdown list, then type a value in the Expression field. If the call data matches the expression, the call will be recorded by this recorder.</p> <p>The Recorder Selection Expression is limited to one hundred (100) characters.</p> <p>i The match must be identical and the attribute to be evaluated must be present when the attempt to record is made. If the exact data in the Expression field for that attribute is not present in the call data, then the call will not be recorded by a recorder to which the IP Extension Pool member group is assigned. The call can still be recorded by other member groups or recording resources if the configuration of your system allows.</p> <p>If you are using a custom attribute, you must first add this attribute to the system, under Recording Management > Custom Data—see Create, edit or delete an attribute (page 278).</p> <p>You must also select either LineFirst or LineExclusive as the Recording Resource Allocation Behavior—see Create a phone data source (page 49).</p>

Setting	Description
IP Network Region	<ul style="list-style-type: none"> • Network - Select this type to assign all phones on a subnet to the member group. Complete these additional fields: <ul style="list-style-type: none"> ▪ Network - Enter the IP address that identifies the network on which the phones reside. ▪ Mask - Specify the subnet mask applicable to the network on which the phones reside. • Host IP - Select this type to assign a phone to the member group using the phone IP address. In the Network setting, enter the IP address of the phone. • Host Name - Select this type to assign a phone to the member group using the phone host name. In the Network setting, enter the host name of the phone.
Total Extensions/Total Capacity	This is a read-only field that appears only when the Recorder Load Balancing Type is Dedicated Interception .
Shared Recorders	Use this section to associate one or more Recorders with this Member Group.
Shared Recorder Adapter Proxy Services	A Recorder Adapter Proxy Service (RAPS) server role association is valid only when either Selective Delivery (Duplicate Streamed) or Full Delivery (External Controlled) is selected as the Recorder Control Type . A RAPS server role association is mandatory to support SIP scaling. If you have a legacy SIP deployment, and do not want to support SIP scaling, it is not necessary to associate a RAPS server role to the member group.
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.



Recorder capacity cannot exceed available resources. For Extension Recording resources, available capacity is determined by the number of softphones in the extension recording resources. For Trunk Span Recording Resources, the total number of associated ports determines the capacity.

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Member groups \(page 441\)](#)

Trunk span recording resource member group settings

A Trunk Span Recording Resource is used to represent T1 or E1 lines on TDM switches with recording capabilities such as SO.



To create this type of member group, you must first select a phone data source with an Alcatel, Avaya, or Generic switch type in the left-hand pane.

Setting	Description
Type	Select one of the following trunk span types: Extensions, or Trunk Group (other types may be available depending on your switch type). The fields that appear below will be different depending on the Type you choose.
Name	Type a unique name for the member group.
Description	Type a description for this extension group (optional).
Port Count	Specify the number of channels (phone extensions) available on the voice card.
Recorder Control Type	Set to either Service Observe or Single Step Conference (not available for Alcatel, which is set to DRLink by default). See Recorder control types (page 450) for descriptions.
Crystal	Alcatel only. Enter the number representing the Crystal shelf. The Crystal, Couple, and First Time Slot numbers are combined to create group member names in the Group Members section below. These identifiers depend on the voice card in use.
Coupler	Alcatel only. Enter the coupler number for the Alcatel 4400.
First Time Slot	Alcatel only. For TDM setups, enter the number of the first time slot.
Shared Recorders	Use this section to associate one or more Recorders with this Member Group.
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Member groups \(page 441\)](#)

Extension recording resource member group settings

An Extension Recording Resource is used to represent a list of extensions used on IP switches with recording capabilities like SO and SSC (for example, these extensions are used on Avaya as softphone

extensions).



To create this type of member group, you must first select a phone data source with an Alcatel, Avaya, or Generic switch type in the left-hand pane.

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for this extension group (optional).
Recorder Control Type	Set to either Service Observe (not available for Alcatel) or Single Step Conference . See Recorder control types (page 450) for descriptions.
CLAN Boards	To specify the recording location based on extension, type an IP address (or series of addresses, separated by commas) of a CLAN in this field (optional).
Recorder Selection Expression	<p>This setting allows individual calls to be directed to the recorder associated with this member group based on specific call data (for example, the call's trunk group). Select an Attribute from the dropdown list, then type a value in the Expression field. If the call data matches the expression, the call will be recorded by this recorder.</p> <p>The Recorder Selection Expression is limited to one hundred (100) characters.</p> <p>i The match must be identical and the attribute to be evaluated must be present when the attempt to record is made. If the exact data in the Expression field for that attribute is not present in the call data, then the call will not be recorded.</p> <p>If you are using a custom attribute, you must first add this attribute to the system, under Recording Management > Custom Data—see Create, edit or delete an attribute (page 278).</p> <p>You must also select either LineFirst or LineExclusive as the Recording Resource Allocation Behavior—see Create a phone data source (page 49).</p> <p>In the context of this member group type, this feature is applicable to Avaya DMCC environments only.</p>
Recording Beep Tone	Recording Beep Tone: When enabled, participants on a call hear a beep when the Recorder starts recording the call. By default, the beep tone is disabled. To enable this option, select the check box. Note: The duration, pitch, and repetition of the tone are configured in Avaya Communication Manager.
Shared Recorders	Select one or more IP Recorders to associate to this member group.
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.

i Depending on the Trunk Span Type you selected, additional fields may appear—refer to the associated Integration Guide for more information.

i Recording Resource extensions can be assigned with only one member group (other extensions can be associated with multiple member groups).

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Member groups \(page 441\)](#)

Selective extension pool member group settings

Used for Selective Service Observe or Single Step Conference deployments. This member group type applies only to Alcatel, Avaya DMCC, and Generic Switch Types. You must create a [Trunk span recording resource member group settings \(page 75\)](#) or [Extension recording resource member group settings \(page 75\)](#) before completing the following procedure. (See the Avaya or Alcatel *Integration Guide* for more information.)

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for this extension group (optional).
Associated Member Groups	Select one or more recording resources—this is the member group that defines how and where recording is actually performed. Only Extension Recording Resource and Trunkspan Recording Resource member groups will be available for association with Selective Extension Pools.
Recorder Fallback Type	Select one of the following from the drop-down list: <ul style="list-style-type: none"> Never (Application)—If CTI is disconnected, no audio or screen recording will occur. If CTI is up, CTI segments will be retained. On CTI Disconnection (Performance)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, only CTI segments with recorded audio are retained; if we receive CTI for a call but no audio (for any reason), recording will not occur. VOX segments (not associated to CTI calls) will be discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings will be held.
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.

After you finish creating or editing a Selective Extension Pool Member Group settings, click **Assign & Create Phones**, then select one or more phones and click **Assign Selected or Assign Range**. The Member Groups screen displays the list of extensions (secondary extensions are not included in this list).



You can only assign primary extensions to selective extension pools. You cannot assign recording resources/virtual extensions to Selective Extension Pool member groups.

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Member groups \(page 441\)](#)

Dedicated extension pool member group settings

Used with the Avaya switch for Dedicated SO (either with DMCC [IP] or TDM). Specific extensions to be recorded are statically assigned to channels (for TDM) or softphones (for DMCC/IP) and the channels or softphones will remain service observed onto the recorded extensions. A dedicated extension pool member group must be associated with a recording resource—see [Trunk span recording resource member group settings \(page 75\)](#) and [Extension recording resource member group settings \(page 75\)](#) to create these before you proceed.

For recording resources to be available to this member group, only one recorder must be associated with the recording resource. The **Recorder Control Type** of the recording resource must be set to **Service Observe**, and the recording resource must not be associated with any other member group.



This member group cannot be associated with a selective extension pool.

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for this extension group (optional).
Recorder Fallback Type	Select one of the following from the drop-down list: <ul style="list-style-type: none"> On CTI Disconnection (Performance)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, only CTI segments with recorded audio are retained; if we receive CTI for a call but no audio (for any reason), recording will not occur. VOX segments (not associated to CTI calls) will be discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings will be held. Always (Liability)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, both CTI- and VOX- detected segments will be retained. (If a signalling protocol is configured, it will be used before VOX to record the call.) (If a signalling protocol is configured, it will be used before VOX to record the call.)
Associated Member Groups	Select a Trunk Span or Extension Recording Resources to associate with this member group.
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.

When you have finished editing this member group click **Assign & Create Phones**, then select one or more phones and click **Assign Selected** or **Assign Range**. Note that the number of configured phones must not exceed the number of recording resources.

i There are two ways that load balancing can be applied to extensions: automatic and manual. Automatic will occur only if the recorders are over capacity. If you select Dedicated Interception as the Load Balancing Type, you can perform manual rebalancing by clicking **Rebalance Extensions**, and rebalancing will occur regardless of whether the recorders are at capacity.

! Recorder capacity cannot exceed available resources. For Extension Recording resources, available capacity is determined by the number of softphones in the extension recording resources. For Trunk Span Recording Resources, the total number of associated ports determines the capacity.

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Member groups \(page 441\)](#)

Multiple registration extension pool member group settings

Used in Avaya DMCC environments with multiple registration, which allows you to have multiple devices associated with a single extension (to a maximum of three devices in total). With Aura 8.0.1 and newer, the multiple registration limit of devices that can be registered to a common extension is increased from 3 to 10.

i The Multiple Registration Extension Pool member group can be created for either an Avaya or generic data source.

See the *Avaya and Avaya NES Integration with Recorder Guide* for more details, including prerequisites and limitations.

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for this extension group (optional).
Recorder Control Type	Read-only field that shows Multiple Registration Control for this member group.

Setting	Description
Recorder Fallback Type	<p>In environments with multiple registration, fallback options are limited to those in which audio recording continues when the CTI or recorder disconnects from the Integration Service.</p> <p>Select one of the following from the drop-down list:</p> <ul style="list-style-type: none"> • Never (Application). If CTI is disconnected, no audio or screen recording occur. If CTI is up, recording with CTI marking occurs. • On CTI Disconnection (Performance). If CTI is disconnected, audio recording continues (VOX-detected segments are retained), but screen recording does not. If CTI is up, audio recording with CTI marking occurs. If we receive CTI for a call but no audio (for any reason), recording does not occur. VOX segments (not associated to CTI calls) are discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings are held. • Always (Liability). If CTI is disconnected, audio recording continues (VOX-detected segments are retained), but screen recording does not. If CTI is up, both CTI- and Vox- detected segments are retained. (If a signaling protocol is configured, it is used before VOX to record the call.)
Total Extensions/Total Capacity	Displays the number of extensions in use, relative to the total capacity.
Enable Stereo Recording	Enables recording of separate customer and agent streams for recorded calls. Enabling this feature affects the licensing. For more details, see the related information.
DMCC Control Type	<p>The Avaya DMCC Multiple Registration automatically selects dependent and independent modes for the softphones assigned to the local stations. However, you can manually set the control type, if needed. Select one of the following from the drop-down list:</p> <ul style="list-style-type: none"> • Automatic (Default). The system automatically determines the proper mode based on the station type queried from the system. H.323 phones register in dependent mode. SIP phones register in independent (non-persistent) mode. When Automatic is selected, the Station Monitoring option is available. • Independent (Non-persistent). All phones register in independent mode, but do not persist past the main station registration. If the main station goes out-of-service, the independent softphones are unregistered. • Independent (Persistent). All phones register in independent mode and persist indefinitely. The registration state of the main station does not impact the state of the softphone registration.

Setting	Description
Station Monitoring	<p>By default, this option is turned off and is accessible only when the DMCC Control Type is set to Automatic.</p> <p>The Verint adapter only captures interactions from registered Avaya stations (softphones). When in Automatic mode, upon startup, the Verint adapter queries Avaya for agent stations.</p> <p>With Station Monitoring off, as agents sign in, the Verint adapter queues station registrations, potentially causing delays in larger systems. A DMCC license is only consumed when softphone stations are active and an agent is logged in, possibly leading to unnecessary alarms in large systems.</p> <p>With Station Monitoring on, the Verint adapter instantly registers all Avaya stations, eliminating registration queues and reducing recording initiation time. However, it consumes a DMCC license for each station, irrespective the status of the stations.</p> <p>Changes you make take effect immediately, without requiring a restart or re-registration of the stations.</p>
Recording Beep Tone	<p>Recording Beep Tone: When enabled, participants on a call hear a beep when the Recorder starts recording the call. By default, the beep tone is disabled. To enable this option, select the check box. Note: The duration, pitch, and repetition of the tone are configured in Avaya Communication Manager.</p>
Advanced Parameters	<p>Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.</p>

When you have finished editing this member group, click **Assign & Create Phones**, then select one or more phones and click **Assign Selected** or **Assign Range**.

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Member groups \(page 441\)](#)

Related information

Multiple Registration Licensing Requirements (*Recorder Integration Service Avaya Integration Guide*)

DMCC recording group member group settings

This member group is used in Avaya DMCC environments to support Avaya record on demand. It contains both the extensions being recorded and the resources (or DMCC soft phones) used to capture the audio recording. You can assign a pool of IP Recorders to this member group. The assigned resources are load balanced across the pool of assigned IP Recorders.

Setting	Description
Name	Type a unique name for the member group.

Setting	Description
Description	Type a description for this extension group (optional).
Recorder Control Type	The parameter is always set to Record on Demand and cannot be changed. This type supports the Avaya record-on-demand functionality.
Recorder Fallback Type	<p>In multiple registration environments, fallback options are limited to those in which audio recording continues in the event of CTI or recorder disconnection from the Integration Service.</p> <p>Select one of the following from the drop-down list:</p> <ul style="list-style-type: none"> • Never (Application) - If CTI is disconnected, no audio or screen recording occur. If CTI is up, recording with CTI marking will occur. • On CTI Disconnection (Performance)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, audio recording with CTI marking will occur; if we receive CTI for a call but no audio (for any reason), recording will not occur. VOX segments (not associated to CTI calls) will be discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings will be held. • Always (Liability)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, both CTI- and Vox- detected segments will be retained. (If a signaling protocol is configured, it will be used before VOX to record the call.)
Recording Beep Tone	<p>Recording Beep Tone: When enabled, participants on a call hear a beep when the Recorder starts recording the call. By default, the beep tone is disabled. To enable this option, select the check box. Note: The duration, pitch, and repetition of the tone are configured in Avaya Communication Manager.</p>
Assigned Recorders	Select the Avaya recorders to be associated to this member group. Select multiple recorders to create a pool of recorders to support the Avaya record-on-demand functionality.
Assigned Phones	The extensions assigned to the member group. Extensions are associated to the DMCC soft phones. Click the Assign & Create Phones button to assign extensions to the member group.
Assigned Resources	<p>The DMCC soft phones assigned to the member group. The assigned DMCC soft phones are used to capture the audio recording.</p> <p>To add phones to this member group, click Assign & Create Resources, select the DMCC soft phones to add to this member group, and then click Save.</p> <p>After adding or removing phones and resources, or when the recorder capacity changes, use the Rebalance Resources option to distribute the load of resources (soft phones) evenly across the pool of assigned recorders.</p> <p> Clicking Rebalance Resources interrupts recording while rebalancing occurs. Use this option when recording activity is at its lowest.</p>

Setting	Description
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.

Gateway side correlation pool member group settings

Use this member group to record traffic at a Session Interface Protocol (SIP) Trunk. This includes environments in which SIP trunk sessions are replicated by an edge device such as Acme Packet SBC to the Recorder.

SIP Trunk Recording is established at the member group level (not at the extension level). For more information—including additional configuration details—see [SIP trunk recording \(page 462\)](#), and the *Avaya or Genesys Integration Guide*.

When used with an IP Trade data source, only the Recorder Control Type, Recorder Load Balancing Type, and Recorder Fallback Type settings are available. Each of these settings is configured with a default value that cannot be changed. For more information, see the *IP Trade Unified Integration Guide*.

When used with a Five9 VoiceStream data source, the Recorder Control Type and Recorder Load Balancing type are configured with a default value that cannot be changed. The other settings are configurable. For more information, see the *Five9 VoiceStream Integration with Recorder Guide*.

- The Gateway Side Correlation Pool member group type is only available for Avaya, Genesys, IP Trade, Five9 VoiceStream, and Generic phone data sources. In certain cases, you may need to configure a Collection data source—see [Create a collection data source for gateway recording \(page 61\)](#).

VOX metadata with Gateway Correlation recording

With Gateway Correlation recording, the CTI feed provides all extension-level information. If the IP Recorder is disconnected from the CTI feed (either through disconnection from the Recorder Integration Service itself or the CTI adapter going down), the resulting VOX recordings will not have extension-level information associated with them. Customers can choose to retain or discard these VOX recordings through the Recorder Fallback setting in the member group.

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for this extension group (optional).

Setting	Description
Recorder Control Type	<ul style="list-style-type: none"> • Recorder Controlled—Use this option when the Recorder itself (rather than the Integration Service) starts and stops recording. This option applies to IP interception environments where recording occurs through SIP session replication or standard SIP trunk spanning. • Full Delivery (External Controlled)—Use this option in compliance delivery SIPREC recording environments where recording is controlled by a 3rd party application. • Selective Delivery (Duplicate Streamed)—Use this option in selective recording SIPREC environments where the Integration Service issues requests to start recording to a 3rd party application.
Recorder Load Balancing Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • None—A single recorder records all calls and no load balancing will occur. • Media Only—Multiple recorders are used to record the calls and all recorders will be aware of signaling (both call control and media control messages) for all calls. Only one of the recorders will be aware of the audio. Example deployments are: <ul style="list-style-type: none"> ▪ Using a load balancing device or link protector to manage the traffic. ▪ Using IP Analyzer to control a group of recorders. • Media with Signaling—Multiple recorders are used to record the calls. Use only in Recorder Controlled environments where one of the recorders will be aware of the call (that is, call control and media control messages + audio), while other recorders are not aware of this call. Do not use this option in CTI controlled environments. An example deployment would be the use of Acme Packet SBC to load balance the traffic. <p>This setting is unavailable when Selective Delivery (Duplicate Streamed) is selected as the Recorder Control Type.</p>

Setting	Description
Recorder Fallback Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Never (Application)—If CTI is disconnected, no audio or screen recording will occur. If CTI is up, CTI segments will be retained. • On CTI Disconnection (Performance)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, only CTI segments with recorded audio are retained; if we receive CTI for a call but no audio (for any reason), recording will not occur. VOX segments (not associated to CTI calls) will be discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings will be held. • Always (Liability)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, both CTI- and VOX- detected segments will be retained. (If a signalling protocol is configured, it will be used before VOX to record the call.) <p>This setting is unavailable when Selective Delivery (Duplicate Streamed) is selected as the Recorder Control Type.</p>
Recorder Selection Expression	<p>This setting allows individual calls to be directed to the recorder associated with this member group based on specific call data (for example, the call's trunk group). Select an Attribute from the dropdown list, then type a value in the Expression field. The "expression" is a standard regular expression and can be used to create a selection based on multiple values for the selected attribute. If the call data matches the expression, the call will be recorded by this recorder.</p> <p>The Recorder Selection Expression is limited to one hundred (100) characters.</p> <div data-bbox="442 1136 474 1178" style="background-color: #3366CC; color: white; border-radius: 50%; padding: 2px 5px; font-weight: bold;">i</div> <p>The match must be identical and the attribute to be evaluated must be present when the attempt to record is made. If the exact data in the Expression field for that attribute is not present in the call data, then the call will not be recorded by any recorder to which a Gateway-Side Correlation Pool member group is assigned (the call can still be recorded by other member groups or recorders if the configuration of your system allows).</p> <p>If you are using a custom attribute, you must first add this attribute to the system, under Recording Management > Custom Data—see Create, edit or delete an attribute (page 278).</p> <p>You must also select either LineFirst or LineExclusive as the Recording Resource Allocation Behavior—see Create a phone data source (page 49).</p> <p>The Recorder Selection Expression feature is no longer required to record internal calls using DMCC with SIPREC solutions. When a selective extension pool is available, recording of internal calls through DMCC is done automatically.</p>

Setting	Description
Correlation Key	<p>Create a Correlation Key to use an attribute other than the default (see your Integration Guide for details) to establish an association between a call recording and its CTI attributes.</p> <p>⚠ You should only do this if instructed to do so by your support representative.</p> <p>A Correlation Key allows the Integration Service to associate the CTI attributes of a call with the call recording in custom configurations. When a call is received by a data source in a SIP recording environment, the following occurs:</p> <ul style="list-style-type: none"> • CTI attributes are sent from the data source to the Integration Service (to provide the Integration Service with call metadata). • SIP messages are sent from the data source to the Recorder (to set up the call on the Recorder). <p>The Correlation Key associates a CTI attribute with a matching value in a SIP header field. To create a correlation key:</p> <ol style="list-style-type: none"> 1. Click the Add button. 2. From the CTI Attributes drop-down box, select an Attribute. 3. In the Recorder Attribute text box, type the name of a SIP message header that specifies the same value as a CTI Attribute. <p>Example: The following example illustrates the use of a Correlation Key:</p> <ul style="list-style-type: none"> • A data source sends the CTI attribute "SomeID" (a unique identifier of the call) to the Integration Service. For this data source, the equivalent CTI attribute might be mapped to a custom attribute called "SomeID". • The data source also sends a SIP request to the Recorder that includes a header called Vendor-SomeID header. This SIP header specifies the same value as the equivalent CTI attribute. In this scenario, to create the Correlation Key, select SomeID as the CTI Attribute, and specify Vendor-SomeID as its associated Recorder Attribute in the text box.

Setting	Description
	<p>Notes:</p> <ul style="list-style-type: none"> • Create multiple Correlation Keys only if there is no single Correlation Key that can accomplish the association of CTI attributes to call recordings for every call. If you specify multiple keys, the order will be the order of preference (that is, the system will use the second key only if the first key doesn't establish a correlation, and so on). • IP Gateway Side recording is the only form of IP recording for which you configure a Correlation Key. All other IP recording configurations use the CTI attribute and the SIP message header that specify the device extension as the common value that ensures that a call's CTI attributes are associated to its recording. With Gateway Side recording, the Recorder cannot identify the device extension in a SIP message header, so the system relies on a different attribute (other than device extension) to make the association. • The correlation keys are required to be unique in the call space. This means that no two (2) independent calls shall have the same correlation value. Related calls may share a correlation value, but are expected to contain identical media for the portion of time they overlap. • The correlation keys are recommended to be unique, non-repeating, and call specific identifiers. Selecting a correlation key that does not have these qualities can yield undesired results in recording and playback. • Unique means that no two (2) independent calls share the same value at the same time. • Non-repeating means that no two (2) independent calls share the same value ever. • Call specific means that as the call is updated / moved, the identifier updates / moves with the call. • If the correlation value changes, it must do so in the signaling (e.g. SIPREC) and CTI feed simultaneously. • For SIP feeds, the correlation key should come from a SIP header. • For SIPREC feeds, the correlation key should come from the metadata XML. • Customers should minimize the number of correlation keys to be tracked by the system. More keys will complicate the configuration, impact performance, and make troubleshooting and support more difficult.

Setting	Description
IP Network Region	<ul style="list-style-type: none"> Network - Select this type to assign all phones on a subnet to the member group. Complete these additional fields: <ul style="list-style-type: none"> Network - Enter the IP address that identifies the network on which the phones reside. Mask - Specify the subnet mask applicable to the network on which the phones reside. <p> Specifying a subnet mask of 255.255.255.255 is the same as specifying an individual IP address.</p> Host IP - Select this type to assign a phone to the member group using the phone IP address. In the Network setting, enter the IP address of the phone. Host Name - Select this type to assign a phone to the member group using the phone host name. In the Network setting, enter the host name of the phone.
Shared Recorders	Use to associate one or more Recorders with this Member Group.
Shared Recorder Adapter Proxy Services	A Recorder Adapter Proxy Service (RAPS) server role association is valid only when either Selective Delivery (Duplicate Streamed) or Full Delivery (External Controlled) is selected as the Recorder Control Type . A RAPS server role association is mandatory to support SIP scaling. If you have a legacy SIP deployment, and do not want to support SIP scaling, it is not necessary to associate a RAPS server role to the member group.
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.



In your Phone data source you must specify the **IP Address** or **Host Name** of the call center's SIP trunk interface. Set the Server Type under **Settings > Device IP Configuration** to **PSTN Side - Far End**.

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Member groups \(page 441\)](#)

[Create a phone data source \(page 49\)](#)

Device Location member group Settings

The following applies to certain Trading systems only.

Field	Description
Name	Member group name (required).
Description	Description of the member group (optional).
Recorder Control Type	Set to Full Delivery (External Controlled) (display only).
Recorder Load Balancing Type	Set to Media With Signaling (display only).
Recorder Fallback Type	Set to Always (Liability) (display only).
Default Location	Main device location. Each data source can have one default device location. The recorders assigned to the default device location resource are used to record turrets whose device location does not match another device location member group.
Device Location	One or more location strings can be added for member groups created for remote sites. Member groups for the default location (main site) do not use the location string since the Default Location setting is already enabled. The location string is case sensitive.  If a Location is changed and saved in the Device Location Resource member group, ensure that all traders log off the turret in order for the changes to take effect.
Shared Recorders	IP Recorder server roles that will record turrets at this location.
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Member groups \(page 441\)](#)

Amazon Connect member group settings

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for this extension group (optional).
Recorder Control Type	The setting Selective Delivery (Duplicate Streamed) is selected by default and cannot be changed. The Recorder Integration Service will dynamically engage the audio stream in real time based off the CTI feed.
Recorder Fallback Type	The setting Never (Application) is selected by default and cannot be changed. With this setting, If CTI is disconnected, no audio or screen recording will occur. If CTI is up, CTI segments will be retained.
Recorder Load Balancing Type	The setting None is selected by default and cannot be changed. The Recorder Integration Service will internally load balance the calls to the recorders.
Shared Recorders	In this section, you must associate one or more IP Recorders with this member group.
Shared Recorder Adapter Proxy Services	In this section, you must associate one or more Recorder Adapter Proxy Service server roles with this member group. The Recorder Adapter Proxy Service server role must be on the same server as the Recorder server role associated to the member group in the Shared Recorders setting. A correct association includes the Recorder Adapter Proxy Service + IP Recorder.
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Member groups \(page 441\)](#)

Microsoft Teams Group member group settings

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for this member group (optional).

Setting	Description
Recorder Control Type	<ul style="list-style-type: none"> Full Delivery (External Controlled) - Recording is controlled by a 3rd party application which redirects audio to the Recorder. This setting is the default. Selective Delivery (Duplicate Streamed) - The Recorder Integration Service will dynamically engage the audio stream in real time based off the CTI feed.
Recorder Load Balancing Type	<p>The setting None is selected by default and cannot be changed. The Recorder Integration Service will internally load balance the calls to the recorders.</p>
Recorder Fallback Type	<ul style="list-style-type: none"> Never (Application) - With this setting, if CTI is disconnected, no audio or screen recording will be kept. If CTI is up, CTI segments will be retained. On CTI Disconnection (Performance) - If CTI is disconnected, audio recording continues (VOX-detected segments will be retained). If CTI is up, only CTI segments with recorded audio are retained. VOX segments (not associated to CTI calls) will be discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings will be held. Always (Liability) - If CTI is disconnected, audio recording continues (VOX-detected segments will be retained). If CTI is up, both CTI- and VOX-detected segments will be retained. (If a signaling protocol is configured, it will be used before VOX to record the call.) This setting is the default.
Shared Recorders	<p>Use this section to associate one or more Recorder server roles with this Member Group. You must associate the member group either to an IP Recorder server role, an IP Recorder Video server role, or both.</p>
Shared Recorder Adapter Proxy Services	<p>Use this section to associate one or more Recorder Adapter Proxy Service server roles with this Member Group. You must associate a Recorder Adapter Proxy Service server role to the member group. The Recorder Adapter Proxy Service server role must be on the same server as the Recorder server role associated to the member group in the Shared Recorders setting.</p> <p>Correct associations include any of the following:</p> <ul style="list-style-type: none"> Recorder Adapter Proxy Service + IP Recorder Recorder Adapter Proxy Service + IP Recorder Video Recorder Adapter Proxy Service + IP Recorder + IP Recorder Video
Advanced Parameters	<p>Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.</p>

AudioHook Recording member group settings

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for this extension group (optional).
Recorder Control Type	<ul style="list-style-type: none"> Full Delivery (External Controlled) - Recording is controlled by a 3rd party application which redirects audio to the Recorder. This setting is the default. Selective Delivery (Duplicate Streamed) - The Recorder Integration Service will dynamically engage the audio stream in real time based off the CTI feed.
Recorder Load Balancing Type	The setting None is selected by default and cannot be changed. The Recorder Integration Service will internally load balance the calls to the recorders.
Recorder Fallback Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> Never (Application)—If CTI is disconnected, no audio or screen recording will occur. If CTI is up, CTI segments will be retained. If Selective Delivery (Duplicate Streamed) is selected as the Recorder Control Type, this setting is selected by default and cannot be changed. On CTI Disconnection (Performance)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, only CTI segments with recorded audio are retained; if we receive CTI for a call but no audio (for any reason), recording will not occur. VOX segments (not associated to CTI calls) will be discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings will be held. If Full Delivery (External Controlled) is selected as the Recorder Control Type, this setting is selected by default. Always (Liability)—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, both CTI- and VOX- detected segments will be retained. (If a signalling protocol is configured, it will be used before VOX to record the call.)
Shared Recorders	In this section, you must associate one or more IP Recorders with this member group.
Shared Recorder Adapter Proxy Services	<p>In this section, you must associate one or more Recorder Adapter Proxy Service server roles with this member group. The Recorder Adapter Proxy Service server role must be on the same server as the Recorder server role associated to the member group in the Shared Recorders setting.</p> <p>A correct association includes the Recorder Adapter Proxy Service + IP Recorder.</p>
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.

Streaming Media Capture Pool member group settings

Use the Streaming Media Capture Pool member group to record call media in real time from a Streaming Media Capture server.

Setting	Description
Name	Enter a unique name for the member group.
Description	Optional. Describe the group.
Recorder Control Type	<p>Full Time Recording: The Recorder automatically starts recording each SMC connection that it receives. The Recorder Integration Service keeps or discards call audio based on real-time event notifications and the fallback mode, making it more resilient to logical errors and failures.</p> <p>Selective Recording: The recorder does not automatically start recording each received SMC connection and must be commanded to start and stop each connection. The Recorder Integration Service commands the recorder to enable and disable the streams based on the real-time event stream.</p>
Recorder Load Balancing Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • None—A single recorder records all calls and no load balancing occurs. If this option is set to None and cannot be changed, then the Recorder Control Type is Full Time Recording. • Media Only—Multiple recorders are used to record calls, and all recorders are aware of signaling (both call control and media control messages) for all calls. Only one of the recorders is aware of the audio. Example deployments are: <ul style="list-style-type: none"> ■ Using a load-balancing device or link protector to manage the traffic. ■ Using IP Analyzer to control a group of recorders. • Media with Signaling—Multiple recorders are used to record calls. Use this setting only in Recorder-Controlled environments where one recorder is aware of the call (including call control, media control messages, and audio), while other recorders are not. Do not use this option in CTI-controlled environments. An example deployment is using Acme Packet SBC to load balance the traffic.

Setting	Description
Recorder Fallback Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • On CTI Disconnection (Performance)—If CTI is disconnected, audio recording continues (VOX-detected segments are retained), but screen recording does not. If CTI is up, only CTI segments with recorded audio are retained; if we receive CTI for a call but no audio (for any reason), recording does not occur. VOX segments (not associated to CTI calls) are discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings are held. This setting is available when Recorder Control Type is Full time Recording. • Always (Liability)—If CTI is disconnected, audio recording continues (VOX-detected segments are retained), but screen recording does not. If CTI is up, both CTI- and VOX-detected segments are retained. (If a signaling protocol is configured, it is used before VOX to record the call.) This setting is available when Recorder Control Type is Full time Recording. • Never (Application)—If CTI is disconnected, no audio or screen recording occurs. If CTI is up, CTI segments are retained.
Streaming Media Capture Identifier	<p>This setting contains a Globally Unique Identifier (GUID) that identifies this specific configuration on the Streaming Media Capture interface.</p> <p>The GUID is automatically generated when the member group is created. You can change the GUID during creation, but it is uneditable after the member group is saved.</p>
Participant Configuration	<p>Select one of the following:</p> <p>External Participants: Captures the customer's audio. There must be a member group that captures the external participants.</p> <p>Internal Participants: Optional. Captures the agents on the consultative segment of a customer call.</p>

Setting	Description
Correlation Key	<p> Only required when instructed to do so by Verint support.</p> <p>Create a Correlation Key to use an attribute other than the default (see your Integration Guide for details) to establish an association between a call recording and its CTI attributes.</p> <p>A Correlation Key allows the Integration Service to associate the CTI attributes of a call with the call recording in custom configurations. When a call is received by a data source in a SIP recording environment, the following occurs:</p> <ul style="list-style-type: none"> • CTI attributes are sent from the data source to the Integration Service (to provide the Integration Service with call metadata). • SIP messages are sent from the data source to the Recorder (to set up the call on the Recorder). <p>The Correlation Key associates a CTI attribute with a matching value in a SIP header field. To create a correlation key:</p> <ol style="list-style-type: none"> 1. Click the Add button. 2. From the CTI Attributes drop-down box, select an Attribute. 3. In the Recorder Attribute text box, type the name of a SIP message header that specifies the same value as a CTI Attribute. <p>Example:</p> <p>The following example illustrates the use of a Correlation Key:</p> <ul style="list-style-type: none"> • A data source sends the CTI attribute "SomeID" (a unique identifier of the call) to the Integration Service. <p>For this data source, the equivalent CTI attribute might be mapped to a custom attribute called "SomeID."</p> <ul style="list-style-type: none"> • The data source also sends a SIP request to the Recorder that includes a header called Vendor-SomeID header. This SIP header specifies the same value as the equivalent CTI attribute. <p>In this scenario, to create the Correlation Key, select SomeID as the CTI Attribute, and specify Vendor-SomeID as its associated Recorder Attribute in the text box.</p>

Setting	Description
	<p>Notes:</p> <ul style="list-style-type: none"> • Create multiple Correlation Keys only if there is no single Correlation Key that can accomplish the association of CTI attributes to call recordings for every call. If you specify multiple keys, the order is the order of preference (that is, the system uses the second key only if the first key does not establish a correlation, and so on). • IP Gateway Side recording is the only form of IP recording for which you configure a Correlation Key. All other IP recording configurations use the CTI attribute and the SIP message header that specify the device extension as the common value that ensures that a call's CTI attributes are associated to its recording. With Gateway Side recording, the Recorder cannot identify the device extension in a SIP message header, so the system relies on a different attribute (other than device extension) to make the association. • The correlation keys are required to be unique in the call space. This means that no two (2) independent calls shall have the same correlation value. Related calls may share a correlation value, but are expected to contain identical media for the portion of time they overlap. • The correlation keys are recommended to be unique, non-repeating, and call-specific identifiers. Selecting a correlation key that does not have these qualities can yield undesired results in recording and playback. • Unique means that no two independent calls share the same value at the same time. • Non-repeating means that no two independent calls share the same value ever. • Call specific means that as the call is updated / moved, the identifier updates / moves with the call. • If the correlation value changes, it must do so in the signaling (e.g. SIPREC) and CTI feed simultaneously. • For SIP feeds, the correlation key should come from a SIP header. • For SIPREC feeds, the correlation key should come from the metadata XML. • Customers should minimize the number of correlation keys to be tracked by the system. More keys complicate the configuration, impact performance, and make troubleshooting and support more difficult.
Shared Recorders	Associate one or more IP Recorders to this member group.
Associated Recording Profile	<p>Select one or more recording profiles for this member group.</p> <p>To capture the agent-to-agent parts of a customer call, you can associate multiple recording profiles to the same Streaming Media Capture Pool member group.</p>

Setting	Description
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.

Related information

Configuration, overview, and limitations (*Avaya Experience Platform Integration with Recorder*)

Related topics

[Create and edit member groups and extensions \(page 63\)](#)

[Member groups \(page 441\)](#)

[Create a phone data source \(page 49\)](#)

Stream Recording member group settings

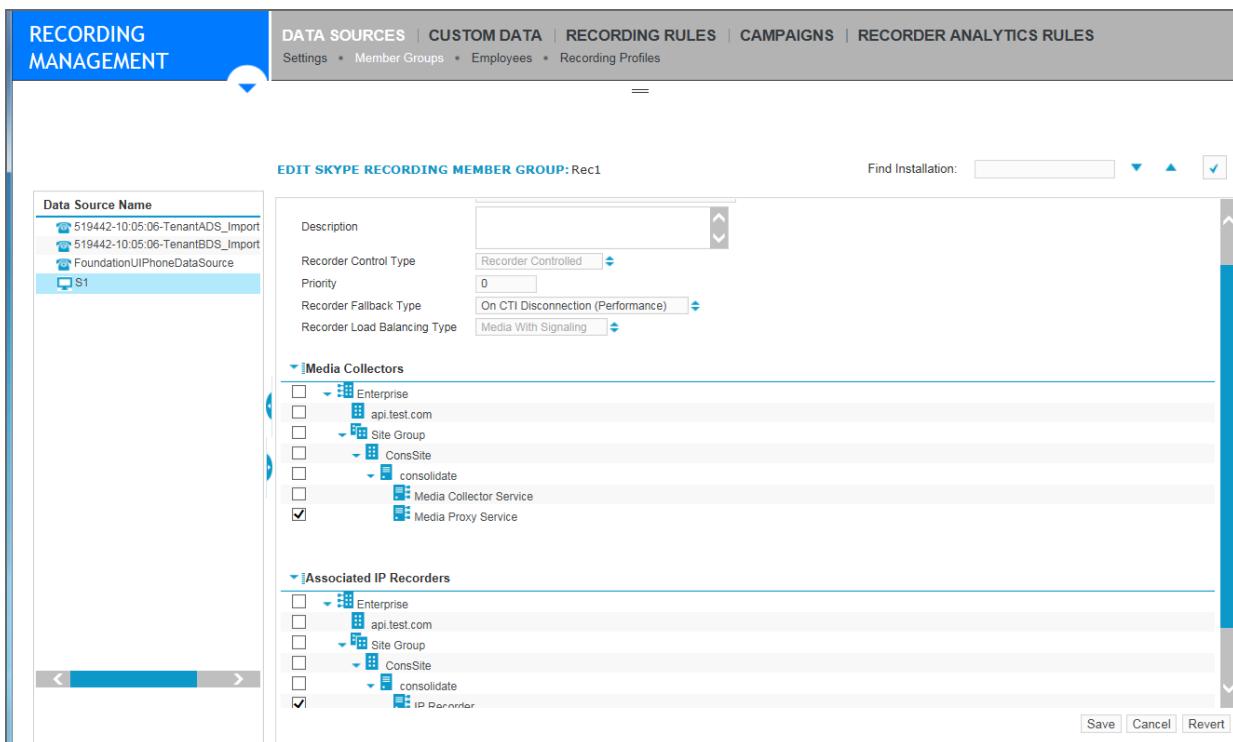
The following settings are available to the Stream Recording member group.

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for this extension group (optional).
Recorder Control Type	<p>Recorder Control Type: The method used to record assigned to a given member group. The following options may be listed for the selected data source:</p> <ul style="list-style-type: none"> • Full Delivery (External Controlled): Recording is controlled by a third-party application, which redirects audio to the recorder. This is the default setting. • Selective Delivery (Duplicate Streamed): The Recorder Integration Service dynamically engages the audio stream in real time based on the CTI feed. <p>For Twilio Flex, only Selective Delivery is available.</p> <p>For Zoom Contact Center, only Full Delivery is available.</p>
Recorder Load Balancing Type	By default, Recorder Load Balancing is set to None and cannot be changed. The Recorder Integration Service balances the call load to the recorders.

Setting	Description
Recorder Fallback Type	<p>Recorder Fallback Type options include:</p> <ul style="list-style-type: none"> • Never (Application)—When CTI is disconnected, neither audio nor the agent screen is recorded. When CTI is connected, CTI segments are retained. When the Recorder Control Type parameter is Selective Delivery (Duplicate Streamed), the fallback type is automatically set to Never and cannot be changed. • On CTI Disconnection (Performance)—When CTI is disconnected, audio recording continues (VOX-detected segments are retained), but agent screen recording stops. When CTI is connected, only the CTI segments that have recorded audio are retained; if we receive CTI for a call but no audio (for any reason), recording does not occur. VOX segments (not associated to CTI calls) will be discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings will be held. When the Recorder Control Type is Full Delivery (External Controlled), the fallback type is automatically set to On CTI Disconnection (Performance). • Always (Liability)—If CTI is disconnected, audio recording continues (VOX-detected segments are retained), but agent screen recording stops. If CTI is connected, both CTI- and VOX- detected segments are retained. When a signalling protocol is configured, it is used before VOX to record the call.
Shared Recorders	Select one or more IP Recorders to associate to this member group.
Shared Recorder Adapter Proxy Service	Select one or more Recorder Adapter Proxy Service (RAPS) server roles to associate to this member group. The RAPS and IP Recorder must be collocated on the same Shared Recorder. A correct association includes the Recorder Adapter Proxy Service + IP Recorder.
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.

Skype Recording member group settings

This member group is used in Skype recording to associate the Media Proxy Service or the Media Collector Service to the IP Recorder.



Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for the member group (optional).
Recorder Control Type	This setting defaults to Recorder Controlled and cannot be changed. <ul style="list-style-type: none"> Recorder Controlled—The Recorder controls recording of the extensions or trunks, and implements the default recording modes. In this case the Integration Service is used for segmentation, stitching, and tagging purposes.
Priority	In most deployments, there is no need to configure the Priority setting and you can accept the default setting of 0. <p>The Priority setting is used for configuring geographical routing for recorders or for supporting load balancing or fail over between recorders. Configure this setting in deployments where Skype servers are located in different physical locations. Provide a higher Priority setting to the Skype servers that are at the local site, and a lower priority to servers at the remote site. The remote servers are used only when all local Media Proxy servers are not available.</p> <p>For more information, see the related topics.</p>

Setting	Description
Recorder Fallback Type	<p>This setting defaults to On CTI Disconnection (Performance). If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, only CTI segments with recorded audio are retained; if we receive CTI for a call but no audio (for any reason), recording will not occur. VOX segments (not associated to CTI calls) will be discarded. You can set a Rollback Period in the Skype data source to specify the length of time preceding a disconnection for which recordings will be held.</p>
Recorder Load Balancing Type	<p>This setting defaults to Media With Signaling and cannot be changed.</p> <ul style="list-style-type: none"> • Media with Signaling—Multiple recorders are used to record the calls. Use only in Recorder Controlled environments where one of the recorders will be aware of the call (that is, call control and media control messages + audio), while other recorders are not aware of this call.
Media Collectors	<p>Select one or more check boxes to associate this member group with the Media Collector Service on an edge server or a Media Proxy Service on a recorder or standalone server. The Media Proxy Service or Media Collector Service forwards the media stream to an associated IP Recorder.</p>
Associated IP Recorders	<p>Select one or more check boxes to associate this member group with an IP Recorder.</p>
Advanced Parameters	<p>Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.</p>

Related topics

[Configuring Media Proxy member groups to support high availability and load balancing \(page 102\)](#)
[Example: Geographical routing and failover with Skype member groups \(page 103\)](#)

Skype Interaction Capture member group settings

Use the Interaction Capture member group to create an association between the Skype Filtering service on a front end server and Interaction Capture server role.

RECORDING MANAGEMENT

DATA SOURCES | CUSTOM DATA | RECORDING RULES | CAMPAIGNS | RECORDER ANALYTICS

Settings • Member Groups • Employees • Recording Profiles

EDIT SKYPE TEXT CAPTURE MEMBER GROUP: TC

Find Installation: ▼ ▲ ✓

Data Source Name	
<input type="checkbox"/>	519442-10-05-06-TenantADS_Import
<input type="checkbox"/>	519442-10-05-06-TenantBDS_Import
<input type="checkbox"/>	FoundationUIPhoneDataSource
<input checked="" type="checkbox"/>	S1

Settings

Name:

Description:

Associated Skype Installations

- Enterprise
 - api.test.com
- Site Group
 - ConsSite
 - consolidate
 - Skype Filtering Service

Associated Text Capture Installations

- Enterprise
 - api.test.com
- Site Group
 - ConsSite
 - consolidate
 - Text Capture

Save Cancel Revert

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for the member group (optional).
Associated Skype Installations	Select one or more check boxes to associate this member group with the Skype Filtering Service on a Skype Front End Server. The Skype Filtering Service gathers information about Skype interactions and distributes it to the Interaction Capture Service.
Associated Interaction Capture Installations	Select one or more check boxes to associate this member group with the Interaction Capture server role on a recorder server.
Advanced Parameters	Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.

Configuring Media Proxy member groups to support high availability and load balancing

You can set up a single Media Proxy service server as a standalone proxy or set up multiple Media Proxy service servers to support load balancing, failover, or geographical routing.

A Media Proxy member group associated with a Skype data source allows the configuration of the following:

- Priority - The priority of a Media Proxy service server.
- Subnet - The endpoint subnets assigned to a Media Proxy service server.

When configuring the Priority or Subnet setting, you can configure Priority only, Subnet only, or both Priority and Subnet.

Configuration example 1 - Three proxies with load balancing

In this configuration, three Media Proxy servers are deployed, each with an associated Media Proxy member group.

In the Priority setting of each member group, either no priority or the same priority for all proxies is configured. (No proxy means Priority 0.) With this configuration, the Skype Filtering service load balances connections to the proxy servers.

Media Proxy member group	Priority Setting
Media Proxy member group 1	0
Media Proxy member group 2	0
Media Proxy member group 3	0

Configuration example 2 - Two proxies with fail over

In this configuration, two Media Proxy servers are deployed, each with an associated Media Proxy member group.

In the Priority setting of each member group, a different Priority level is specified for each of the two member groups. With this configuration, fail over is supported for the two proxies. For more information about using the Priority settings, see the related topics.



The Priority setting is usually used only when you have Skype servers located in different physical locations. For more information about the Priority setting, see the related topics.

Media Proxy member group	Priority Setting
Media Proxy member group 1	2
Media Proxy member group 2	1

Configuration example 3 - Two proxies for manual subnet-based load balancing or for geographical routing

In this configuration, endpoint subnets of the Media Proxy servers are specified in the **Subnets** field of the Media Proxy member group. Specify the endpoint subnets at the proxy connections. You can

specify multiple subnets and separate the multiple entries with a comma.

- i** If you specify multiple proxies with the same subnet configuration, fail over is supported only between the proxies.

Media Proxy member group	Subnets Setting
Media Proxy member group 1	156.125.1.0/24, 156.125.2.0/24
Media Proxy member group 2	12.0.0.0/9

Configuration example 4 - Combining priorities and subnets for geographical routing in large deployments

In this configuration, specify the subnets of the branch sites with higher priority at the branch site proxy connections. Specify the proxy connection of the central site (where most of the users are located and there are plenty of subnets) with a lower Priority setting, without subnets.

- i** If subnet filtering is used with a specific priority, then subnet filtering with the same priority must be used at the other proxy connections.

Media Proxy member group	Subnets and Priority Settings
Media Proxy member group 1	Subnets: 156.125.1.0/24, 156.125.2.0/24 Priority: 2
Media Proxy member group 2	Subnets: 156.125.3.0/24, 156.125.4.0/24 Priority: 2
Media Proxy member group 3	Subnets: Priority: 1

Related topics

[Example: Geographical routing and failover with Skype member groups \(page 103\)](#)

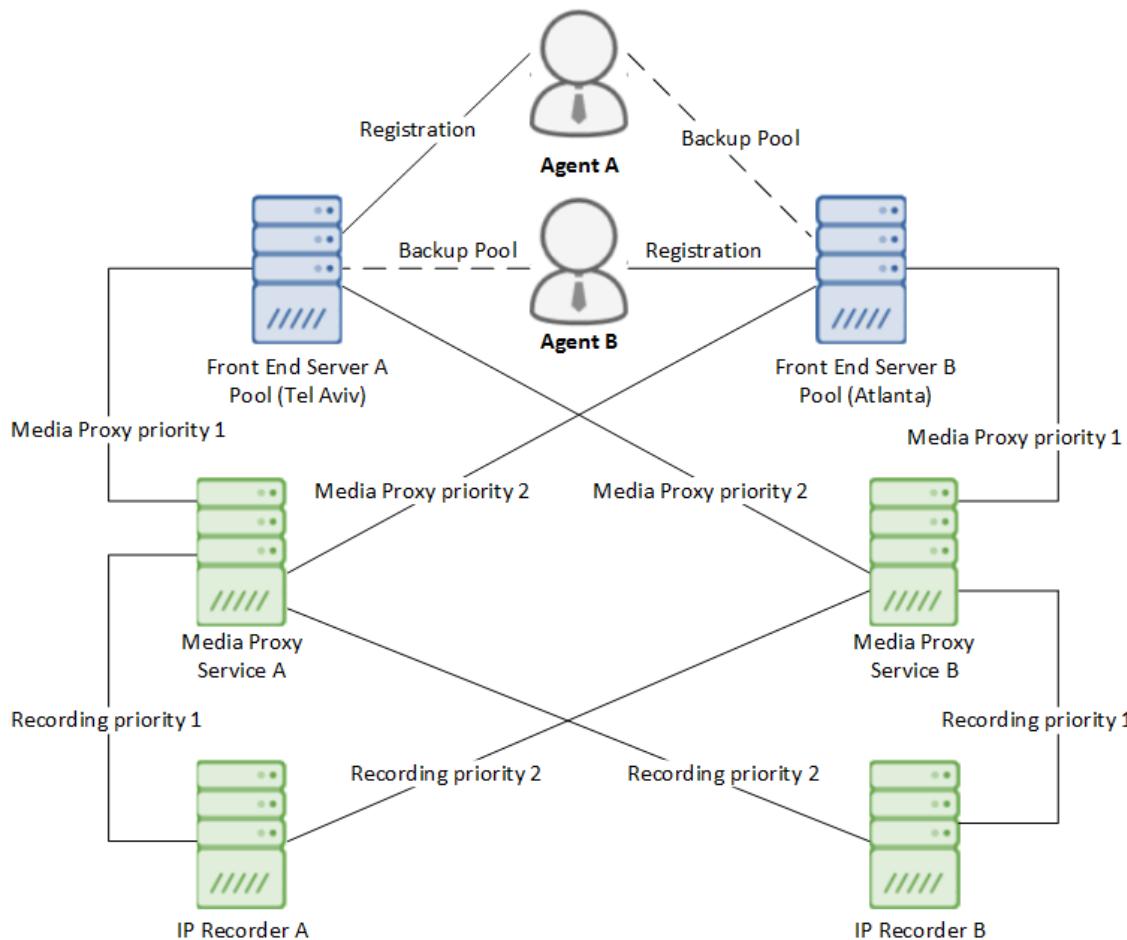
Example: Geographical routing and failover with Skype member groups

This example illustrates how you can use the Priority setting in the Skype Media Proxy and Recording member groups to configure geographical routing and failover in a Skype recording environment.

The Skype Filtering Service on the Skype front end servers uses the configured Subnets and Priority settings of the Media Proxy member groups to decide which Media Proxy service should be selected for each Skype call.

Having Priority configuration under both Recording member groups and Media Proxy member groups provides fall back and primary and secondary server selection for each component involved in recording of Skype calls.

The example diagram below shows two pools of Skype front end servers with each pool deployed in a different geographical location.



During normal operation, agents from Site A connect to the front end servers in Tel Aviv and agents from Site B connect to the front end servers in Atlanta. If for some reason, the servers in Tel Aviv become unreachable, agents from Tel Aviv can fall back to the servers in Atlanta. Similarly, if for some reason the servers in Atlanta become unreachable, the agents from Atlanta can fall back to the servers in Tel Aviv.

In this example, the customer requirement is to record agents using the local recorder. If the local recorder or local Member Proxy service is unavailable, calls should be recorded using any other recorder or routed through any other proxy service.

To support the customer requirement, the following Skype data source and member group configuration is required.

1. All agents must be associated to the same Skype data source.
2. Media Proxy member group 1 is created and associated to front end server A and Media Proxy service A. This member group is assigned **Priority 1**.
3. Media Proxy member group 2 is created and associated to front end server B and Media Proxy service B. This member group is assigned **Priority 1**.
4. Media Proxy member group 3 is created and associated to front end server A and Media Proxy service B. This member group is assigned **Priority 2**.

5. Media Proxy member group 4 is created and associated to front end server B and Media Proxy service A. This member group is assigned **Priority 2**.
6. Recording member group 1 is created and associated to Media Proxy service A and IP Recorder A. This member group is assigned **Priority 1**.
7. Recording member group 2 is created and associated to Media Proxy service B and IP Recorder B. This member group is assigned **Priority 1**.
8. Recording member group 3 is created and associated to Media Proxy service A and IP Recorder B. This member group is assigned **Priority 2**.
9. Recording member group 4 is created and assigned to Media Proxy service B and IP Recorder A. This member group is assigned **Priority 2**.

In this example, eight member groups are necessary to achieve full fall back between each of the components on two remote sites under the same data center.

Set up screen recording

You can configure recording of both screens and audio, or screen-only recording. For screens and audio, you will create both Phone and LAN data sources, and map the phones/extensions to workstations in the LAN. For screen-only recording you only need to create the LAN data source, without associating it to any phone extensions.



Employees being monitored using screen recording must only log into one machine at a time. Ensure that employees log out of their Windows sessions before initiating a separate session on a different machine.

Complete the following tasks to set up screen recording.

- Install the Screen Capture module on each desktop to capture, as described in the *Desktop Applications Deployment Reference and Installation Guide*.
- Associate a Recorder with the Integration Service ([page 46](#))
- Create a phone data source ([page 49](#))
- Create a LAN data source ([page 107](#)) (only required to record both screens and audio)
- Set up workstations and workstation groups ([page 109](#))
- Create employees and add employee IDs ([page 143](#))
- Map employees to data sources ([page 145](#))
- Set up recording rules ([page 303](#))



To use screen recording with audio recording you must associate phones and extensions with workstations, or LAN employee IDs with phone employee IDs in the Employee Mapping section under **Recording Management > Data Sources > Employee**. See [Map employees to data sources \(page 145\)](#).



No special configuration is required for recording screens with SIP Trunk Recording.

Related topics

[Workflow: Screen recording \(page 38\)](#)

Create a LAN data source

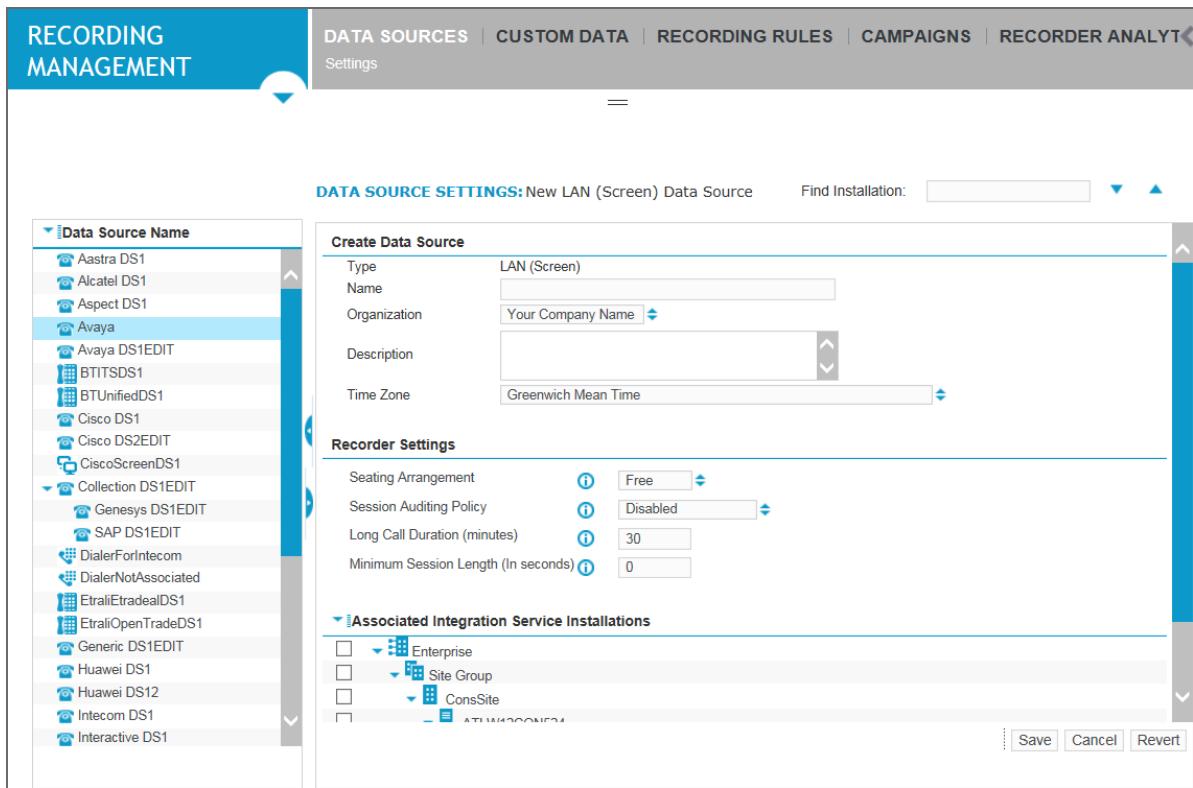
Use the following procedure to create a LAN data source for screen recording.

Workflow sequence

[Workflow: Screen recording \(page 38\)](#): Task 2 of 7

Procedure

1. Click **Recording Management**.
2. Under **Data Sources**, click **Settings > Data Sources**.
3. Click **Create Data Source**.
4. In the **Data Source Type** dialog box, select **LAN (Screen)**, then click **Select**.



The data source types available to you depend on licensing.

5. Type a **Name** and a **Description** for the data source (the description is optional).
6. Select a **Time Zone** from the dropdown list. The recorder relies on the time zone for recording start and end times.
7. Under Recorder Settings, select one of the following under **Seating Arrangement**:

- **Free** seating, the default, indicates that employees do not have permanently-assigned workstations. They are assigned an Employee ID and can log in from any location in the call center. Extensions are assigned dynamically when the employee logs in.
 - **Fixed** seating indicates that an employee has a permanently assigned workstation and is associated with a specific extension.
 - **Hybrid** seating refers to a mixed arrangement that contains both Free and Fixed seating for employees.
8. **Session Auditing Policy**—Defines the type of session/interaction that should be marked and kept in the system. "Disabled" (the default) will only mark sessions/interactions with some kind of content. Two additional options will create a basic entry in the database for sessions/interactions that occurred but were not recorded: "Missed Recordings" will mark sessions/interactions that should have been recorded, but were not, while "Full Switch" will mark all sessions/interactions for which we receive CTI without recording (for example, sessions/interactions that were blocked). You may then search for these types of interactions in the Portal. The Recorder Integration Service will select a viable recorder associated with any device within the Session workspace to audit the interaction. If no viable recorder could be located at the time of the audit, the audit will be lost.
- i** Recorded employee segments marked through auditing will appear in playback once all Sessions/Interactions in the related Contact are closed, after a delay of up to five minutes.
9. **Long Call Duration** - This setting allows you to specify the length of a screen recording, in minutes, after which the system will trigger an alarm. Enter any number between 1 and 1440 (24 hours)—an alarm is raised in the cases where screen recordings exceed this number of minutes. The default is 120.
- i** The Integration Service runs maintenance checks every five minutes to close screen recordings that last for more than the length of time specified as the **Long Call Duration**. An alarm will indicate that a call was closed because it was too long. These maintenance checks are not run more frequently in order to avoid imposing an additional load on the system. Therefore it may take up to five minutes to close a long screen recording after it has passed the defined **Long Call Duration** threshold.
10. To prevent the retention of very short screen recordings, specify a **Minimum Session Length (seconds)**. Active calls (from connected to closed) that are shorter than the specified value will be deleted automatically. If set to zero (0), this feature is disabled and no calls will be deleted based on this setting. The maximum value is 3600 (or one hour). This setting applies to the active duration of CTI Sessions or the entire duration of VOX Sessions. Inactive CTI Sessions can be retained using the Session Auditing Policy.
11. In the **Default Employee** section, specify the employee to be associated to a recording that has no employee associated to it.

There are situations where recordings do not have employees associated to them. Examples include:

- IVR recordings where there is no employee or phone device
 - Back office environments where phones are shared and not associated to a specific employee
- Assigning a **Default Employee for Interactions** to a data source provides a way to provide replay access to recordings that do not include a specific employee. When a **Default Employee for**

Interactions is assigned to a data source, any recording that is not assigned to a specific employee will be associated to the **Default Employee for Interactions**.

To capture recordings for a default employee, select the **Organization** to which the **Default Employee for Interactions** belongs, and then select one employee as the **Default Employee for Interactions**.

The default employee must not have a configured end date. Also, do not select an employee who will soon move or transfer to a different organization.

Once an employee is selected as the **Default Employee for Interactions**, an error message is displayed on the data source screen if the employee has been deleted, terminated, or changed to a different organization since the last time the data source was saved.

12. Under **Associated Integration Service Installations**, select the server that is providing Integration Services for this recorder, if applicable.
13. Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system. This should only be done in consultation with Field Engineers.
14. Click **Save**.

What do to next

Screen recording: [Set up workstations and workstation groups \(page 109\)](#)

Set up workstations and workstation groups

To use screen recording, you must define the workstations on which you want to record activity. Each is part of the LAN data source. You can create either dynamic or static workstations.

- Dynamic workstations: Contacts can be recorded by any available employee. Employee workstations are not tied to employee IDs. Dynamic workstations are recommended and configured for most deployments.
- Static workstations: Referred to as fixed workstations in Enterprise Manager, static workstations are used in rare, specific cases.

You can define the nodes on which screens are to be recorded as either workstations or as part of a subnet. Workstations can be identified either by host name or IP address, while those stations that are part of a subnet are identified by IP address.

Use the following procedures to set up workstations for screen recording:

- [Create workstation groups \(page 110\)](#)
[Define workstations \(page 112\)](#)
- *or* [Create subnets \(page 114\)](#)
- [Create a workstation group and assign workstations \(page 113\)](#)
- [Unassign workstations \(page 114\)](#)

i The associations established between workstations, extensions, and employee are described in detail under [Static/Dynamic Workspaces \(page 455\)](#) and [Static/Dynamic Workstations \(page 455\)](#).

Create workstation groups

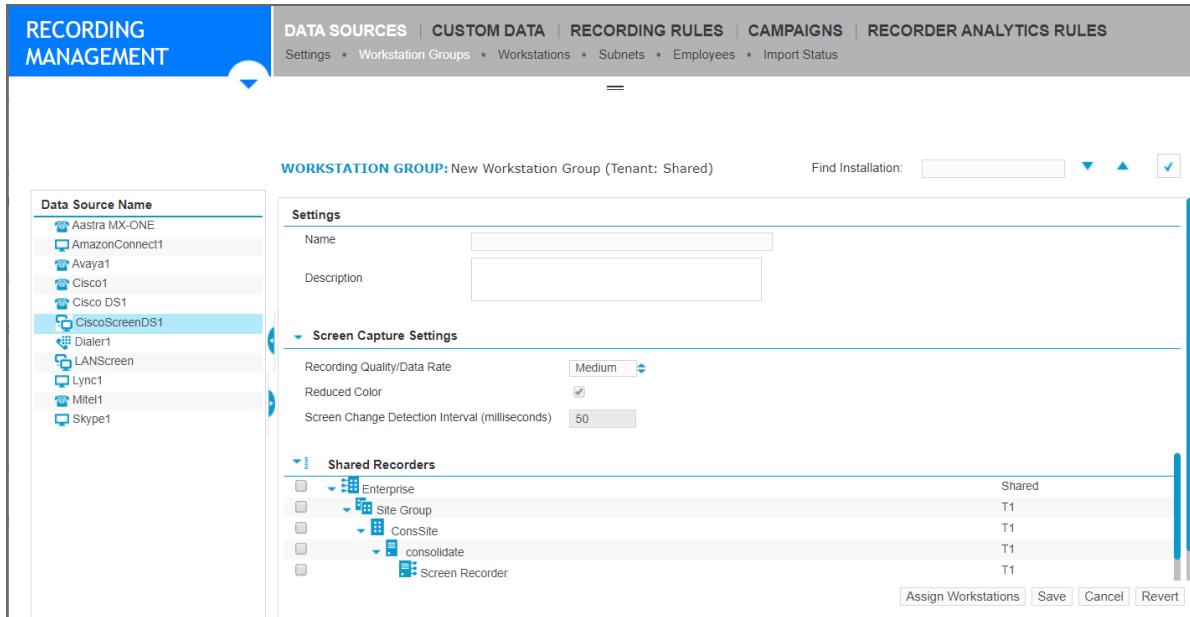
Workstation groups define the pools of screen recorders to use for an assigned node (static or dynamic workstation). For recording to work, each LAN data source must have at least one (1) workstation group.

If all screen recorder servers reside in a single data center, then only one (1) workstation group is needed.

If the screen recorder servers are spread across multiple data centers, a customer can create multiple workstation groups to represent each data center site. To optimize the network path for recording, customers can use workstation groups to direct a specific node to a specific pool.

Procedure

1. Click **Recording Management > Data Sources > Settings**, then select a LAN data source.
2. Click **Workstation Groups**, then click **Create**.



In a multi-tenant enabled environment, the tenant to which the selected data source is associated displays in parentheses in the screen heading. An organization belongs to a tenant. When a data source is associated to an organization, the screen heading displays the tenant to which the organization belongs. The data source can be associated to a particular tenant or have the **Shared** status. A data source associated to a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

3. Type a **Name** and a **Description** for the Workstation Group (the description is optional).
4. Specify the **Screen Capture Settings**:

- **Recording Quality/Data Rate** — Select the recording quality from the drop-down list: High, Medium, Low, or Custom. The lower the setting, the higher the compression and the smaller the file size is. To enable the Reduced Color option, select Custom.
 - **Reduced Color** — Availability of this option depends on the **Recording Quality**.
 - **Screen Change Detection Interval (milliseconds)** — Type a value, in milliseconds, representing the change detection rate in milliseconds. The minimum value is 50 and the maximum is 1000. This option is only available if the **Recording Quality/Data Rate** is set to **Custom**.
5. Under **Shared Recorders**, select one or more recorder installations with which you want to associate the workstation.
 6. Click **Save**.

What to do next

[Define workstations \(page 112\)](#)

Define workstations

You can define the stations to be recorded either as static Workstations or as part of a subnet (described in the next procedure).

Procedure

1. Click **Recording Management > Data Sources > Settings**, then select a LAN data source.
2. Click **Workstations**, then click **Create**.

In a multi-tenant enabled environment, the tenant to which the selected data source is associated displays in parentheses in the screen heading. An organization belongs to a tenant. When a data source is associated to an organization, the screen heading displays the tenant to which the organization belongs. The data source can be associated to a particular tenant or have the **Shared** status. A data source associated to a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

3. Type a **Host Name** and a **Description** for the Workstation (the description is optional).
4. Specify the following information:
 - **Platform**—This is the platform or operating system for this workstation. Select **Windows, OS/2, or Windows Terminal Server**. If you select Windows Terminal server, Phone data source and Extension are disabled.
 - **Workstation Group**—Select the Workstation Group created above. A workstation can belong to only one workstation group.
 - **Phone Data Source**—Select the Phone data source if you are creating static workspace by assigning the workstation to Extension.



In a multi-tenant enabled environment, only Phone data sources associated to the same tenant as the LAN data source selected earlier in this procedure are available for selection.

- **Extension**—Click the pencil button to specify the TDM or IP telephone extension associated with this workstation. This applies only if you are creating static workspaces.



You can only have one workstation associated with an extension.

5. Click **Save**.

Create a workstation group and assign workstations

Procedure

1. Complete the following fields:
 - **Platform**—This is the platform or operating system for this workstation. Select **Windows, OS/2**, or **Windows Terminal Server**. If you select Windows Terminal server, Phone Data Source and Extension are disabled.
 - **Phone Data Source**—Select the Phone data source if you are creating static workspace by assigning the workstation to Extension.
 - **Extension**—Click the pencil button to specify the TDM or IP telephone extension associated with this workstation. This applies only if you are creating static workspaces.
2. Click **Assign**.

Assign workstations to workstation groups

Before you begin

Create workstations and workstation groups.

Procedure

1. Select one or more workstations to assign to this workstations group.
2. Click **Assign Selected**.

Unassign workstations

Unassign Workstations in a Workstation Group to detach Workstation host names and platforms from the current group. Workstation Groups are groups of Workstations that share the same screen recording characteristics. When you unassign Workstations, you release these screen recording characteristics.

Procedure

1. Click **Recording Management > Data Sources > Settings**, and select a LAN data source.
2. Click **Workstation Groups**, select one or more workstations, then click **Unassign Workstations**.
3. Click **Save**.

Create subnets

You can define the stations to be recorded either as part of a subnet (a range of IP addresses denoting the network segment that includes the stations) or as static workstations.

To represent a connecting client node without a configured static workstation, the recording site attempts to create a dynamic workstation.

The recording site looks for a configured subnet that matches one (1) of the IP addresses reported by the client node:

- If a matching subnet is not found, a dynamic workstation is not created within the recording site.
- If the client node matches to multiple subnets, the subnet with the highest degree of specificity is selected.

The size of the subnet mask determines specificity. Avoid creating overlapping subnet configurations where a single IP address could potentially match to multiple configured subnets.

Subnet matching is primarily useful for selecting the workstation group to use for recording. To minimize the complexity of the configuration, only define enough subnets to differentiate between multiple workstation groups. If a single workstation group is defined, then a single subnet can be used to capture all client nodes to that group.



For more information on configuring subnets and masks, see [Subnets and subnet masks \(page 464\)](#).

Procedure

1. Click **Recording Management > Data Sources > Settings**, then select a LAN data source.
2. Click **Subnets**, then click **Create**.

In a multi-tenant enabled environment, the tenant to which the selected data source is associated displays in parentheses in the screen heading. An organization belongs to a tenant. When a data source is associated to an organization, the screen heading displays the tenant to which the organization belongs. The data source can be associated to a particular tenant or have the

Shared status. A data source associated to a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

- a. Select a **Workstation Group** from the drop-down list.
- b. Type an IP address in the **Network Address** field, for example, 10.100.104.0, and a **Subnet Mask**, for example, 255.255.255.0.

This option requires that the NT Logon be associated with a **Person**.

Workstations whose IP address matches the subnet IP address range are categorized as the dynamic workstations. To record dynamic workstations, you must assign the Windows Logon ID to an employee and assign the phone extension or phone logon ID to the employee to build the workspace dynamically.

3. Click **Save & Close**.

What to do next

[Create a workstation group and assign workstations \(page 113\)](#)

Related topics

[Subnets and subnet masks \(page 464\)](#)

Set up a dialer integration

When employees login to dialers, typically a call is placed from the dialer to the employee through the PBX, and a connection is established and maintained for their entire dialer login session. This call is typically called a “nailup call.” In trunk side recording deployments it is necessary to tap the trunks that are between the dialer and the PBXs that are used to establish these nailup calls, in order to record the voice for dialer calls.

You can configure this by creating a Phone Data Source with a Trunk Side Member Group for the dialer trunks. Usually these trunks are set up by the PBX administrator with either Trunk IDs or with Extension IDs, so the member group “Type” field should be set accordingly. In the Member Group you should configure either the Extensions or Trunk IDs for the trunks between a dialer and the PBX that are being used for nailup calls. In addition, you must select the Dialer Data Source that defines the dialer to which the trunks are connected.

The steps to set up a dialer integration are as follows:

- [Create a dialer data source \(page 116\)](#)
- [Create and edit phones for dialers \(page 123\)](#)
- [Create member groups for dialers \(page 123\) \(necessary for trunk-side only\)](#)

What to do next

[Create a dialer data source \(page 116\)](#)

Related topics

[Workflow: Integrate Dialer integration \(page 39\)](#)

Create a dialer data source

Use the following procedure to create a dialer data source.

Workflow sequence

[Workflow: Integrate Dialer integration \(page 39\)](#): Task 3 of 7

Before you begin

Unless you are using a standalone dialer deployment, you should create a phone data source before you begin. See [Create a phone data source \(page 49\)](#), and [Phone Data Sources for Dialer Integrations \(page 428\)](#).

Procedure

1. Go to **Recording Management**. Under **Data Sources**, select **Settings**.
2. Select **Create Data Source**.
3. In the **Data Source Type** dialog box, select **Dialer**, and a **Switch/Sub Type**, then click **Select**.



The data source types available to you are dependent on licensing.

4. Type a **Name** and a **Description** for the data source (the description is optional).
5. Under **Recorder Settings**:
 - a. Specify a **Seating Arrangement**—Fixed, Free, or Hybrid.
 - **Free** seating, the default, indicates that employees do not have permanently-assigned workstations. They are assigned an Employee ID and can log in from any location in the call center. Extensions are assigned dynamically when the employee logs in.
 - **Fixed** seating indicates that an employee has a permanently assigned workstation and is associated with a specific extension.
 - **Hybrid** seating refers to a mixed arrangement that contains both Free and Fixed seating for employees.
 - b. In a multi-tenant enabled (cloud) environment, if the Seating Arrangement is Fixed or Hybrid, the Service Provider Administrator (SPA) can specify a **Maximum Allowed Extensions** value for this data source. The Maximum Allowed Extensions setting limits the number of extensions a Tenant Administrator can create for the data source. This setting allows a SPA to prevent tenants from creating more extensions than their assigned capture capacity supports.

If this setting is not set and the data source currently has no extensions associated with it, this setting defaults to 1000 at the time a Tenant Administrator creates the first extension.

In an upgrade scenario, a data source may already have extensions assigned to it. In this scenario, when a Tenant Administrator adds extensions, the system updates this setting to 120% of the existing number of extensions or 1000, whichever is higher. For example, if 2000 extensions are associated with the data source at the time of the upgrade, this setting defaults to 2400 when a Tenant Administrator adds extensions.

This setting does not limit the number of extensions a SPA can create. For example, if the setting is 1000, a SPA can create more than 1000 extensions. If the SPA creates more extensions than this setting specifies, the Tenant Administrator cannot create any extensions.

If a Tenant Administrator configures the maximum number of allowed extensions, the SPA can increase this number to allow the Tenant Administrator to create additional extensions.

Before increasing this setting, the SPA should verify that the tenant's environment has the resources necessary to handle the increased load.
 - c. To save the last employee's status after the computer is shut down, select the Persist Agent State on Shut Down check box.

Specify the amount of time in minutes for which you want to save the employee's data. The default is 600 minutes (10 hours). Data from within this time period will not be loaded, (while data from after this duration has passed will be).

Note that if the CTI adapter is down,

 - If unselected, all employees on the data source are logged out right away.
 - If selected, all employees on the data source are logged out once the persistence period has elapsed.
 - d. To prevent the retention of very short calls, specify a **Minimum Session Length (seconds)**. Active calls (from connected to closed) that are shorter than the specified value will be deleted automatically. If set to zero (0), this feature is disabled and no calls will be deleted based on this setting. The maximum value is 3600 (or one hour). This setting applies to the active duration of

CTI Sessions or the entire duration of VOX Sessions. Inactive CTI Sessions can be retained using the Session Auditing Policy.

- e. Enable the **Rollback Period (minutes)** to ensure that a recording is kept for a certain amount of time before deletion, so that in the event of a disconnection it is possible to retrieve it. A rollback period is applicable only to Performance Mode (set in the IP Extension Pool member group) and N+N redundancy. The default value is 15, and the maximum value is 60.
- f. RTP detection is enabled in Performance and Liability fallback modes to prevent audio loss. Coordination between the Integration Service and RTP, using the following settings, ensures that there will only be one recording for a given call:
 - **Start Overlay (milliseconds)**—This threshold indicates the longest amount of audio (from before CTI starts) that will be associated to that CTI call. Anything over this threshold will be treated as VOX.
 - **End Overlay (milliseconds)**—This threshold indicates the longest amount of audio (after CTI ends) that will be associated to that CTI call. Anything over this threshold will be treated as VOX.
- g. **Long Call Duration (minutes)**—This setting allows you to specify the length of a call, in minutes, after which the system will trigger an alarm. The system will also stop tracking the call from a CTI perspective, so in CTI-controlled application or performance mode environments this may cause loss of recording. Enter any number between 1 and 1440 (24 hours)—an alarm is raised in the cases where calls exceed this number of minutes. The default is 120.



The Integration Service runs maintenance checks every five minutes to close calls that last for more than the length of time specified as the **Long Call Duration**. An alarm will indicate that a call was closed because it was too long. These maintenance checks are not run more frequently in order to avoid imposing an additional load on the system. Therefore it may take up to five minutes to close a long call after it has passed the defined **Long Call Duration** threshold.

- h. **Long Hold Duration (minutes)**—Indicates the maximum duration of a single hold. Any holds over this duration will raise an alarm. Enter any number between 1 and 3000, representing the number of minutes. The default is 30.
- i. **Recording Resource Allocation Behavior**—This setting is for duplicate streaming solutions, which allow you to distribute recordings across multiple recorders.
 - **IgnoreLine**—Records the next recording on the least-utilized recorder connected to the Integration Service, regardless of data source, member group, and extension list settings.
 - **LineFirst**—First attempts to record on the least-utilized recorder that contains the extension being recorded in a member group associated with the recorder. If the Integration Service can't find an associated recorder it will attempt to find any connected recorder with the capacity (whether or not the extension is associated with the recorder). LineFirst provides a way to keep recorders local to the extensions/site. The Integration Service will fail over to another set of recorders if a call can't be recorded locally. If you don't want fail over to another set of recorders, use 'LineExclusive', described below. This is the default.

- **LineExclusive**—First attempts to allocate the recording to the least-utilized recorder that contains the extension being recorded in a member group associated to the recorder. If the Integration Service fails to find a recorder associated with the line to be recorded, it will not record the call.

The "least-utilized" recorder is the one with the most unused capacity. For example, if one recorder has 300 licenses and 50 calls are currently being recorded, and another recorder has 100 licenses and 10 calls currently being recorded, the capacity left on the recorders are 250 and 90 respectively. The system will attempt to record the next duplicate streamed call on the first recorder.

- j. **Always Report Extension as Primary Extension**—If enabled, the extension field of the interaction will always be the primary extension on a telephone. If disabled, the extension field will contain the DN/extension that first answered the call. This only affects multiline phones. Enabled by default.
- k. **Contact Policy Type**—This setting allows you to set the call stitching method.
 - **Follow the call**—When follow the call is enabled, there will be one contact that includes all audio from the beginning of the call to the end. This is the default.
 - **Backoffice - Contact per call**—Enables the "Back office" style of stitching, which creates sessions/interactions based on CTI calls. If one employee is on two calls at the same time (for example, a customer call and a consultation call), the system creates two sessions/interactions. This is used more often in trading environments rather than contact center environments.
- l. **Record Extensions for Internal Calls**—This setting applies to trunk side environments (such as the Avaya switch in trunk-side environment), and hybrid systems where the same data source is used for TDM recording and IP recording (one data source and two member groups). Select this check box to allow the recording of internal calls on selective recording resources.
- m. **Raise Alarm for Out Of Service Devices**—If enabled, the Integration Service will raise alarms for any devices that go out of service. This is currently only available for Cisco JTAPI and Genesys adapters.
- n. **Alarm - Device Not Recorded Call Count**—The number of calls for a configured device that must fail to record before triggering the DeviceNotRecording alarm. The default is 1.
- o. **Alarm - Device Not Recorded Duration (milliseconds)**—Failed call durations under this threshold will not count against the Device Not Recorded Call Count. The default is 15 seconds.
- p. **Enable Nailup Algorithm**—This setting is selected by default, and is used by the Integration Service to identify nailup calls (otherwise, manual configuration of dialer trunks may be required).
- q. **Session Auditing Policy**—Defines the type of session/interaction that should be marked and kept in the system. "Disabled" (the default) will only mark sessions/interactions with some kind of content. Two additional options will create a basic entry in the database for calls that occurred but were not recorded: "Missed Recordings" will mark calls that should have been recorded, but were not, while "Full Switch" will mark all sessions/interactions for which we receive CTI without recording (for example, calls that were blocked, or interception calls that were met with a busy tone or unanswered ringtone). You may then search for these types of interactions in the Portal. The Recorder Integration Service will select a viable recorder

associated with any device within the Session workspace to audit the interaction. If no viable recorder could be located at the time of the audit, the audit will be lost.



Recorded employee segments marked through auditing will appear in playback once all interactions in the related Contact are closed, after a delay of up to five minutes.

- r. **Recorder Allocation Based On Audio Location**—Use this setting in a SIP-based VoIP delivery environment to control how Recorders are selected to record calls, and ensure that each call is recorded by a Recorder local to the media gateway at which the call arrives. This setting is designed primarily for environments where recording occurs at multiple sites and each site has its own gateway.

Note that this setting must be used in conjunction with either a Gateway Side Correlation Pool member group or an IP Extension Pool member group configured for the data source. Within these member groups, you must specify the IP addresses or host names of the phones associated with the member group in the IP Network Region configuration.

The Recorder Allocation Based on Audio Location setting instructs the system to examine the IP address in a SIP message and compare this address to the addresses listed in the IP Network Region settings of the Gateway Side Correlation Pool or IP Extension Pool member group associated with the data source.

If an address in the SIP message matches one of those specified in the member group IP Network Region settings, the system will route the call to a Recorder associated with that member group.

The options for this setting are:

- **Inactive**—The system attempts to record the call, but does not use an address found in a SIP message to route the call to a particular Recorder. This is the default setting.
- **From Signaling**—The system examines the SIP header section of the SIP Invite. The system compares the address found in a SIP header field (such as From, Contact, Via, or Socket) to the addresses configured in the member group IP Network Region settings. If there is a match, the system routes the call to a Recorder associated with that member group. If the system does not find a match, the **Recording Resource Allocation Behavior** setting will determine how the call is recorded.
- **From Media**—The system examines the SDP message attached to a SIP Invite. The system compares the IP addresses found in the SDP message to those configured in the member group IP Network Region settings. If there is a match, it routes the call to a Recorder associated with that member group. If the system does not find a match, the **Recording Resource Allocation Behavior** setting determines how the call is recorded. This option does not work if SIP operates in Delayed-Offer mode.

Note that this setting works in combination with the **Recording Resource Allocation Behavior** setting to determine recording behavior. If the **Recording Resource Allocation Behavior** setting specifies:

- **IgnoreLine**—The system acts as if the Inactive setting is selected for this setting. If either the From Signaling or From Media is selected, those settings are ignored. In this case, any Recorder associated with the data source can record the call.
 - **LineFirst**—The system makes two attempts to record the call using the address obtained from the SIP message. If the system cannot successfully route the call to a Recorder using the SIP message address, any Recorder associated with the data source can record the call.
 - **LineExclusive**—If the system cannot successfully route the call to a Recorder using the address from the SIP message, the call is not recorded. In this case, the system raises an alarm.
- s. **Video Recording Mode** - Choose one of the following video recording modes:
- **Start On Trigger** - Do not record video calls for the extensions associated with this data source until a recording rule is triggered or an external API command starts recording. If the recorder is set to recorder controlled, recording starts whenever the call starts, but video prior to the recording trigger is deleted.
 - **Application Controlled** - Record every video call for every extension associated with this data source, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the video call. If the call is kept, the recording includes all video from the start of the call to the end.
 - **Do Not Record** - Do not record video calls for extensions associated with this data source. Recording rules are ignored and cannot trigger the recording of calls.
 - **Record** - Record all video calls for all extensions associated with this data source. Only a block recording rule, AIM command, or external API command can prevent calls from being recorded.
- t. **Require Replay Audio Redaction** - When redaction is enabled for the system, select whether redaction occurs for interactions that the data source captures. Redaction obscures sensitive customer information in captured audio and transcriptions. Select from the following for interactions that the data source captures:
- **Disabled**: No information in the interaction is obscured. *Disabled* is the default setting.
 - **Always**: Sensitive customer information is obscured.
 - **In Fallback**: Sensitive customer information is obscured, but only in the event of CTI or recorder disconnection from the Integration Service.
- u. **Require Replay Audio Morphing** - When morphing is enabled for the system, select whether replay of interactions captured by the data source requires morphing. Morphing changes the voice heard during replay such that the speaker remains anonymous and the audio remains intelligible. Select from the following options for interactions that the data source captures:
- **Disabled**: The original voice of the agent and the customer are heard during interaction replay. *Disabled* is the default setting.
 - **Always**: The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting.

- **In Fallback:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting, but only in the event of CTI or recorder disconnection from the Integration Service.
- v. **Audio Morphing Channel** - Enabled when **Require Replay Audio Morphing** is set to **Always** or **In Fallback**, choose the audio channel or channels that use morphing. Select from:
- **Agent:** Only the voice of the agent channel is morphed during interaction replay. The voice on the customer channel is the original captured voice. *Agent* is the default setting.
 - **Agent and Customer:** The voice of the agent channel and the customer channel are morphed during interaction replay.
6. Under **Associated Phone Data Sources**, click **Add** to associate the PBX/ACD in use in your system (that is, the phone data source you created earlier—if you are using a standalone dialer you can skip this step) with the dialer data source.
- a. Select the **Phone Data Source**.
 - b. Specify a **Dial Code**, **Discard Digits**, and **New Prefix**. These fields define the transformation of the dialer extensions into ACD extensions. For example, if the dialer extension is 551234, and the ACD is 81234, enter "55" as the Dial Code, "2" under Discard Digits (that is, the total number of digits to be discarded), and the Prefix, "8". In this example, any 55xxxx, would translate to 8xxxx.
- You can associate multiple phone data sources with the dialer data source. It is important to note that the combination of the phone extension plus the dialer code must be unique. (For example, if the dialer codes are 21 and 211, and the associated extensions are 12 and 2 respectively, this creates a conflict.)
7. In the **Default Employee** section, specify the employee to be associated to a recording that has no employee associated to it.
- There are situations where recordings do not have employees associated to them. Examples include:
- IVR recordings where there is no employee or phone device
 - Back office environments where phones are shared and not associated to a specific employee
- Assigning a **Default Employee for Interactions** to a data source provides a way to provide replay access to recordings that do not include a specific employee. When a **Default Employee for Interactions** is assigned to a data source, any recording that is not assigned to a specific employee will be associated to the **Default Employee for Interactions**.
- To capture recordings for a default employee, select the **Organization** to which the **Default Employee for Interactions** belongs, and then select one employee as the **Default Employee for Interactions**.
- The default employee must not have a configured end date. Also, do not select an employee who will soon move or transfer to a different organization.
- Once an employee is selected as the **Default Employee for Interactions**, an error message is displayed on the data source screen if the employee has been deleted, terminated, or changed to a different organization since the last time the data source was saved.
8. If applicable, expand the **Associated Integration Service Installations** area and select the server that is providing Integration Services for the recorder for which you are configuring this data source.

9. Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system. This should only be done in consultation with Field Engineers.
10. Click **Save**.

What to do next

Dialer integration: [Create employees and add employee IDs \(page 143\)](#)

Create and edit phones for dialers

If you are using a standalone dialer deployment, create phones/extensions for the dialer data source; otherwise (and in most cases) you must create the phones/extensions on the phone data source. In both cases, see [Create and edit member groups and extensions \(page 63\)](#).

Create member groups for dialers

Procedure

1. Select a dialer data source.
2. Click **Member Groups**, then click **Create**.
3. Select one of the following:
 - Compliance Station Extension Group—proceed to [Compliance station extension member group settings for TDM \(page 67\)](#).
 - Compliance Trunk Span—proceed to [Compliance trunk span member group settings for TDM \(page 68\)](#).
 - IP Extension Pool—proceed to [IP extension pool member group settings \(page 71\)](#).

Set up phones and extensions

Setting up phones and extensions includes these tasks.

Tasks

- [Create and edit phones/extensions \(page 125\)](#)
- [Set a default recording mode \(page 129\)](#)
- [Map workstations to phones \(page 130\)](#)
- [Edit multiple extensions \(page 130\)](#)
- [Create a range of extensions \(page 131\)](#)
- [Generate extension numbers or trunk group members \(page 133\)](#)
- [Delete extensions \(page 134\)](#)
- [Assign a range of IP extensions \(page 134\)](#)
- [Edit IP extensions \(page 136\)](#)
- [Batch edit IP extensions \(page 137\)](#)
- [Unassign IP extensions \(page 138\)](#)
- [Unassign a range of extensions \(page 139\)](#)
- [Create and import large numbers of extensions \(page 140\)](#)
- [IP recorder extensions \(page 141\)](#)
- [Recorder extensions \(page 141\)](#)
- [View IP recorder extensions \(page 142\)](#)
- [View TDM recorder extensions \(page 142\)](#)

Duplicate extensions support

This release includes support for duplicate extensions over multiple data sources—that is, the same extension identifier can exist on two different data sources, and be recorded by a single IP or TDM recorder. For example, you may be recording on two different switches, each of which uses the same set of extensions, or extension ranges that overlap. See "Recording Duplicate Extensions" under [Extensions \(page 430\)](#) for specific details and limitations.

Long extensions support

This release also supports long extensions, such as those required for SIP, up to 255 characters in length.

 Extensions will not be recorded if the extension is not associated with a recorder.



When you set up phones and extensions, you will specify a Recording Mode. The Integration Service uses this and other settings (including those in the associated member group) to determine what should be recorded and when—see “Recording Decisions” in the *Technical Overview* for more information about how these settings impact one another.

Create and edit phones/extensions

You can add or edit primary and secondary extensions (for example, you may wish to change an extension’s recording mode). You can only edit secondary extensions when editing a single extension.

Secondary extensions and Real-time Monitoring

It is important to understand that Real-time Monitoring is not supported for secondary extensions.

Before you begin

If you will be using screen recording, you must set up a LAN data source and Workstations before completing the following procedure (in order to associate extensions with said workstations). See [Create a LAN data source \(page 107\)](#) and [Set up workstations and workstation groups \(page 109\)](#).

Procedure

1. Click **Recording Management > Data Sources > Settings**. Select a Phone data source from the left pane.
2. Click **Phones**.
In a multi-tenant enabled environment, the tenant to which the selected data source is associated displays in parentheses in the screen heading. An organization belongs to a tenant. When a data source is associated to an organization, the screen heading displays the tenant to which the organization belongs. The data source can be associated to a particular tenant or have the **Shared** status. A data source associated to a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.
3. Click **Create** (or click **Edit** to modify an existing phone).

The screenshot shows the 'RECORDING MANAGEMENT' interface. At the top, there are tabs for 'DATA SOURCES', 'CUSTOM DATA', 'RECORDING RULES', 'ARCHIVE', and 'RECORDER ANALYTICS RULES'. Below these are links for 'Settings', 'Member Groups', 'Phones', 'Data Source Groups', 'Employees', and 'Import Status'. The main area is titled 'PHONE: New Phone'. It shows a 'Data Source Name' section with a 'Phone' icon and the name 'Phone'. Under 'Primary Extension', the 'Extension' field is empty, 'Recording Mode' is set to 'Record', 'LAN (Screen) Data Source' is set to 'Select LAN (Screen) Data Source', and 'Workstation Name' is empty. There is a pencil icon next to the 'Workstation Name' field. Below this is a section for 'Secondary Extensions' with a table header '# Extension' and 'Recording Mode'. One row is shown with '# 1', 'Extension' empty, and 'Recording Mode' set to 'Record'. There are 'Add' and 'Delete' buttons. At the bottom right are 'Save', 'Cancel', and 'Revert' buttons.

4. Specify or edit the following:

- **Extension**—Type the extension number, including any prefix or suffix, such as 3344, or X3344, or X3344A (the prefix and suffix are not case-sensitive).
- **Recording Mode**—Choose one of the following extension recording modes:

⚠ Block Recording Rules and Block commands through AIM, Connect and other third party APIs will cause the interaction or contact to not be recorded, regardless of the extension recording mode, recording rules or other third party API commands.

- **Record**—Record all calls on this extension.
- **Recording Resource**—Only for soft phones. Use in conjunction with a Service Observe or Single Step Conferencing Recorder Control Type.
- **Start on Trigger**—Do not record calls on this extension until a recording rule is triggered or an external API command starts recording. If the recorder is set to recorder controlled, recording will start whenever the recorder starts, but audio prior to the recording trigger will be deleted; the interaction will start there, and continue to the end of the call.
- **Application Controlled**—Record every call, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the call.
- **Do Not Record**—Do not actively record this extension. Other extensions on the same call will follow their respective Recording Mode, and may record audio for this extension. External API commands or recording rules do not override this setting.



Using start/stop recording commands when screen recording is active will result in only the first screen recording segment being captured. Subsequent use of start/stop will only affect the audio and not the screen, meaning screens will continue to not be recorded after the first stop (regardless of whether start is issued again).

If the `RestartSession` parameter is set to false through the Recorder API (or if the parameter is not present), the behavior will be as above. If `RestartSession` is set to true, a new segment and a new recording will be created upon receipt of a start command.



Application Controlled is for use with the Cisco Phone Services adapter (formerly `ExecRecord`)—see the *Cisco Integration Guide* for more information. This feature allows you to record calls on demand, in recording environments that use Cisco CallManager equipment and IP phones.

- **Content Type**—Select **Audio**, **Screen**, or **Audio and Screen**. This determines the type of content that will be recorded on this particular extension. The default is Audio.
 - **LAN (Screen) Data Source**—Required for screen recording. Select the LAN data source with which the phone must be associated.
-
- In a multi-tenant enabled environment, only LAN data sources associated to the same tenant as the phone data source selected earlier in this procedure are available for selection.
- **Workstation Name**—In setups involving a LAN data source, you can map phones to workstations. Click the pencil icon. Select a workstation, then click Set.

SELECT WORKSTATION:

Find Workstation

Workstation (Host Name)

ptedkw71
vtdktp01
vtdktp02
vtdktp03
vtdktp04
vtdktp05
vtdktp06
vtdktp07
vtdktp08
vtdktp09
vtdktp10
vtdktp11
vtdktp12
vtdktp13
vtdktp14
vtdktp15
vtdktp16
vtdktp17
vtdktp18
vtdktp19

5. Under **Secondary Extensions**, type the secondary extension number in the **Extension** field. This number must be distinct from the primary number. For example, add a prefix or suffix to the primary number. Primary and Secondary extensions are not case-sensitive. Set the **Recording Mode** for the extension and the **Content Type to Record** (see above for descriptions).
6. Click **Add** to add new secondary extensions as needed.
7. Click **Save**.

Related topics

[Set up phones and extensions \(page 124\)](#)

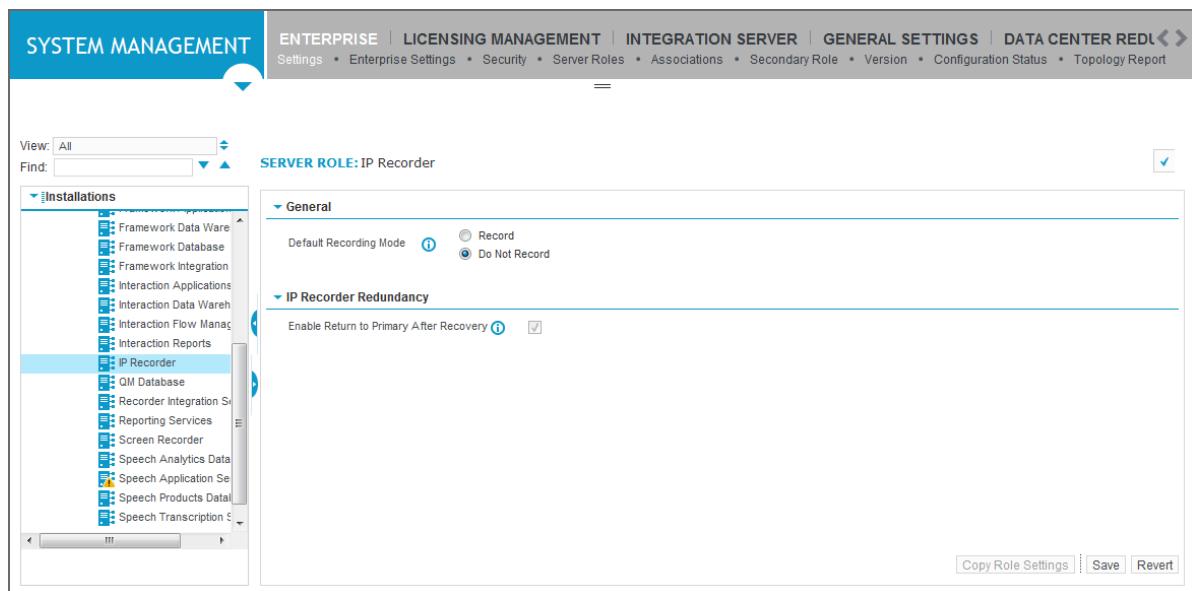
Set a default recording mode

In Recorder-controlled IP recording, use the following procedure to:

- set a default behavior for those extensions not explicitly configured in a member group (record all, or record none).
- specify the type of content to record.

Procedure

- Click **System Management > Settings**.
- Under **Installations**, expand the Recorder node and select the **IP Recorder** role.



- Set the **Default Recording Mode** to **Record** or **Do Not Record**.
- Click **Save**.

Fallback for Unconfigured Extensions

The Default Recording Mode setting applies to extensions configured in member groups. Fallback modes can be applied to these extensions. However, if you set the Default Recording Mode to Record, unconfigured extensions will not have an associated fallback mode. To remedy this, complete the following procedure.

- Open the file `IPCaptureConfig.xml` in a text editor such as Notepad.
- Search for `RecordingErrorAlarmThreshold`.
- Below this section, add the setting `DefaultRecorderFallbackType`, with value of **Never**, **OnCTIDisconnection**, or **Always** — see [Fallback modes \(page 431\)](#) for descriptions.

OnCTIDisconnection is the default value.

Example:

```
<x:RecordingErrorAlarmThreshold>30</x:RecordingErrorAlarmThreshold>
<x:DefaultRecorderFallbackType>OnCTIDisconnection</x:DefaultRecorderFall
backType>
```

4. Save the file.

Related topics

[Set up phones and extensions \(page 124\)](#)

Map workstations to phones

Mapping workstations to phones creates an association between an IP or TDM phone switch and a Screen (LAN) Data Source. For a Screen Data Source, you do not need to select a Workstation, as the extension is created while creating extensions in the Workstation.

Related topics

[Set up phones and extensions \(page 124\)](#)

Edit multiple extensions

You can change multiple non-clustered extensions for a selected switch at one time, using the following procedure.

Procedure

1. Click **Recording Management > Data Sources > Settings**, then select a Phone data source.
2. Click **Phones**, then select two or more extensions.
3. Click **Edit**.

Extension	Recording Mode	LAN (Screen) Data Source	Workstation Name
211	Record	Screen Recording	vtdktp03
212	Record	Screen Recording	vtdktp01

4. Complete the fields as described in [Create and edit phones/extensions \(page 125\)](#).
5. Click **Save**.

Related topics

[Set up phones and extensions \(page 124\)](#)

Create a range of extensions

You can automatically create a series of extension numbers between a specified start and end range, including prefixes and postfixes, allowing you to create up to five thousand extensions at once. All extensions in the range assume the same recording mode, and are not case-sensitive.

Procedure

1. Click **Recording Management > Data Sources > Settings**.
2. Select a Phone data source.
3. Click **Phones**.

In a multi-tenant enabled environment, the tenant to which the selected data source is associated displays in parentheses in the screen heading. An organization belongs to a tenant. When a data source is associated to an organization, the screen heading displays the tenant to which the organization belongs. The data source can be associated to a particular tenant or have the **Shared** status. A data source associated to a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

4. Click **Create Range**.

The screenshot shows the 'CREATE PHONE RANGE' window. On the left, a sidebar lists data sources: Aastra MX-ONE, AmazonConnect1, Avaya1, Cisco1, Cisco DS1, CiscoScreenDS1, Dialer1, LANScreen, Lync1, Mitel1, and Skype1. The main area is titled 'CREATE PHONE RANGE: New Phone Range (Tenant: T1)'. It contains sections for 'Primary Extension' (Prefix, Extension Range, Postfix, Recording Mode set to 'Record', Overwrite Existing checked) and 'Secondary Extensions' (Delete if Extension exists as primary, Overwrite Existing). Below these are tables for '# Secondary Extensions' and 'Recording Mode', showing one entry with value '1' and mode 'Record'. At the bottom are 'Save', 'Cancel', and 'Revert' buttons.

5. In the Create Phone Range window, complete the following fields:
 - **Prefix**—Type any digit or letter that will precede the extensions number, such as X.
 - **Extension Range**—Type an extension number range, such as 1-100.
 - **Postfix**—Type any digit or letter that will appear after the extension, as an identifier.
 - **Recording Mode**—Choose one of the following extension recording modes:

A Block Business Rules and Block commands through AIM, Connect and other third party APIs will cause the interaction or contact to not be recorded, regardless of the extension recording mode, recording rules or other third party API commands.

- **Record**—Record all calls on this extension.
- **Recording Resource**—Only for soft phones. Use in conjunction with a Service Observe or Single Step Conferencing Recorder Control Type.
- **Start on Trigger**—Do not record calls on this extension until a recording rule is triggered or an external API command starts recording. If the recorder is set to recorder controlled, recording will start whenever the recorder starts, but audio prior to the recording trigger will be deleted; the interaction will start there, and continue to the end of the call.
- **Application Controlled**—Record every call, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the call.
- **Do Not Record**—Do not actively record this extension. Other extensions on the same call will follow their respective Recording Mode, and may record audio for this extension. External API commands or recording rules do not override this setting.

! Using start/stop recording commands while screen recording is active will result in only the first screen recording segment being captured. Subsequent use of start/stop will only affect the audio and not the screen, meaning screens will continue to not be recorded after the first stop (regardless of whether start is issued again).

If the RestartSession parameter is set to false through the Recorder API (or if the parameter is not present), the behavior will be as above. If RestartSession is set to true, a new segment and a new recording will be created upon receipt of a start command.

6. Select the **Overwrite Existing** check box to have existing identical extensions replaced with new ones created in the range. The new one then assumes the characteristics of the range. If unchecked, the identical extension will remain with its existing characteristics (such as recording mode).
7. Under **Secondary Extensions**, select the **Delete if Extension exists as primary** check box to delete the primary extension if a primary extension with the same number/identification is detected. Select the **Overwrite Existing** check box to have existing identical extensions replaced with new ones created in the range.

Next, type the range of secondary extension numbers, which must be distinct from the primary numbers. Secondary extensions assume the same prefix and postfix as the primary extension, and are not case-sensitive. Refer to the following table for extension range guidelines:

Extension type	Allowable ranges
Primary Extension	1000, 1500-2000, 3000
1st Secondary Extension	4000, 4500-5000, 6000
2nd Secondary Extension	7000, 7500-8000, 9000

8. If necessary, click **Add** to add a new secondary extension.

9. Click **Save**.

Related topics

[Set up phones and extensions \(page 124\)](#)

Generate extension numbers or trunk group members

Use one of the following procedures to generate extensions or trunk group members automatically.

Extensions

When you create extensions you may generate extension numbers automatically, assigning phone extension numbers to available channels on a voice card.

Complete the following fields, then click **Assign**:

- **Starting Port Number**—Type the first port number, as shown under **Port #** in the **Create/Edit Station Side Extension Group** window.
- **Number of Ports**—Shows the number of ports, as specified under **Port Count** on the settings page.
- **Starting Extension Number**—Type number of the first extension in the range.

A sequence of numbers will appear beside each port number.

Trunk Group Members

Complete the following fields, then click **Assign**:

- **Trunk Group Number**—The number of the trunk group.
- **Starting Port Number**—The starting number for the range.
- **Number of Ports**—The total number in the group.
- **Starting Trunk Member**—The number of the starting trunk member.
- **Trunk Member Prefix**—The prefix to append to the trunk member.
- **Trunk Member to Skip**—This is applicable if your data source is Avaya with E1 (30 channels), and may be required for ISDN type E1 trunks.

Related topics

[Map employees to data sources \(page 145\)](#)

[Create and edit phones/extensions \(page 125\)](#)

Delete extensions

Use the following procedure to delete extensions.

Procedure

1. Click **Recording Management > Data Sources > Settings**.
2. Select a Phone data source.
3. Click **Phones**, then select one or more extensions.
4. Click **Delete**, then click **OK**. Wait a few seconds until the deletion is complete.

Related topics

[Set up phones and extensions \(page 124\)](#)

Assign a range of IP extensions

Assign IP extensions by specifying a range, as opposed to selecting specific extensions, to associate these primary extensions with a Member Group. Any secondary extensions are also included in the assignment. You can specify a contiguous range, or you can specify single or sub-ranges of extensions by separating with a comma, such as 1000, 1050-1075, and 1080-1090.

Procedure

1. Click **Recording Management > Data Sources > Member Groups**, and then select a Data Source that supports IP Extensions.
2. Choose an IP Extension Pool that has extensions already created, and then click **Edit**.
3. Click **Assign & Create Phones > Assign Range**.

ASSIGN EXTENSION RANGE: To Pool 'mg'

Primary Extension	
Prefix	<input type="text"/>
Extension Range	<input type="text"/>
Postfix	<input type="text"/>
Recording Mode	Record
Overwrite Existing	<input checked="" type="checkbox"/>
▼ Secondary Extensions	
Delete if Extension exists as primary	<input checked="" type="checkbox"/>
Overwrite Existing	<input checked="" type="checkbox"/>
# Secondary Extensions	Recording Mode
1	Record
Add Delete	
Assign Cancel Revert	

4. Complete following fields:

Primary Extension	
Prefix	Type any digit or letter that will precede the extensions number.
Extension Range	Type an extension number range, such as 1,2, 3-100. Here, extensions 1 through 100 would be created. Extensions are case-insensitive.
Postfix	Type any digit or letter that will appear after the extension, as an identifier.
Recording Mode	Choose an extension recording mode as described in Extension recording modes (page 429) .
Overwrite Existing	Select this check box to have existing extensions replaced with new ones created in the range if there are duplications. The new one then assumes the characteristics of the range. If left unchecked, the original extension will remain with its existing characteristics (such as recording mode).

Secondary Extension	
Delete if Extension exists as primary	Select this check box to indicate that the primary extension will be deleted if a primary extension with the same number/identification is detected.

Secondary Extension	
Overwrite Existing	Select this check box to have existing extensions replaced with new ones created in the range if there are duplications. The new one then assumes the characteristics of the range. If left unchecked, the original extension will remain with its existing characteristics (such as recording mode).
Secondary Extensions	Type in only secondary extensions whose recording modes will be changed. If you do not type in secondary extensions they are assigned with the same recording mode as the primary extension. Click Add to add additional rows so that you can type in other secondary extensions.
Recording Mode	<p>Choose an extension recording mode:</p> <ul style="list-style-type: none"> • Record—Record all calls on this extension. • Recording Resource—Not available in all cases, and only used for soft phones. Use in conjunction with a Service Observe or Single Step Conferencing Recorder Control Type. • Start on Trigger—Do not record calls on this extension until a recording rule is triggered or an external API command starts recording. If the recorder is set to recorder controlled, recording will start whenever the recorder starts, but audio prior to the recording trigger will be deleted; the interaction will start there, and continue to the end of the call. • Application Controlled—Record every call, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the call. • Do Not Record—Do not actively record this extension. Other extensions on the same call will follow their respective Recording Mode, and may record audio for this extension. External API commands or recording rules do not override this setting.

5. Click **Assign**.

Related topics

[Edit IP extensions \(page 136\)](#)

[Set up phones and extensions \(page 124\)](#)

Edit IP extensions

Change IP extensions to edit the Recording Modes of individual extensions.

Procedure

1. Click **Recording Management > Data Sources > Settings**.
2. Select a **Phone data source**.
3. Click **Phones**.
4. Select the extension to be edited.
5. Complete the following Primary and Secondary Extension fields:

Item	Description
Extension	Shows the selected extension. Note that extensions are not case-sensitive.
Recording Mode	Change the recording mode for this extension as necessary. See Create and edit phones/extensions (page 125) for more information.

6. Click **Add** to add another Secondary extension.
7. Click **Save**.

Related topics

[Assign a range of IP extensions \(page 134\)](#)

[Set up phones and extensions \(page 124\)](#)

Batch edit IP extensions

Use batch edit mode to change multiple extensions at the same time.

Procedure

1. Click **Recording Management > Data Sources > Phones**.
2. Under **Data Source Name**, select a phone data source.

Extension	Recording Mode	LAN (Screen) Data Source	Workstation Name
211	Record	Screen Recording	vtdktp03
212	Record	Screen Recording	vtdktp01

3. Select one or more extensions and click **Edit**.
4. Make changes as necessary (refer to [Create and edit phones/extensions \(page 125\)](#) for more information on phone settings).
5. Click **Save**.

Related topics

[Edit IP extensions \(page 136\)](#)

[Assign a range of IP extensions \(page 134\)](#)

[Set up phones and extensions \(page 124\)](#)

Unassign IP extensions

Use the following procedure to free selected extensions, including secondary extensions, or a range of extensions, from a Member Group (thereby making them available to other Member Groups).

Procedure

1. Click **Recording Management > Data Sources > Settings**, and then choose a data source that supports IP Extension Pools.
2. Click **Member Groups**, select an IP Extension Pool Member Group, and then click **Edit**.
3. Click **Unassign Phones**. The **Unassign Phones from Member Group** window appears, listing phones already assigned to the Member Group. (Secondary extensions do not appear.)

The screenshot shows a table titled "UNASSIGN PHONES FROM MEMBER GROUP: Phones assigned to this pool". The table has two columns: "Extensions Primary/Secondary" and "Recording Mode". The "Extensions Primary/Secondary" column lists phone numbers from 1000 to 1016. The "Recording Mode" column shows that all extensions are set to "Record". A vertical scroll bar is visible on the right side of the table. At the bottom of the window, there are several buttons: "Select All", "Select None", "Unassign Selected", "Unassign Range", and "Done".

Extensions Primary/Secondary	Recording Mode
1000	Record
1001	Record
1002	Record
1003	Record
1004	Record
1005	Record
1006	Record
1007	Record
1008	Record
1009	Record
1010	Record
1011	Record
1012	Record
1013	Record
1014	Record
1015	Record
1016	Record

4. Select one or more extensions and click **Unassign Selected** to unassign the extensions from the currently selected Member Group.



To search a large number of phone extension records, in the **Find Phone** area type the first few letters or numbers of the extension, and then click **GO**. If no matching records are found, a message indicating this appears beside the **Find Phone** area.

5. Click **Save** when done.

Related topics

- [Set up phones and extensions \(page 124\)](#)
[Assign a range of IP extensions \(page 134\)](#)

Unassign a range of extensions

Use the following procedure to remove an entire range of extensions from membership in the selected Member Group. (Secondary extensions will also be unassigned.)

Procedure

1. Follow procedures as described in [Unassign IP extensions \(page 138\)](#), and then click **Unassign Range**.

UNASSIGN EXTENSIONS: From IP Pool 'IPTestCalls-FreeSwitchPool'

Primary Extension

Prefix |

Extension Range

Postfix

Unassign Cancel Revert

2. Complete the following fields:

Item	Description
Prefix	Type a prefix for the primary extension, such as FL2200.
Extension Range	Type primary extensions or ranges of primary extensions separated by commas, such as 1, 2, 3-488, 499 for extensions 1, 2, 499, and all extensions in the range 3 to 488. All secondary extensions are included and are unassigned along with the primary extensions.
Postfix	Type a postfix for the primary extension, such as FL in 2200FL.

3. Click **Unassign**.

Related topics

[Set up phones and extensions \(page 124\)](#)

[Assign a range of IP extensions \(page 134\)](#)

Create and import large numbers of extensions

There are limitations on the number of extensions you can assign to an IP Extension Pool Member Group or to an IP Recorder.

- You can assign a maximum of 20,000 extensions to a Member Group or to a single Recorder. This is the default limit. If you need to assign more than this number, contact the supplier of your Recorder.

Example: Member Group A has 5,000 extensions. Member Group B has 18,000 extensions. You cannot assign both of these Member Groups to one IP Recorder, because the total number of extensions assigned to this Recorder will be 23,000, and the maximum is 20,000.

This rule applies when clustering or assigning new phones to Member Groups in a cluster. For example, if the total number of extensions belonging to all the Member Groups in a cluster exceeds 20,000, the operation will fail (an error message will indicate this).

- You cannot create a range of more than 5,000 extensions at a time.

Example: To create 10,000 extensions using the **Create Range** option, you must create the range 1 to 4,999, and then another range from 5,000 to 9,999. The same rule applies when unassigning phones from an IP Member Group: you must unassign in groups of 5,000.

- You can assign duplicate extensions to a Recorder within a single Data Source, through Member Group association (that is, you can have the same extension number in different Member Groups).

Example: Assume you have Data Sources named DS1 and DS2. Assume also that you have two Member Groups, MG1 and MG2:

- MG1-DS1 can be assigned with extension 1-10 in Data Source DS1
- MG1-DS2 can be assigned with extension 4-6 in Data Source DS2
- MG2-DS1 can be assigned with extension 5-8 in Data Source DS1
- You cannot have duplicate extensions across data sources.

Example: You cannot associate the Member Groups MG1-DS1 and MG1-DS2 (above) to a Recorder, because this would cause duplicate extensions (4 - 6) across Data Sources.

These extensions include primary and secondary extensions. For example, if a phone has one primary and five secondary extensions, the total extensions considered for calculation is six.

i When importing and exporting extensions from a .csv file, all of the above rules apply, with the exception of the 5000 extension range limitation. When importing or exporting from a .csv file, you can export or import a maximum of 80,000 extensions.

Related topics

[Set up phones and extensions \(page 124\)](#)

IP recorder extensions

You can add primary and secondary telephone extensions for use throughout the organization, and set whether phone extensions are recorded, and select a recording mode.



This release includes support for duplicate extensions over multiple data sources—that is, the same extension identifier can exist on two different data sources. This release also supports long extensions, such as those required for SIP, up to 255 characters in length.



Extensions will not be recorded if the extension is not associated with a recorder.

Related topics

- [Set up a dialer integration \(page 116\)](#)
- [Set up screen recording \(page 106\)](#)
- [Create and edit phones/extensions \(page 125\)](#)
- [Edit multiple extensions \(page 130\)](#)
- [Create a range of extensions \(page 131\)](#)
- [Generate extension numbers or trunk group members \(page 133\)](#)
- [Set up phones and extensions \(page 124\)](#)

Recorder extensions

You can add primary and secondary telephone extensions for use throughout the organization, and set whether phone extensions are recorded, and select a recording mode.

Related topics

- [Create and edit phones/extensions \(page 125\)](#)
- [Edit multiple extensions \(page 130\)](#)
- [Create a range of extensions \(page 131\)](#)
- [Generate extension numbers or trunk group members \(page 133\)](#)
- [Set up phones and extensions \(page 124\)](#)

View IP recorder extensions

You can view all telephone extensions associated with a particular IP Recorder and configure the extensions individually.

Procedure

1. Click **Recording Management > Data Sources >Member Groups**.
2. Select an IP Recorder, then a Member Group, and then click **View Members**.
3. Review the Primary and Secondary extensions and their Recording Modes.
4. Click **Done**.

Related topics

[Edit IP extensions \(page 136\)](#)

[Set up phones and extensions \(page 124\)](#)

View TDM recorder extensions

View telephone extensions from Enterprise Manager in a station-side or trunk-side TDM Recorder environment to access all extensions associated with a particular Recorder.

Procedure

1. Click **System Management > Settings**.
2. Under **Installations**, click **Member Groups**.
3. Select a TDM Recorder, select a Member Group, and then click **View Members**.
4. Review the Port numbers, Trunk Group (if present), Channels, and Extension numbers, as applicable to the switch type, and click **Done**.

Related topics

[Set up phones and extensions \(page 124\)](#)

Create employees and add employee IDs

You can add agents to the system either individually or by importing a list of agents from an existing source. The following sections describe how to do this and how to specify a seating arrangement and edit agent mappings.

- [Create an employee \(page 143\)](#) or [Import employee from an existing source \(page 145\)](#)
- [Map employees to data sources \(page 145\)](#)
- [Edit employee mappings \(page 147\)](#)



You should configure Employees and Employee IDs if you want Employee name, Supervisor or Logged on Duration for tagging or recording rules. However, if you require only Employee ID tagging, you do not need to configure these.

Related topics

[Create an employee \(page 143\)](#)

[Import employee from an existing source \(page 145\)](#)

Create an employee

Use the following procedure to create an employee.

Procedure

1. Click **User Management > Employees > Profiles**.

2. Click the **Create** button.
3. Type the Employee's Last Name, First Name, Middle Initial (all required) and Suffix (optional).

Step through Step are optional if you are not using Workforce Management.

4. Under Contact Information, type the following information for the employee: E-mail, Fully Qualified User Name, Home Phone, Work Phone, Cell Phone.
5. Under Home Address, type the employee's address details in the relevant fields.
6. Under Administrative Details, specify details for that employee.



If an employee who has a user account is terminated, the employee's user account is automatically put in Locked – By Admin status at midnight of the employee's final day. If, subsequently, the employee is un-terminated (the end date is deleted or moved to the future), you must modify their user account status manually.

7. In the Data Source section, associate the employee with a data source by typing their employee ID or extension in the field next to the appropriate data source. The seating arrangement you set when creating the data source determines what you must specify here.



For LAN data sources in a Free Seating or Hybrid Environment, the Employee ID is the Network Login ID on the domain (such as the Windows Login ID). You will also specify this ID when mapping employees to the data source (as described in [Map employees to data sources \(page 145\)](#)).

If the seating arrangement is	specify the
Fixed	Extension. Employees are assigned to extensions permanently and do not share extensions with other Employees. No login events are required to assign the Employees to their extensions.
Free	Employee ID. The System will dynamically assign Employees to extensions based on received login events.
Hybrid	Employee ID or Extension. On a per Employee basis, each Employee can either be designated as using fixed or free seating. The arrangement used is determined by whether they have an Extension assigned. If an extension is assigned the Employee seating arrangement is considered fixed.

You can either type the phone extension, or click the Pencil icon to show the Select Extension window, choose the extension, and then click **Set**.



You can specify multiple Employee IDs by typing the IDs separated by commas, or by clicking the Pencil icon and using the **Add** button.

8. Click **Save**.

What to do next

[Map employees to data sources \(page 145\)](#)

Related topics

[Create employees and add employee IDs \(page 143\)](#)

Import employee from an existing source

You can import a list of Employees from an existing source, such as a .csv file containing information from LDAP.

Procedure

1. Click **User Management > Employees > Profiles**.
2. Click **Import**.
3. Under File Setup, click **Browse** and select the file to import.
4. As the **Delimiter**, specify whether Tabs, Commas, or Semicolons separate the data in the source file.
5. Type the number of lines appearing at the start of the file that should be ignored.
6. From the list of fields, select those that appear in your file, and indicate the column number in which that data appears. Last Name, First Name, and Organization are mandatory.
7. Click **Save**.

What to do next

[Map employees to data sources \(page 145\)](#)

Related topics

[Create employees and add employee IDs \(page 143\)](#)

Map employees to data sources

You can map Employees to data sources to provide employees in your organization with a switch ID, and associate this ID with data sources such as a phone switch or LAN. Data sources appear in the left pane, and only those Employees associated with a data source appear in the right pane.

You can add, edit and delete Employee mappings, as described in the following topics:

- [Add employee mappings \(page 146\)](#)
- [Edit employee mappings \(page 147\)](#)



You must have the "View and Configure Data Sources" privilege to edit these settings.

Related topics

[Add employee mappings \(page 146\)](#)

[Edit employee mappings \(page 147\)](#)

[Map employees to data sources \(page 145\)](#)

Add employee mappings

Add Employee mappings to associate Employees with data sources.

Procedure

1. Select **Recording Management > Data Sources > Employees**.
2. Select a data source.

In a multi-tenant enabled environment, the tenant to which the selected data source is associated displays in parentheses in the screen heading. An organization belongs to a tenant. When a data source is associated to an organization, the screen heading displays the tenant to which the organization belongs. The data source can be associated to a particular tenant or have the **Shared** status. A data source associated to a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

3. Click **Add Employee Mapping**.

The screenshot shows a 'SELECT EMPLOYEE' dialog box. At the top, there are 'View:' and 'Find:' dropdowns. The 'View:' dropdown is set to 'PTE Department'. Below the dropdowns is a list of employees under the 'Name' header. The list includes 'User, First', 'User, Install', and 'User, Second'. At the bottom of the dialog box are four buttons: 'Select All', 'Select None', 'Add', and 'Cancel'.

4. Select one or more Employees, and then click **Add**.
5. Specify the following information (see [Create an employee \(page 143\)](#) for more information):
 - For free seating, specify an **Employee ID** (this is a **Network ID** in the case of LAN data sources). For Phone and Dialer data sources this is the Employee ID on the Switch or Dialer (for Phone data sources, this is only visible for Free or Hybrid seating arrangements). For LAN data sources, this is the Network Login ID on the domain (such as the Windows Login ID), which you must also specify for the agent on the User Management page (see [Create an employee \(page 143\)](#)). You can enter multiple IDs for a single data source (up to a maximum of ten), by using commas to separate each ID, or using the **Add** button.

- For fixed seating, specify an **Extension** (or a **Workstation** for LAN data sources), either by typing the extension in the field, or clicking the pencil icon to select one.



Once you map a person to a workstation, you will not be able to delete the workstation. To delete the workstation you must remove the association with the person.

- For hybrid seating, specify both an **Employee ID** and **Extension**.

6. Click **Save**.

What to do next

[Set up attributes, tagging, and recording rules \(page 269\)](#)

Related topics

[Map employees to data sources \(page 145\)](#)

Edit employee mappings

You can edit Employee mappings to associate new or updated Employee IDs or Network IDs with agents.

Complete one of the following procedures:

- To select Employee IDs for Free Seating and Hybrid Seating arrangements, see [To edit Employee mappings for free and hybrid seating \(page 147\)](#).
- To select extensions for Fixed Seating arrangements, see [To select extensions for fixed seating \(page 148\)](#).



You must have the "View and Configure Data Sources" privilege to edit these settings.

To edit Employee mappings for free and hybrid seating

- Select **Recording Management > Data Sources > Employees**.
- Select a data source and one or more Employees.

In a multi-tenant enabled environment, the tenant to which the selected data source is associated displays in parentheses in the screen heading. An organization belongs to a tenant. When a data source is associated to an organization, the screen heading displays the tenant to which the organization belongs. The data source can be associated to a particular tenant or have the **Shared** status. A data source associated to a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

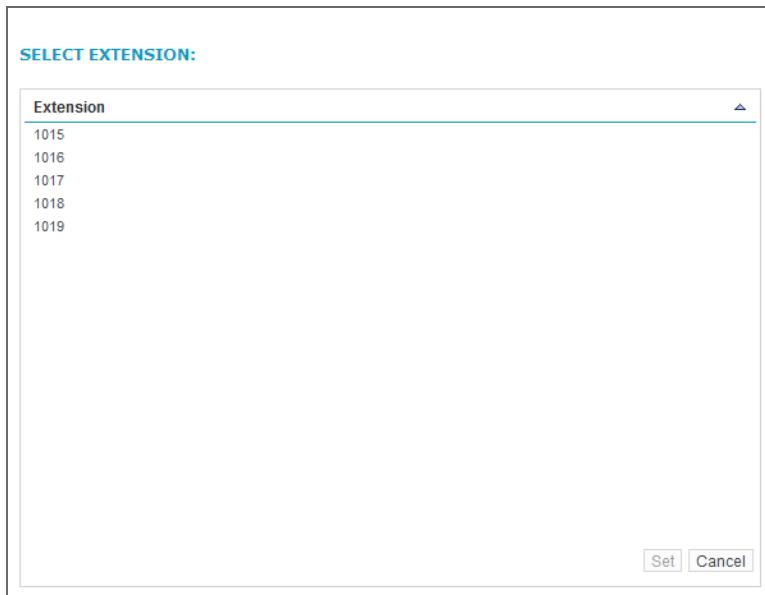
- Click **Edit Employee Mapping**.
- Depending on the Employee settings on the User Management page, and whether you are editing a phone or LAN data source, you may edit one of the following settings:

- **Employee ID:** Type the employee's unique ID. For Phone and Dialer data sources this is the employee ID on the Switch or Dialer (for Phone data sources, this is only visible for Free or Hybrid seating arrangements). For LAN data sources, this is the Network Login ID on the domain (such as the Windows Login ID).
- **Extension:** Type the extension numbers, separated by commas, to which the Employee must be mapped, or click the pencil icon  to select extensions as described in [To edit Employee mappings for free and hybrid seating \(page 147\)](#).
- **Workstation:** Type the workstation name for LAN data sources.
- **Network ID:** Available for LAN (Screen) data sources only, if a Fixed or Hybrid seating arrangement has been specified. Shows the Workstation ID on the network.

5. Click **Save**.

To select extensions for fixed seating

1. Edit Employee mappings as described in [Edit employee mappings \(page 147\)](#), and then click the pencil icon to select extensions to be mapped to the Employee.



2. Select the extension(s) to be mapped to the Employee. If multiple pages of extensions exist, you can search by typing the first few digits in the **Find Extension** field and then clicking **Go**.
3. Click **Set**, and then click **Save**.

Related topics

[Map employees to data sources \(page 145\)](#)

[Add employee mappings \(page 146\)](#)

Create a recording profile

You can have employees for whom you only want to record chat, others for whom you only want to record audio, and still others for whom you want to record both. You can use Recording Profiles to stipulate the type of content you want to capture for multiple employees at once.



You can create a maximum of 200 Recording Profiles.

How Recording Profiles are applied to interactions

When a user takes a call, the profile applied to the interaction is the profile in the organization tree that is closest to the user. The closest profile that can be assigned to a user is an employee recording profile to which the user is directly assigned. For an organization recording profile, the closest profile that can be assigned to the user is a profile that is assigned to the organization to which the user directly belongs. If no profile is assigned to the organization to which the user directly belongs, the system will walk up the organization tree, checking each organization level for an assigned profile. The first assigned profile will be the profile selected for the interaction. If no profile is found, the system will default to record the audio and text of the user's interaction, and to not record the video and screen activity of the interaction. Changes to the recording profiles will not take effect for in-progress interactions, but will take effect for future interactions.

Create a Recording Profile

1. In Enterprise Manager, select **Recording Management**. Under **Data Sources**, click **Settings**.
2. From the pane on the left side, select the data source associated with the employees for whom you want to specify recording settings.
3. Click **Recording Profiles** (in the gray bar at the top of the display). This screen displays all available Recording Profiles.
In a multi-tenant enabled environment, the tenant to which the selected data source is associated displays in parentheses in the screen heading. An organization belongs to a tenant. When a data source is associated to an organization, the screen heading displays the tenant to which the organization belongs. The data source can be associated to a particular tenant or have the **Shared** status. A data source associated to a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.
4. Click **Create**.
5. Type a **Name** for the profile.
6. Enter a **Description** (optional).
7. If the **Record Audio** option appears, select one of the following settings:
 - **Record** - Record all audio calls for this group of employees. Only a block recording rule, AIM command, or external API command can prevent calls from being recorded.
 - **Do Not Record** - Do not record audio calls for this group of employees. Recording rules are ignored and cannot trigger the recording of audio calls.
 - **Application Controlled** - Record every audio call for this group of employees, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the audio call. If the call is kept, the recording includes all audio from the start to the end of the call.

- **Start On Trigger** - Do not record audio calls for this group of employees until a recording rule is triggered or an external API command starts recording. Audio recording starts whenever the call starts, but the audio that came before the recording trigger is deleted.
8. If the **Record Chat** option appears, specify whether chat should be recorded for this group of employees by setting **Record Chat to Record** or **Do Not Record**.
9. If the **Record Video** option appears, select one of the following settings pertaining to video calls:
- **Record** - Record all video calls for this group of employees. Only a block recording rule, AIM command, or external API command can prevent calls from being recorded.
 - **Do Not Record** - Do not record video calls for this group of employees. Recording rules are ignored and cannot trigger the recording of video calls.
 - **Application Controlled** - Record every video call for this group of employees, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the video call. If the call is kept, the recording includes all video from the start to the end of the call.
 - **Start On Trigger** - Do not record video calls for this group of employees until a recording rule is triggered or an external API command starts recording. Video recording starts whenever the call starts, but the video that came before the recording trigger is deleted.
10. If the **Record Screen Share** option appears, select one of the following settings pertaining to screen sharing activity in calls:
- **Record** - Record all screen sharing activity for this group of employees. Only a block recording rule, AIM command, or external API command can prevent screen sharing activity during calls from being recorded.
 - **Do Not Record** - Do not record screen sharing activity in calls for this group of employees. Recording rules are ignored and cannot trigger the recording of screen sharing activity during calls.
 - **Application Controlled** - Record all screen sharing activity during calls for this group of employees, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the screen sharing activity. If the screen sharing activity is kept, the recording includes all screen sharing activity from the start to the end of the call.
 - **Start On Trigger** - Do not record screen sharing activity during calls for this group of employees until a recording rule is triggered or an external API command starts recording. Screen sharing recording starts whenever the call starts, but the screen sharing activity that came before the recording trigger is deleted.
11. If the **Record Text** option appears, specify whether chat interactions should be recorded for this group of employees by setting **Record Text to Record** or **Do Not Record**.
12. If the **Record Email** option appears, specify whether email should be recorded for this group of employees by setting **Record Email to Record** or **Do Not Record**.
13. If the **Record Instant Messaging** option appears, specify whether instant messages should be recorded for this group of employees by setting **Record Instant Messaging to Record** or **Do Not Record**. Instant messages are messages that are sent on any messaging platform including social media platforms such as Instagram, Facebook Messenger, WhatsApp and others.
14. If the **Record Social Media** option appears, specify whether public social media posts, such as tweets or Facebook posts, should be recorded for this group of employees by setting **Record Social Media to Record** or **Do Not Record**.

15. There are two ways to add Employees to a Recording Profile. Note that you may mix and match both types, including both Organizations and individual employees in the same profile:
 - **Organization:** These are organizations created under **Organization Management**. You may add multiple Organizations to a single Recording Profile. Selecting a parent Organization will automatically select its children, but you may cancel the selection of these individually.
An organization cannot be assigned to more than one Recording Profile in a data source. If an organization is assigned to a Recording Profile in a data source, the organization is not available to be assigned to other Recording Profiles in that same data source. In this scenario, a warning message displays indicating the organizations listed do not include organizations that are already assigned to a Recording Profile.
 - **Employee:** Employees are set up under **User Management**. Select one or more employees from the left-hand pane, then use the arrow buttons to move them to the right. If there is a large number of employees, you can use the filter tool to narrow the selection.
An employee cannot be assigned to more than one Recording Profile in a data source. If an employee is assigned to a Recording Profile in a data source, the employee is not available to be assigned to other Recording Profiles in that same data source. In this scenario, a warning message displays indicating the employees listed do not include employees that are already assigned to a Recording Profile.

16. Click **Save**.

Related topics

[Edit a recording profile \(page 151\)](#)

Edit a recording profile

You can edit existing recording profiles using the following procedure.

Edit a Recording Profile

1. In Enterprise Manager, under **Recording Management > Data Sources**, click **Settings**.
2. From the left-hand pane, select the data source associated with the Employees for whom you want to specify recording settings.
3. Click **Recording Profiles** (in the gray bar at the top of the screen). This screen displays all available Recording Profiles.
4. Select a profile, then click **Edit**.
5. Type a **Name** for the profile.
6. Enter a **Description** (optional).
7. If the **Record Audio** option appears, select one of the following settings:
 - **Record** - Record all audio calls for this group of employees. Only a block recording rule, AIM command, or external API command can prevent calls from being recorded.
 - **Do Not Record** - Do not record audio calls for this group of employees. Recording rules are ignored and cannot trigger the recording of audio calls.
 - **Application Controlled** - Record every audio call for this group of employees, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder

- to keep the audio call. If the call is kept, the recording includes all audio from the start to the end of the call.
- **Start On Trigger** - Do not record audio calls for this group of employees until a recording rule is triggered or an external API command starts recording. Audio recording starts whenever the call starts, but the audio that came before the recording trigger is deleted.
8. If **Record Chat** appears, specify whether chat should be recorded for this group of Employees by setting **Record Chat** to **Record** or **Do Not Record**.
9. If the **Record Video** option appears, select one of the following options pertaining to video calls:
- **Record** - Record all video calls for this group of employees. Only a block recording rule, AIM command, or external API command can prevent calls from being recorded.
 - **Do Not Record** - Do not record video calls for this group of employees. Recording rules are ignored and cannot trigger the recording of video calls.
 - **Application Controlled** - Record every video call for this group of employees, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the video call. If the call is kept, the recording includes all video from the start to the end of the call.
 - **Start On Trigger** - Do not record video calls for this group of employees until a recording rule is triggered or an external API command starts recording. Video recording starts whenever the call starts, but the video that came before the recording trigger is deleted.
10. If the **Record Screen Share** option appears, select one of the following settings pertaining to screen sharing activity in calls:
- **Record** - Record all screen sharing activity for this group of employees. Only a block recording rule, AIM command, or external API command can prevent screen sharing activity during calls from being recorded.
 - **Do Not Record** - Do not record screen sharing activity in calls for this group of employees. Recording rules are ignored and cannot trigger the recording of screen sharing activity during calls.
 - **Application Controlled** - Record all screen sharing activity during calls for this group of employees, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the screen sharing activity. If the screen sharing activity is kept, the recording includes all screen sharing activity from the start to the end of the call.
 - **Start on Trigger** - Do not record screen sharing activity during calls for this group of employees until a recording rule is triggered or an external API command starts recording. Screen sharing recording starts whenever the call starts, but the screen sharing activity that came before the recording trigger is deleted.
11. If the **Record Text** option appears, specify whether text should be recorded for this group of Employees by setting **Record Text** to **Record** or **Do Not Record**.
12. If the **Record Email** option appears, specify whether email should be recorded for this group of employees by setting **Record Email** to **Record** or **Do Not Record**.
13. If the **Record Instant Messaging** option appears, specify whether instant messages should be recorded for this group of employees by setting **Record Instant Messaging** to **Record** or **Do Not Record**. Instant messages are messages that are sent on any messaging platform including social media platforms such as Instagram, Facebook Messenger, WhatsApp and others.

14. If the **Record Social Media** option appears, specify whether public social media posts, such as tweets or Facebook posts, should be recorded for this group of employees by setting **Record Social Media to Record or Do Not Record**.
15. There are two ways to add Employees to a Recording Profile. Note that you may mix and match both types, including both Organizations and individual Employees in the same profile:
 - **Organization:** These are organizations created under **Organization Management**. You may add multiple Organizations to a single Recording Profile. Selecting a parent Organization will automatically select its children, but you may de-select these individually.
An organization cannot be assigned to more than one Recording Profile in a data source. If an organization is assigned to a Recording Profile in a data source, the organization is not available to be assigned to other Recording Profiles in that same data source. In this scenario, a warning message displays indicating the organizations listed do not include organizations that are already assigned to a Recording Profile.
 - **Employee:** Employees are set up under **User Management**. Select one or more employees from the left-hand pane, then use the arrow buttons to move them to the right. If there is a large number of employees, you can use the filter tool to narrow the selection.
An employee cannot be assigned to more than one Recording Profile in a data source. If an employee is assigned to a Recording Profile in a data source, the employee is not available to be assigned to other Recording Profiles in that same data source. In this scenario, a warning message displays indicating the employees listed do not include employees that are already assigned to a Recording Profile.
16. Click **Save**.

Related topics

[Create a recording profile \(page 149\)](#)

Create data source groups

In Phone or Dialer data sources, data source groups represent groups of telephone extensions that allow automation. For example, in a hunt group, incoming calls are passed from extension to extension within the group until the call is accepted, optimizing Employee and extension usage. This section describes how to create and edit groups, import group information from a .csv file, and access the queues for multiple groups.



This section describes Data Source Groups from a Recorder perspective, however they may be used for broader purposes in the context of the full product suite. See the *Verint® Enterprise Recording™ System Administration Guide* for complete details.

Related topics

- [Create and edit data source groups \(page 154\)](#)
- [Upload data source group information \(page 156\)](#)

Create and edit data source groups

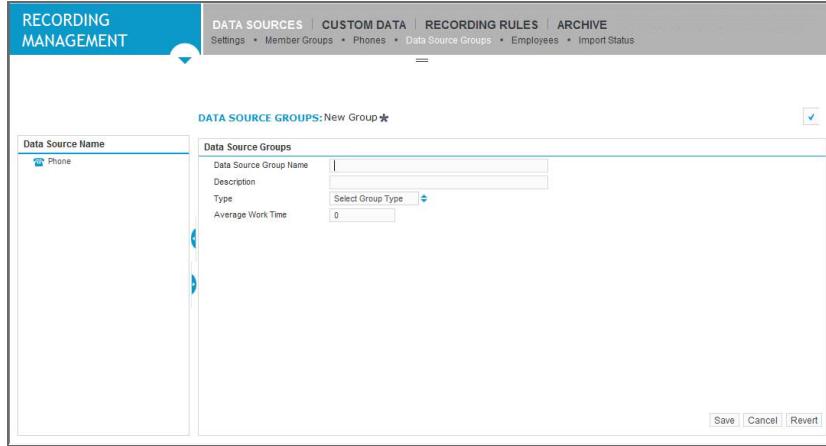
Procedure

1. Click **Recording Management > Data Sources > Data Source Groups**.
2. Select a data source in the left pane.

In a multi-tenant enabled environment, the tenant to which the selected data source is associated displays in parentheses in the screen heading. An organization belongs to a tenant. When a data source is associated to an organization, the screen heading displays the tenant to which the organization belongs. The data source can be associated to a particular tenant or have the **Shared** status. A data source associated to a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

3. Do one of the following:

- Click **Create Group** to create a new Data Source group for the selected Data Source.
- Select a Data Source group in the right pane and click **Edit Group** to edit an existing group.



4. Complete the following fields:

- **Data Source Group Name**—This is a unique value, determined by your switch type. For example, if your switch is Avaya, you would select either Hunt Group or VDN as the group “Type” (as described in the table below), then enter the actual hunt group or VDN number configured in the customer’s switch. Refer to the table below for complete details.
- **Description**—Type a description of the group (optional).
- **Type**—The options that appear under Type are determined by the switch type you have assigned to the data source, as follows. You must enter the number corresponding to the option you choose as the Data Source Group Name, above.

Switch Type	Data Source Group Type Options
Aastra	Select Hunt Group (to distribute phone calls from a single telephone number to a group of several phone lines).
Alcatel	Select Pilot Number. Pilot Number is a term used to refer to an Agent Group.
Aspect	For a phone data source, select Trunk Group or Agent Groups. For a dialer data source, select Call Queue or Agent Groups.
Avaya	For a phone data source, select one of the following: <ul style="list-style-type: none"> Hunt Group—to distribute phone calls from a single telephone number to a group of several phone lines. VDN—Vector Directory Number, which is a soft extension number. For a Dialer data source, select Call Queue or Agent Groups.

Switch Type	Data Source Group Type Options
Nortel	Select one of the following: <ul style="list-style-type: none"> ■ CDN—Controlled Directory Number, wherein calls are queued and can be routed or receive other commands. ■ ACD Queue DN (QDN)—an Automatic Call Distribution Queue, in which calls are held until an employee becomes available.
Cisco, Genesys, or Interactive Intelligence	Select Route Points or Agent Groups.
Unify (Siemens)	Select Call Queue.

Please refer to your switch documentation for more information about the distinctions between these options.

 Do not configure agent group/hunt group extensions as phone extensions in any other places, otherwise you will not receive AgentLoggedOn/Off events from the CTI switch.

- **Average Work Time**—Shows the average work time in hours for the group. Not applicable for data sources that are associated only with the Recorder Integration Service.

5. Click **Save**.

Related topics

[Upload data source group information \(page 156\)](#)

[Create data source groups \(page 154\)](#)

Upload data source group information

You can export Data Source Group information in .csv format. You must ensure that the data being uploaded is in the proper format to be accepted by the Data Source.

Procedure

1. Click **Recording Management > Data Sources > Data Source Groups** and select a data source from the left pane.
2. Click **Upload From File**.

UPLOAD DATASOURCE GROUPS:

File Setup

File:	<input type="button" value="Browse..."/>
Delimiter:	Comma[,]
Prefix for comment lines:	#
Data Source:	Avaya Phone

Field Name	Column Number	Default
<input checked="" type="checkbox"/> Name	1	
<input checked="" type="checkbox"/> Queue Name	2	
<input type="checkbox"/> Average Work Time	3	0
<input type="checkbox"/> Media	4	Phone
<input checked="" type="checkbox"/> Group Type	5	Agent Groups
<input type="checkbox"/> Org Name	6	

3. Complete the following fields:
 - File—Click **Browse** to locate the .csv file containing the information to be uploaded to the Data Source.
 - Delimiter—Specify how the fields in the .csv file are separated: Comma, Tab, or Semi-colon.
 - Prefix for comment lines—Type the character used to indicate lines to be ignored (if applicable).
4. Under Field Name, select each field that appears in the .csv file, and then type the column number in which it appears.
 - Beside the Average Work Time field you can type a default value to indicate the average work time per Employee, in hours (for WFM tracking only).
 - Beside the Media field you can select a default media type: **Voice over IP, Callback, Chat, Email, Fax, Phone, or Phone Outbound**.
5. Click **Upload**.

Related topics

[Create and edit data source groups \(page 154\)](#)

[Create data source groups \(page 154\)](#)

Set up data sources, member groups, and devices for radio recording

Complete the basic tasks required to set up data sources, member groups, and devices for trunked radio systems.

Tasks

- [Create a Radio data source \(page 158\)](#)
- [Create a Devices Pool member group for a Radio data source \(page 162\)](#)
- [Create or edit devices for radio recording \(page 164\)](#)

Create a Radio data source

To set up voice recording for a trunked radio system, you must create a radio data source. A radio data source provides the system with needed information about the radio source to be recorded, such as the switch type and the seating arrangement of employees using the radios.

Procedure

1. Navigate to **RecordingManagement > Data Sources > Settings**, and click **Create Data Source**.
2. In the **Data Source Type** page, do the following:
 - a. From the **Type** drop-down list box, select **Radio**
 - b. From the **Switch/Sub Type** list box, select a switch/sub-type.
3. Click **Select**.
4. Type a **Name** for the radio data source.
5. Specify the **Organization** to which you want to associate the data source.

In a multi-tenant enabled environment, if the selected organization is associated with a tenant, the data source is also associated with that same tenant. In this scenario, when you click **Save** to save the data source, the tenant name of the organization that is associated with the data source is displayed in the screen heading. The data source can be associated with a particular tenant or have the **Shared** status. A data source associated with a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.
6. Type a **Description** for the data source (optional).
7. Select a **Time Zone** from the drop-down list. You can specify whether tagging should be based on this time zone or that of the organization.



The data source types available to you depend on licensing. Similarly, some of the following options are only applicable if you are using a specific switch; therefore, they do not appear in all cases.



It is essential that the time zone is always correct on each server.

7. Under **Recorder Settings**, do the following:

- a. Specify a **Seating Arrangement**—*Fixed, Free, or Hybrid*.
 - **Fixed** seating indicates that an employee has a permanently assigned workstation and is associated with a specific extension. For the Bosch data source sub-type, only the Fixed seating arrangement is available.
 - **Free** seating, the default, indicates that employees do not have permanently-assigned workstations. They are assigned an Employee ID and can log in from any location in the call center. Extensions are assigned dynamically when the employee logs in.
 - **Hybrid** seating refers to a mixed arrangement that contains both Free and Fixed seating for employees.
- b. To prevent the retention of very short calls, specify a **Minimum Session Length (seconds)**. Active calls (from connected to closed) that are shorter than the specified value will be deleted automatically. If set to zero (0), this feature is disabled and no calls will be deleted based on this setting. The maximum value is 3600 (or one hour). This setting applies to the active duration of CTI Sessions or the entire duration of VOX Sessions. Inactive CTI Sessions can be retained using the Session Auditing Policy.
- c. If you are working with a system that uses Performance Mode (set in the IP Extension Pool member group) or N+N redundancy, enable the **Rollback Period (minutes)**.

This ensures that an amount of additional overlapping audio is kept for a period of time, so that in the event of a disconnection it is possible to retrieve it. The default value is 15 minutes, and the maximum value is 60 minutes.

i A rollback period is applicable only to Performance Mode (set in the IP Extension Pool member group) and N+N redundancy.
- d. **Long Call Duration (minutes)**—This setting allows you to specify the length of a call, in minutes, after which the system triggers an alarm. The system also stops tracking the call from a CTI perspective, so in CTI-controlled application or performance mode environments, this may cause loss of recording. Enter any number between 1 and 1440 (24 hours)—an alarm is raised in the cases where calls exceed this number of minutes. The default is 120.

i The Integration Service runs maintenance checks every five minutes to close calls that last for more than the length of time specified as the **Long Call Duration**. An alarm indicated that a call was closed because it was too long. These maintenance checks are not run more frequently in order to avoid imposing an additional load on the system. Therefore it may take up to five minutes to close a long call after it has passed the defined **Long Call Duration** threshold.
- e. **Recording Resource Allocation Behavior**—This setting is for duplicate streaming solutions, which allow you to distribute recordings across multiple recorders.



To use the CTI-based recorder selection feature available for Shared Interception or Avaya DMCC environments, you must select either LineFirst or LineExclusive.

For details, see the *Recorder Configuration and Administration Guide*:

- For Shared inception, see the section “IP Extension Pool Member Group Settings”.
- For Avaya, see the section “Extension Recording Resource Member Group Settings”.

- **IgnoreLine**—Records the next recording on the least-utilized recorder connected to the Integration Service, regardless of data source, member group, and extension list settings.
- **LineFirst**—First attempts to record on the least-utilized recorder that contains the extension being recorded in a member group associated with the recorder. If the Integration Service can't find an associated recorder it will attempt to find any connected recorder with the capacity (whether or not the extension is associated with the recorder). LineFirst provides a way to keep recorders local to the extensions/site. The Integration Service will fail over to another set of recorders if a call can't be recorded locally. If you don't want fail over to another set of recorders, use 'LineExclusive', described below. This is the default.
- **LineExclusive**—First attempts to allocate the recording to the least-utilized recorder that contains the extension being recorded in a member group associated to the recorder. If the Integration Service fails to find a recorder associated with the line to be recorded, it will not record the call. By recording calls on a recorder co-located with the PBX for agents taking calls on a remote site, the use of this setting has the advantage of reduced WAN traffic.

The “least-utilized” recorder is the one with the most unused capacity. For example, if one recorder has 300 licenses and 50 calls are currently being recorded, and another recorder has 100 licenses and 10 calls currently being recorded, the capacity left on the recorders are 250 and 90 respectively. The system will attempt to record the next duplicate streamed call on the first recorder.

- f. **Alarm - Device Not Recorded Call Count**—The number of calls for a configured device that must fail to record before triggering the DeviceNotRecording alarm. The default is 1.
- g. **Alarm - Device Not Recorded (milliseconds)**—Failed call durations under this threshold will not count against the Device Not Recorded Call Count. The default is 15 seconds.
- h. **Session Auditing Policy**—Defines the type of session/interaction that should be marked and kept in the system. “Disabled” (the default) will only mark sessions/interactions with some kind of content. Two additional options will create a basic entry in the database for calls that occurred but were not recorded: “Missed Recordings” will mark calls that should have been recorded, but were not, while “Full Switch” will mark all sessions/interactions for which we receive CTI without recording (for example, calls that were blocked). You may then search for these types of interactions in the Portal.
Recorded employee segments marked by means of auditing will appear in playback once all Interactions in the related Contact are closed, after a delay of up to five minutes.
- i. **Require Replay Audio Redaction** - When redaction is enabled for the system, select whether redaction occurs for interactions that the data source captures. Redaction obscures sensitive customer information in captured audio and transcriptions. Select from the following for interactions that the data source captures:

- **Disabled:** No information in the interaction is obscured. *Disabled* is the default setting.
 - **Always:** Sensitive customer information is obscured.
 - **In Fallback:** Sensitive customer information is obscured, but only in the event of CTI or recorder disconnection from the Integration Service.
- j. **Require Replay Audio Morphing** - When morphing is enabled for the system, select whether replay of interactions captured by the data source requires morphing. Morphing changes the voice heard during replay such that the speaker remains anonymous and the audio remains intelligible. Select from the following options for interactions that the data source captures:
- **Disabled:** The original voice of the agent and the customer are heard during interaction replay. *Disabled* is the default setting.
 - **Always:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting.
 - **In Fallback:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting, but only in the event of CTI or recorder disconnection from the Integration Service.
- k. **Audio Morphing Channel** - Enabled when **Require Replay Audio Morphing** is set to **Always** or **In Fallback**, choose the audio channel or channels that use morphing. Select from:
- **Agent:** Only the voice of the agent channel is morphed during interaction replay. The voice on the customer channel is the original captured voice. *Agent* is the default setting.
 - **Agent and Customer:** The voice of the agent channel and the customer channel are morphed during interaction replay.
8. Expand the **TimeZone Settings** area, and select one of the **Local Time Tagging Mode** options from the drop-down list:
- **Organization**—to base tagging on the organization. This is useful in scenarios where employees are working in different regions, allowing you to unify tagging across multiple time zones.
- i** If you select **Organization**, it is still necessary to specify the correct time zone for the data source as described in step 6, where you selected a time zone from the **Time Zone** drop-down list.

This is used in fallback selection for monitored extensions without an associated Employee or Profile (that is, extensions that don't belong to an employee).
- **Data Source**—to base tagging on the time-zone specified earlier, where you selected a time zone from the **Time Zone** drop-down list.
9. Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system. This should be done only in consultation with our field engineers.
10. If applicable, expand the **Associated Integration Service Installations** area and select the server that is providing Integration Services for the recorder for which you are configuring this data source.



In a multi-tenant enabled environment, the tenant name associated to each Site Group, Site, and Server appears beside the Site Group, Site, and Server name on the right side of the Installations tree.

11. Click **Save**.

Create a Devices Pool member group for a Radio data source

Follow these instructions to create a Devices Pool member group.

Procedure

1. Click **Recording Management > Data Sources > Settings**.
2. Select a Radio data source in the left pane and then click **Member Groups**.
3. Click **Create**.
4. Complete the Devices Pool member group settings. See the related topics section for details about settings for the member group.
5. Click **Save**.

Related topics

[Devices Pool member group settings \(page 162\)](#)

Devices Pool member group settings

The settings that are available depend on the data source sub-type for which the member group is created. Only a subset of the settings below are available for any given data source sub-type.

Setting	Description
Name	Type a unique name for the member group.
Description	Type a description for the member group (optional).
Recorder Control Type	<ul style="list-style-type: none">For most radio data sources, this field has the value of Full Delivery (External Controlled) and cannot be changed. With this setting, recording is controlled by a 3rd party application which redirects audio to the Recorder.For the Bosch Telex data source member group, this field has the value of Recorder Controlled and cannot be changed. With this setting, the Recorder controls recording of the radios or consoles, and implements the default recording modes. In this case the Integration Service is used for segmentation, stitching, and tagging purposes.
Recorder Load Balancing Type	The value of None cannot be changed.

Setting	Description
Recorder Fallback Type	<p>The value of Always (Liability) cannot be changed.</p> <p>With this value, if the radio event interface is disconnected, audio recording continues (VOX-detected segments will be retained). If radio event interface is up, both radio event interface and VOX detected segments will be retained.</p>
Shared Recorders	<p>Use this section to associate one or more recorders with the member group.</p>
Assigned Devices	<p>These fields are populated when you assign devices to the member group:</p> <ul style="list-style-type: none"> • Device ID - The individual device ID for a device assigned to the member group. • Device Name - The name of the device (optional). • Device Type - Indicates whether the device is a Radio or a Talkgroup. • Recording Mode - Can be any of the following: <ul style="list-style-type: none"> ■ Record - Record all radio calls on this Radio or Talkgroup. This is the default setting. ■ Do Not Record - Do not actively record this Radio or Talkgroup. ■ Application Controlled - Record every radio call, and then delete it. At any time during a radio call, a recording rule or external API command can cause the recorder to keep the call. ■ Start on Trigger - Do not record radio calls on this Radio or Talkgroup until a recording rule is triggered or an external API command starts recording. If the recorder is set to Recorder Controlled, recording will start whenever the recorder starts, but audio prior to the recording trigger will be deleted. The interaction starts at the recording trigger, continues to the end of the call.

Setting	Description
Joined Devices	<p>This section appears for Bosch Telex radio data sources, and includes the following fields:</p> <ul style="list-style-type: none"> • Multicast Group IP - This IP address represents a multicast group on the network. Each multicast group is tied to communication with a specific radio line (or channel). Each channel is associated to a profile (console name or radio name). • Multicast Group Port - The port on which the recorder listens for multicast group traffic. • Device Type - The device type is always set to Multicast. • Recording Mode - The Recording Mode is always set to Record.
Advanced Parameters	<p>Use the Key and Value fields to enter the advanced parameters required for your system. Only add advanced parameters in consultation with Verint Support or Field Engineers.</p>

Related topics

[Create a Devices Pool member group for a Radio data source \(page 162\)](#)

Set up devices for radio recording

After you have set up a Radio data source and configured a Devices Pool member group, you can set up devices for radio recording.

- [Create or edit devices for radio recording \(page 164\)](#)
- [Delete devices for radio recording \(page 167\)](#)
- [Create a range of devices for radio recording \(page 168\)](#)
- [Assign radio devices to a member group \(page 170\)](#)
- [Create and assign a range of radio devices to a member group \(page 175\)](#)
- [Unassign individual radio devices from a member group \(page 177\)](#)
- [Unassign a range of radio devices from a member group \(page 178\)](#)

Create or edit devices for radio recording

You can create different types of devices for radio recording. For example, you can create these device types:

A **Radio** represents an individual radio with a unique Device ID.

A **Talkgroup** is a generic term that refers to virtual radio channels created for/by a Trunked Radio System (TRS). All radios in a Talkgroup communicate over a single channel. Only one of the radios can

speak on the channel at a time. The recording system can monitor a Talkgroup based on its unique ID (Device ID) and records all communication on that Talkgroup.

A **Multicast** device type (essentially a multicast group used for Bosch radio recording). A multicast group device type has a unique multicast IP address and a multicast group port.

Procedure

1. Click **Recording Management > Data Sources > Settings**.
2. In the left pane, select the Radio data source for which you want to create a device.
3. Click the **Devices** option.
4. Do one of the following:
 - To create a new device, click **Create**.
 - To edit an existing device, select the device and click **Edit**.
5. Complete the fields on the New Device screen. See the related topics for more information on the fields on the New Device screen.
6. Click **Save**.

Related topics

[New Device screen reference \(page 165\)](#)

[Devices screen reference \(page 173\)](#)

New Device screen reference

Complete the New Device screen to add a device to the Radio data source. The New Device screen contains these settings.

RECORDING MANAGEMENT

DATA SOURCES | CUSTOM DATA | RECORDING RULES

Settings • Member Groups • Devices • Employees • Import Status

DEVICE: New Device

Data Source Name	Device Details
Cisco DS1	Device ID
CiscoScreenDS1	Device Name
Radio Data Source	Device Type
	Recording Mode

Save Cancel Revert

Setting	Description
Device ID	<ul style="list-style-type: none"> If you are creating or editing a Radio, enter the Device ID of the Radio. If you are creating or editing a Talkgroup, enter the Device ID of the Talkgroup.
Multicast Group IP	<p>This field appears only for devices created for the Bosch Telex data source. In this case, the "device" being created is a multicast group.</p> <p>Specify an IP address that represents a multicast group on the network. The IP address must be unique within a data source. Each multicast group is tied to communication with a specific radio line (or channel). Each channel is associated to a profile (console name or radio name).</p>
Multicast Group Port	<p>This field appears only for devices created for the Bosch Telex data source. In this case, the "device" being created is a multicast group.</p> <p>Specify the port on which the recorder listens for multicast group traffic.</p>
Device Name	Enter a name for the device. (The name is at your discretion.)

Setting	Description
Device Type	<p>These Device Type options are available:</p> <ul style="list-style-type: none"> • Radio • Talkgroup <p>Talkgroup is a generic term that refers to virtual radio channels created for/by a Trunked Radio System (TRS). All radios in a Talkgroup communicate over a single channel. Only one of the radios can speak on the channel at a time. The recording system can monitor a Talkgroup based on its unique ID (Device ID) and records all communication on that Talkgroup.</p> <ul style="list-style-type: none"> • Multicast Group - This device type setting appears when creating devices (multicast groups) for a Bosch Telex data source. This device type cannot be changed.
Recording Mode	<p>The supported radio recording modes include:</p> <ul style="list-style-type: none"> • Record - Record all radio calls on this Radio, Talkgroup, or Multicast device type. This is the default setting. • Do Not Record - Do not actively record this Radio or Talkgroup. • Application Controlled - Record every radio call, and then delete it. At any time during a radio call, a recording rule or external API command can cause the recorder to keep the call. • Start on Trigger - Do not record radio calls on this Radio or Talkgroup until a recording rule is triggered or an external API command starts recording. If the recorder is set to Recorder Controlled, recording will start whenever the recorder starts, but audio prior to the recording trigger will be deleted. The interaction starts at the recording trigger, continues to the end of the call.

Related topics

[Create or edit devices for radio recording \(page 164\)](#)

Delete devices for radio recording

You can delete either Radio or Talkgroup devices from a Radio data source.

Procedure

1. Click **Recording Management > Data Sources > Settings**.
2. In the left pane, select the Radio data source from which you want to delete devices.
3. Click the **Devices** tab.
4. Do one of the following:
 - Click **Delete All** to delete all devices from the data source.
 - To delete individual devices, select the devices and click **Delete**. (To select multiple devices, hold down the Ctrl or Shift key while clicking on the devices.)

Related topics

[Create or edit devices for radio recording \(page 164\)](#)

Create a range of devices for radio recording

You can create a series (or range) of Device IDs between specified start and end values. You can include prefixes and postfixes for each device in the range.

You can create a range that includes either only Radio devices or only Talkgroup devices. You cannot create a range that includes both Radio and Talkgroup devices.

A device range can consist of up to 5000 devices.

Procedure

1. Click **Recording Management > Data Sources > Settings**.
2. In the left pane, select the data source for which you want to create a range of devices.
3. Click the **Devices** tab.
4. Click **Create Range**.
5. Complete the fields on the New Device Range screen. See the related topics for information on the individual fields.
6. Click **Save**.

Related topics

[New Device Range screen reference \(page 169\)](#)

[Devices screen reference \(page 173\)](#)

New Device Range screen reference

The New Device Range screen contains these settings.

RECORDING MANAGEMENT

DATA SOURCES | CUSTOM DATA | RECORDING RULES

CREATE DEVICE RANGE: New Device Range

Data Source Name	Device Details
Cisco DS1	Prefix: <input type="text"/>
CiscoScreenDS1	Device Range: <input type="text"/>
Radio Data Source	Postfix: <input type="text"/>
	Device Type: Radio
	Recording Mode: Record
	Overwrite Existing: <input type="checkbox"/>

Save Cancel Revert

Setting	Description
Prefix	Type any digit or letter that will precede the device number, such as X.
Device Range	<p>Type the device number range, such as 1-100.</p> <ul style="list-style-type: none"> To create a sequential range of devices, use a hyphen to separate the start number from the end number. For example, entering 1-1000 creates a range of 1000 devices beginning with device 1 and ending with device 1000. You can also combine a sequential range of devices with individual devices. For example, you can enter 1-1000, 2000, 2500-2600. This device range includes devices 1 through 1000, the individual device numbered 2000, and devices 2500 through 2600. In this case separate multiple entries with a comma. Device numbers entered as a range in this text box must consist only of numeric characters. For example, a device range of 1a-100a or 1*-100* is not valid. (You can, however, enter non-numeric characters in the Prefix and Postfix fields.) Any single device number in a range of device numbers cannot exceed 20 digits.
Postfix	Type and digit or letter that will appear after the device number.

Setting	Description
Device Type	Select Radio to create a range of Radio device IDs, or select Talkgroup to create a range of Talkgroup device IDs. Talkgroup is a generic term that refers to virtual radio channels created for/by a Trunked Radio System (TRS). All radios in a Talkgroup communicate over a single channel. Only one of the radios can speak on the channel at a time. The recording system can monitor a Talkgroup based on its unique ID (Device ID) and records all communication on that Talkgroup.
Recording Mode	The supported radio recording modes include: <ul style="list-style-type: none"> • Record - Record all radio calls on this Radio, Talkgroup, or Multicast device type. This is the default setting. • Do Not Record - Do not actively record this Radio or Talkgroup. • Application Controlled - Record every radio call, and then delete it. At any time during a radio call, a recording rule or external API command can cause the recorder to keep the call. • Start on Trigger - Do not record radio calls on this Radio or Talkgroup until a recording rule is triggered or an external API command starts recording. If the recorder is set to Recorder Controlled, recording will start whenever the recorder starts, but audio prior to the recording trigger will be deleted. The interaction starts at the recording trigger, continues to the end of the call.
Overwrite Existing	Select this check box to have existing identical device IDs replaced with new ones created in the range. The new device then assumes the characteristics of the range. If unchecked, the identical device remains with its existing characteristics (such as Recording Mode).

Related topics

[Create a range of devices for radio recording \(page 168\)](#)

Assign radio devices to a member group

Use this procedure to assign the radio devices to a member group. You can assign a range of radio devices, or assign individual devices, to a member group. (When assigning devices created for a Bosch data source, you cannot assign a range of devices to a member group.)

Before you begin

You must have already created devices using either the [Create or edit devices for radio recording \(page 164\)](#) or [Create a range of devices for radio recording \(page 168\)](#) procedure.

You must have already created, or be in the process of creating, a Devices Pool member group for the Radio data source.

Procedure

1. Click **Recording Management > Data Sources > Settings**.
2. Select a Radio data source from the left-hand column.
3. Click **Member Groups**.
4. Click on the Member Group to which you want to assign devices.
5. Click **Edit**.
6. Click **Assign Devices**.
7. In the Assign Devices to Member Group window, click on each device that you want to assign to the member group.

To select multiple devices, hold down the Shift or Ctrl key when selecting the devices. You can also click the **Select All** button to select all devices.



When assigning devices (multicast groups) created for a Bosch Telex data source to a Devices Pool member group, you cannot assign a particular device to more than one member group.

8. Click **Assign Selected**.
9. In the Assign Devices to Member Group window, click **Done**.
10. To verify the devices were assigned to the member group, do the following:
 - a. Click on **Devices** for the Data Source to which the member group belongs.
 - b. On the **Devices** tab, the **Member Groups** column shows the member group to which each device is assigned. Verify the devices were assigned to the correct member group.

Assign or Unassign Devices to Member Group screen reference

The Assign Devices to Member Group screen shows the devices that are not currently assigned to the selected member group.

ASSIGN DEVICES TO MEMBER GROUP: Devices NOT assigned to this pool				Find Device: <input type="text"/> <input type="button" value="Go"/>
Device Number	Device Name	Device Type	Recording Mode	
a10		Radio	Record	
a100		Radio	Record	
a11		Radio	Record	
a12		Radio	Record	
a13		Radio	Record	
a14		Radio	Record	
a15		Radio	Record	
a16		Radio	Record	
a17		Radio	Record	
a18		Radio	Record	
~10		Radio	Record	

Page 1 of 5

The Unassign Devices to Member Group screen shows the devices that are currently assigned to the selected member group.

UNASSIGN DEVICES FROM MEMBER GROUP: Devices assigned to this pool				Find Device:	<input type="text"/>	Go			
Device Number	Device Name	Device Type	Recording Mode						
a151		Radio	Record						
a152		Radio	Record						
a153		Radio	Record						
a154		Radio	Record						
a155		Radio	Record						
a156		Radio	Record						
a157		Radio	Record						
a158		Radio	Record						
a159		Radio	Record						
a160		Radio	Record						
a161		Radio	Record						
a162		Radio	Record						
Page 1 of 3		<input type="button" value="<"/>	<input type="button" value="Page 1"/>	<input type="button" value=">"/>	<input type="button" value="Select All"/>	<input type="button" value="Select None"/>	<input type="button" value="Unassign Selected"/>	<input type="button" value="Unassign Range"/>	<input type="button" value="Done"/>

The screens show these values for each device.

Column	Description
Device Number	The number of an individual device.
Multicast Group IP	This field appears only for devices created for the Bosch Telex data source. In this case, the "device" being created is a multicast group. Specify an IP address that represents a multicast group on the network. The IP address must be unique within a data source. Each multicast group is tied to communication with a specific radio line (or channel). Each channel is associated to a profile (console name or radio name).
Multicast Group Port	This field appears only for devices created for the Bosch Telex data source. In this case, the "device" being created is a multicast group. Specify the port on which the recorder listens for multicast group traffic.
Device Name	The name of an individual device (optional).
Device Type	The Device Type. Possible values are Radio , Talk Group , or Multicast . Talkgroup is a generic term that refers to virtual radio channels created for/by a Trunked Radio System (TRS). All radios in a Talkgroup communicate over a single channel. Only one of the radios can speak on the channel at a time. The recording system can monitor a Talkgroup based on its unique ID (Device ID) and records all communication on that Talkgroup. Multicast indicates the device type is a multicast group. Multicast groups are created for Bosch data sources.

Column	Description
Recording Mode	<p>The supported radio recording modes include:</p> <ul style="list-style-type: none"> • Record - Record all radio calls on this Radio, Talkgroup, or Multicast device type. This is the default setting. • Do Not Record - Do not actively record this Radio or Talkgroup. • Application Controlled - Record every radio call, and then delete it. At any time during a radio call, a recording rule or external API command can cause the recorder to keep the call. • Start on Trigger - Do not record radio calls on this Radio or Talkgroup until a recording rule is triggered or an external API command starts recording. If the recorder is set to Recorder Controlled, recording will start whenever the recorder starts, but audio prior to the recording trigger will be deleted. The interaction starts at the recording trigger, continues to the end of the call.

Related topics

[Create and assign a range of radio devices to a member group \(page 175\)](#)

[Unassign a range of radio devices from a member group \(page 178\)](#)

Devices screen reference

The Devices screen shows all devices that have been created for a data source. The devices screen includes this information.

The screenshot shows the 'RECORDING MANAGEMENT' interface with the 'Devices' tab selected. The top navigation bar includes links for DATA SOURCES, CUSTOM DATA, RECORDING RULES, CAMPAIGNS, and RECORDINGS. Below the navigation is a breadcrumb trail: Settings > Member Groups > Devices > Employees > Import Status. The main content area is titled 'DEVICES: Radio Data Source'. It features a search bar 'Find Device:' with a 'Go' button and a checked checkbox. A table lists devices with columns: Device ID, Device Name, Device Type, Recording Mode, and Member Groups. The table shows multiple entries for 'Radio' devices, all set to 'Record' mode. Two specific entries, 'a2' and 'a21', are grouped under 'Radio recorder member group'. Navigation buttons at the bottom include 'Page 1 of 5', 'Page 1', 'Select All', 'Select None', 'Create', 'Create Range', 'Edit', 'Delete', and 'Delete All'.

Device ID	Device Name	Device Type	Recording Mode	Member Groups
a1		Radio	Record	Radio recorder member group
a10		Radio	Record	
a100		Radio	Record	
a11		Radio	Record	
a12		Radio	Record	
a13		Radio	Record	
a14		Radio	Record	
a15		Radio	Record	
a16		Radio	Record	
a17		Radio	Record	
a18		Radio	Record	
a19		Radio	Record	
a2		Radio	Record	Radio recorder member group
a20		Radio	Record	
a21		Radio	Record	

Column	Description
Device ID	The ID of an individual device.
Device Name	The name of an individual device (optional).
Multicast Group IP	This field appears only for devices created for the Bosch Telex data source. In this case, the "device" being created is a multicast group. Specify an IP address that represents a multicast group on the network. Each multicast group is tied to communication with a specific radio line (or channel). Each channel is associated to a profile (console name or radio name).
Multicast Group Port	This field appears only for devices created for the Bosch Telex data source. In this case, the "device" being created is a multicast group. Specify the port on which the recorder listens for multicast group traffic.
Device Type	<p>These Device Type options are available:</p> <ul style="list-style-type: none"> • Radio • Talkgroup <p>Talkgroup is a generic term that refers to virtual radio channels created for/by a Trunked Radio System (TRS). All radios in a Talkgroup communicate over a single channel. Only one of the radios can speak on the channel at a time. The recording system can monitor a Talkgroup based on its unique ID (Device ID) and records all communication on that Talkgroup.</p> <ul style="list-style-type: none"> • Multicast Group - This device type setting appears when creating devices (or multicast groups) for a Bosch Telex data source. This device type cannot be changed.
Recording Mode	<p>The supported radio recording modes include:</p> <ul style="list-style-type: none"> • Record - Record all radio calls on this Radio, Talkgroup, or Multicast device type. This is the default setting. • Do Not Record - Do not actively record this Radio or Talkgroup. • Application Controlled - Record every radio call, and then delete it. At any time during a radio call, a recording rule or external API command can cause the recorder to keep the call. • Start on Trigger - Do not record radio calls on this Radio or Talkgroup until a recording rule is triggered or an external API command starts recording. If the recorder is set to Recorder Controlled, recording will start whenever the recorder starts, but audio prior to the recording trigger will be deleted. The interaction starts at the recording trigger, continues to the end of the call.
Member Groups	The member groups to which a device is assigned.

Related topics

[Create or edit devices for radio recording \(page 164\)](#)

[Create a range of devices for radio recording \(page 168\)](#)

Create and assign a range of radio devices to a member group

You can create a range (or series) of radio recording device IDs (for either Radios or Talkgroups) and assign those device IDs to a Devices Pool member group.

A device range can consist of up to 5000 devices.

You can include prefixes or postfixes for each device in the range.

Before you begin

You must have already created, or be in the process of creating, a Devices Pool member group for the radio data source.

Procedure

1. Click **Recording Management > Data Sources > Settings**.
2. In the left-hand pane, select the Radio data source that contains the Devices Pool member group for which you want to create and assign a range of devices.
3. Click **Member Groups**.
4. Click on the member group for which you want to create and assign devices.
5. Click **Edit**.
6. Click **Assign & Create** Devices.
7. In the Assign Devices to Member Group window, click **Assign Range**.
8. In the Assign Device Range screen, complete the fields to create the range of devices you want to assign to the member group. See the related topics for more information on the fields in the Assign Device Range screen.
9. Click **Assign**.
10. In the Assign Devices to Member Group window, click **Done**.
11. To verify the devices were assigned to the member group, do the following:
 - a. Click on **Devices** for the data source to which the member group belongs.
 - b. On the **Devices** screen, the **Member Groups** column shows the member groups to which each device is assigned. Verify the devices were assigned to the correct member group.

Related topics

[Assign Device Range screen reference \(page 175\)](#)

Assign Device Range screen reference

The Assign Device Range screen contains these settings. Use this screen to create and assign a range of radio Device IDs to a member group.

ASSIGN DEVICE RANGE: To Pool 'Radio recorder member group 2'

Device Details	
Prefix	<input type="text"/>
Device Range	<input type="text"/>
Postfix	<input type="text"/>
Device Type	Radio
Recording Mode	Record
Overwrite Existing	<input type="checkbox"/>
<input type="button" value="Assign"/> <input type="button" value="Cancel"/> <input type="button" value="Revert"/>	

Setting	Description
Prefix	Type any digit or letter that will precede the device number, such as X.
Device Range	<p>Type the device number range, such as 1-100.</p> <ul style="list-style-type: none"> To create a sequential range of devices, use a hyphen to separate the start number from the end number. For example, entering 1-50 creates a range of 50 devices beginning with device 1 and ending with device 50. You can also combine a sequential range of devices with individual devices. For example, you can enter 1-10, 20, 25-35. This device range includes devices 1 through 10, the individual device numbered 20, and devices 25 through 35. In this case separate multiple entries with a comma. Device numbers entered as a range in this text box must consist only of numeric characters. For example, a device range of 1a-100a or 1*-100* is not valid. (You can, however, enter non-numeric characters in the Prefix and Postfix fields.) Any single device number in a range of device numbers cannot exceed 20 digits.
Postfix	Type a digit or letter that will appear after the device number.
Device Type	<p>Select Radio to create a range of Radio Device IDs, or select Talkgroup to create a range of Talkgroup device IDs.</p> <p>Talkgroup is a generic term that refers to virtual radio channels created for/by a Trunked Radio System (TRS). All radios in a Talkgroup communicate over a single channel. Only one of the radios can speak on the channel at a time. The recording system can monitor a Talkgroup based on its unique ID (Device ID) and records all communication on that Talkgroup.</p>

Setting	Description
Recording Mode	<p>The supported radio recording modes include:</p> <ul style="list-style-type: none"> • Record - Record all radio calls on this Radio, Talkgroup, or Multicast device type. This is the default setting. • Do Not Record - Do not actively record this Radio or Talkgroup. • Application Controlled - Record every radio call, and then delete it. At any time during a radio call, a recording rule or external API command can cause the recorder to keep the call. • Start on Trigger - Do not record radio calls on this Radio or Talkgroup until a recording rule is triggered or an external API command starts recording. If the recorder is set to Recorder Controlled, recording will start whenever the recorder starts, but audio prior to the recording trigger will be deleted. The interaction starts at the recording trigger, continues to the end of the call.
Overwrite Existing	Select this check box to have existing identical device IDs replaced with new ones created in the range. The new device then assumes the characteristics of the range. If unchecked, the identical device remains with its existing characteristics (such as Recording Mode).

Related topics

[Create and assign a range of radio devices to a member group \(page 175\)](#)

Unassign individual radio devices from a member group

You can unassign individual, or all, radio devices from a member group.

Procedure

1. Click **Recording Management > Data Sources > Settings**.
2. In the left-hand pane, select the data source that contains the member group from which you want to unassign devices.
3. Click **Member Groups**.
4. Click on the member group from which you want to unassign devices.
5. Click **Edit**.
6. Click **Unassign Devices**.
7. Click on the devices you want to unassign.
 - To select multiple devices, press the Ctrl or Shift key and click on the devices.
 - To select all devices, click **Select All**.
8. Click **Unassign Selected**.
9. Click **Done**.

Related topics

[Assign or Unassign Devices to Member Group screen reference \(page 171\)](#)

Unassign a range of radio devices from a member group

You can unassign a range (or series) of radio devices from a member group.

Procedure

1. Click **Recording Management > Data Sources > Settings**.
2. In the left pane, select the Radio Data Source that contains the member group from which you want to unassign a range of devices.
3. Click **Member Group**.
4. Click on the member group from which you want to unassign a range of devices.
5. Click **Edit**.
6. Click **Unassign Devices**.
7. Click **Unassign Range**.
8. In the Unassign Devices screen, specify the range of devices you want to unassign from the member group. See the related topics for help on individual fields in the Unassign Devices screen.
9. Click **Unassign**.
10. Click **Done**.

Related topics

[Unassign a range of devices screen reference \(page 178\)](#)

[Assign or Unassign Devices to Member Group screen reference \(page 171\)](#)

Unassign a range of devices screen reference

Use the Unassign Devices screen to unassign a range of devices from a member group.

The screenshot shows the 'UNASSIGN DEVICES' screen. At the top, it says 'From IP Pool 'Radio recorder member group''. Below that is a 'Device Details' section with three input fields: 'Prefix' (containing 'a'), 'Device Range' (containing '1-10'), and 'Postfix'. At the bottom right are three buttons: 'Unassign', 'Cancel', and 'Revert'.

The Unassign Devices screen contains these fields.

Field	Description
Prefix	Type the digit or letter that precedes the device numbers to be unassigned (if applicable).
DeviceRange	Type a device range, such as 1-10. <ul style="list-style-type: none">• To enter a sequential range of devices, use a hyphen to separate the start number from the end number. For example, entering 1-10 unassigns a range of devices beginning with device 1 and ending with device 10.• You can also combine a sequential range of devices with individual devices. For example, you can enter 1-10, 20, 25-50. This device range entry unassigns devices 1 through 10, the individual device 20, and devices 25 through 50. In this case, separate each of the entries with a comma.
Postfix	Type the digit or letter that follows the device numbers to be unassigned (if applicable).

Related topics

[Unassign a range of radio devices from a member group \(page 178\)](#)

Set up for Ingestion Recording

You must set up ingestion recording to have face-to-face recordings uploaded to the recorder, or to use the Recorder Ingestion API.

Ingestion recording requirements

- All application servers must have the Recorder Data Center API role enabled.
- At least one recorder has the Recorder Ingestion Web Service role enabled and the call buffer, licensing, and archiving configured.

The Recorder Ingestion API balances requests across all available Recorder Ingestion Service recorders. It is recommended that these recorders be geographically local with the applications servers.

- The Interaction Data Platform license is enabled.
- If agent resolution is used on ingestion, employees must be configured with a pbx_login_id assigned to a data source that matches the value to be ingested.

Related topics

[Set up voice and video recording \(page 49\)](#)

Related information

Server roles (*Enterprise Manager Configuration and Administration Guide*)

Recorder Ingestion API (*SDK Programmers Guide*)

Face to face recorder (*Face to Face Interaction Recorder Installation and Configuration Guide*)

Set up individual Recorders

This section describes how to use Recorder Manager to set up individual Recorders.

Topics

Recorder configuration workflow	182
Configure database settings	194
TDM recording setup	198
Voice cards and channels	230
IP Recorder and IP Recorder Video configuration	240
IP Analyzer configuration	254
Backup and recover for recorder configuration	262
Start and stop Recorder components	265

Recorder configuration workflow

Use the following procedure to guide you through configuration of an individual Recorder.

Workflow sequence

- [Workflow: IP-based voice and video recording \(page 33\)](#): Task 6 of 8
- [Workflow: Screen recording \(page 38\)](#): Task 5 of 7
- [Workflow: Integrate Dialer integration \(page 39\)](#): Task 6 of 7

Task List

1. The following sections describe configuration tasks that are common to setting up both IP and TDM Recording:
 - [Recorder setup \(page 184\)](#)
 - [Call buffer setup \(page 187\)](#)
 - [Configure compression \(page 188\)](#)
 - [Disk manager setup \(page 191\)](#)
2. Configure your database settings, as described in [Configure database settings \(page 194\)](#).
3. Once you have completed the tasks above, proceed to one of the following, depending on your recording type:
 - [IP Recorder and IP Recorder Video configuration \(page 240\)](#)
 - [TDM recording setup \(page 198\)](#)
4. Once the Recorder is set up, check the alarms.



If you rollback your Recorder from Version 15.2 to 11.1, calls recorded on the Version 15.2 Recorder will not be supported by the 11.1 Recorder for replay, workflow rebuild, or consolidation.

What to do next

Voice recording: [Attributes configuration workflow \(page 270\)](#)

Screen recording: [Recording rules configuration workflow \(page 303\)](#)

Dialer integration: [Install and configure Archive \(page 41\)](#)

Related topics

[View active alarms \(page 515\)](#)

Launch Recorder Manager

Launch from Enterprise Manager

You can launch the Recorder Manager from Enterprise Manager by selecting a recorder under **System Management > Settings**, in the **Installations** panel, then clicking **Launch**. Select **Recorder Manager** if the **Application Type** window appears. You will not need to type the user name and password again.

Launch from the Desktop

The computer on which the Recorder Manager was installed will have a launch icon on the desktop. Double-click this icon to launch Recorder Manager on a local computer.

Initial setup

When you access the Recorder Manager for the first time, you will be prompted to enter the Call Path Buffer (for example, D:\Calls). The call buffer is the disk storage area (also known as the calls cache) where contacts are saved when first recorded. As the call buffer fills up, contacts are copied automatically to more permanent storage, depending on your threshold and archive settings. The Disk Manager begins deleting the oldest contacts from the call buffer once a specified disk threshold is reached.

Related topics

[Getting started with recorders \(page 26\)](#)

Recorder setup

This section describes configuration tasks that are required whether you are setting up IP or TDM recording:

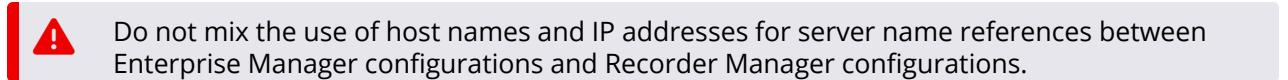
- [Configure Recorder settings \(page 184\)](#)
- [Configure compression \(page 188\)](#)
- [Disk manager setup \(page 191\)](#)

Related topics

[Standardize server name references \(page 184\)](#)

Standardize server name references

If you have upgraded from a previous version, it is essential that you standardize the use of server name references between the Enterprise Manager and the Recorder Manager. Verify that servers are referenced by either host name or IP address in all cases.



If you have a server name defined as an IP address in Enterprise Manager, and then defined as a host name in Recorder Manager, operations such as archiving will fail after the upgrade.

Related topics

[Configure Recorder settings \(page 184\)](#)

[Recorder setup \(page 184\)](#)

Configure Recorder settings

Procedure

1. Under **General Setup > Recorder Settings**, specify a **Call Path Buffer**. The call buffer is the disk storage area (also known as the calls cache) where contacts are saved when first recorded. As the call buffer fills up, contacts are copied automatically to more permanent storage, depending on your threshold and archive settings. The Disk Manager begins deleting the oldest contacts from the call buffer once a specified disk threshold is reached.

If you are setting up a Centralized Analytics Server, you must still configure a Call Path Buffer, even though no Recorder roles will be enabled. This buffer will store files produced when Analytics is run against a campaign, which are used to update the database records of calls that have been processed.



It is strongly recommended that the call buffer be located on a different drive from system files. If you later change the location of the call buffer, refer to [Relocate the call buffer \(page 187\)](#), otherwise the Interactions application will not be able to find and replay some calls.

The screenshot shows the 'RECODER SETTINGS' screen with the following details:

- Recorder Settings:** Recorder settings that are used across all the Recorder components.
- Call Path Buffer:** C:\Calls
- Hostname:** VM-ANN-08
- Serial Number:** 404001
- Audio Recordings:**
 - IP Channel Count: 100
 - TDM Channel Count: 100
- Screen Recordings:**
 - Maximum Number Of Channels: 100
 - Maximum Record Time (Seconds): 3600
- Video Recordings:**
 - Video Channel Count: 50
 - Maximum Record Time (Seconds): 360
- Call Security Settings:**
 - Fingerprint Recordings:

Buttons at the bottom right: Save, Revert.

2. View the **Audio Recordings** settings as noted below:

- **IP Channel Count** - Displays the number of configured voice channels allocated to the IP Recorder server role on the server. This field displays only if an IP Recorder server role is activated on the server. If this field specifies zero, the IP Recorder does not record any calls.
- **TDM Channel Count** - Displays the number of configured voice channels allocated to the TDM Recorder server role on the server. This field displays only if a TDM Recorder server role is activated on the server. If this field specifies zero, the TDM Recorder does not record any calls. You allocate configured voice channels to the IP Recorder and TDM Recorder server roles from the **System Management > License Management > Recording Channels** screen of the enterprise portal.

3. View or change the **Screen Recordings** settings as noted below:

- **Maximum Number of Channels** - Displays the number of configured screen channels allocated to the Screen recorder server role on the server. This field displays only if the Screen Recorder server role is activated on the server. If this field specifies zero, the Screen Recorder does not record any screen activity.

You allocate configured screen channels to the Screen Recorder server role from the **System Management > License Management > Recording Channels** screen of the enterprise portal.

- **Maximum Record Time (Seconds)** - Specify the maximum amount of time allowed for the recording of screens. The setting limits the duration of a single screen Segment/INUM. The default and maximum setting is 3600 seconds. The minimum setting is 300 seconds.
4. View the **Video Recording** settings, as noted below:
- **Video Channel Count** - Displays the number of configured video channels allocated to the IP Recorder Video server role on the server. This field displays only if the IP Recorder Video server role is activated on the server. If this field specifies zero, the IP Recorder Video does not record any video calls.
- You allocate configured video channels to the IP Recorder Video server role from the **System Management > License Management > Recording Channels** screen of the enterprise portal.
- **Maximum Record Time (Seconds)** - Displays the maximum amount of time allowed for a single video recording. If a video recording for an interaction reaches the time limit then recording continues as a new interaction. This value is configured in the enterprise portal from the **System Management > Enterprise > Settings** screen for the IP Recorder Video server role. The default setting is 180 seconds. The minimum setting is 60 seconds and the maximum setting is 3600 seconds.
5. Configure the **Call Security Settings** as noted below:
- **Fingerprint Recordings** - Select this check box to have a checksum string inserted into .wav (for voice), .scn (for screen), or .mp4 (for video) files, allowing the detection and reporting of mismatched files.
6. Click **Save**.

Related topics

[Standardize server name references \(page 184\)](#)

[Recorder setup \(page 184\)](#)

Call buffer setup

Set up the call buffer to specify the hard disk space where contacts are stored after being recorded initially.



The call buffer cannot be located on a remote SAN or on a remote server.

Related topics

[Relocate the call buffer \(page 187\)](#)

[Create a new call buffer location \(page 188\)](#)

Relocate the call buffer

You can use the following procedure to change the hard disk location for recorded contacts specified during installation, porting existing files to the call buffer.



Plan to perform all the following tasks outside business hours.

To change the call buffer location

Change the call buffer location to move all files in the old call buffer into a new location.

1. Click **Operations > Start and Stop**. Select all Recorder components except the Web Service (if present) and click **Stop**.

The screenshot shows the Recorder Operations interface with the 'OPERATIONS' tab selected. The main area displays a table titled 'COMPONENT SERVICES: List of Component Services and Status on PTECON1'. The table has columns for 'Component Name', 'Status', and 'Startup Type'. Most components are listed as 'Started' with 'Automatic' startup type, except for 'Recorder Tomcat(Restart Only)' which is also started. At the bottom of the table are buttons for 'Select All', 'Select None', 'Edit', 'Start', 'Stop', 'Restart', and 'Reboot'.

Component Name	Status	Startup Type
Recorder Agent Server	Started	Automatic
Recorder Alarm Service	Started	Automatic
Recorder Archiver Service	Started	Automatic
Recorder Compressor Service	Started	Automatic
Recorder Consolidator Service	Started	Automatic
Recorder Content Server	Started	Automatic
Recorder DiskManager Service	Started	Automatic
Recorder Integration Service	Started	Automatic
Recorder IP CaptureEngine	Started	Automatic
Recorder Redundancy Controller	Started	Automatic
Recorder Screen CaptureEngine	Started	Automatic
Recorder Tomcat(Restart Only)	Started	Automatic
Recorder Workflow Service	Started	Automatic
WatchDog	Started	Automatic

2. Launch Windows Explorer and create a new call buffer directory on the local machine.



The call buffer cannot be located on a remote SAN or on a remote server.

3. In Windows Explorer, move all files and subfolders from the old call buffer folder to the new call buffer folder.
4. Click **General Setup > Recorder Settings** and change the **Call Path Buffer** to point to the one created in Step 2.
5. Click **Save**.
6. Click **Operations > Start and Stop**, select all stopped components, and click **Start**.

Related topics

[Call buffer setup \(page 187\)](#)

[Create a new call buffer location \(page 188\)](#)

Create a new call buffer location

Assign a new call buffer location to retain files in the old call buffer while using a new call buffer working location. This would be necessary if copying the content from the existing call buffer to the new call buffer is not possible.



If you assign a new call buffer location you cannot replay the contacts recorded and stored in the old call buffer location, although the contacts are still present. You may not be able to play back those contacts, unless they have already been archived.

Procedure

1. Choose **Operations > Start and Stop** and stop the Capture engine.
2. Choose **Operations > Start and Stop** again, then stop all other Recorder components, except the Web Service (if present).
3. Create the new call buffer as described in [To change the call buffer location \(page 187\)](#).
4. Change the call buffer directory using Recorder Manager as described in [Configure Recorder settings \(page 184\)](#) to point to the new call buffer
5. Choose **Operations > Start and Stop** to restart all the components.

Configure compression

Compression takes place for all audio input formats except G723.1 (5.3K), and G729A. Compression is not applicable to IP video recording.

G.711 is not supported above 1000 channels.

Audio recording in G.722 format is supported, however it cannot be replayed until it is transcoded into a different format. Use the following procedures to specify the audio compression type for the compression of recordings.



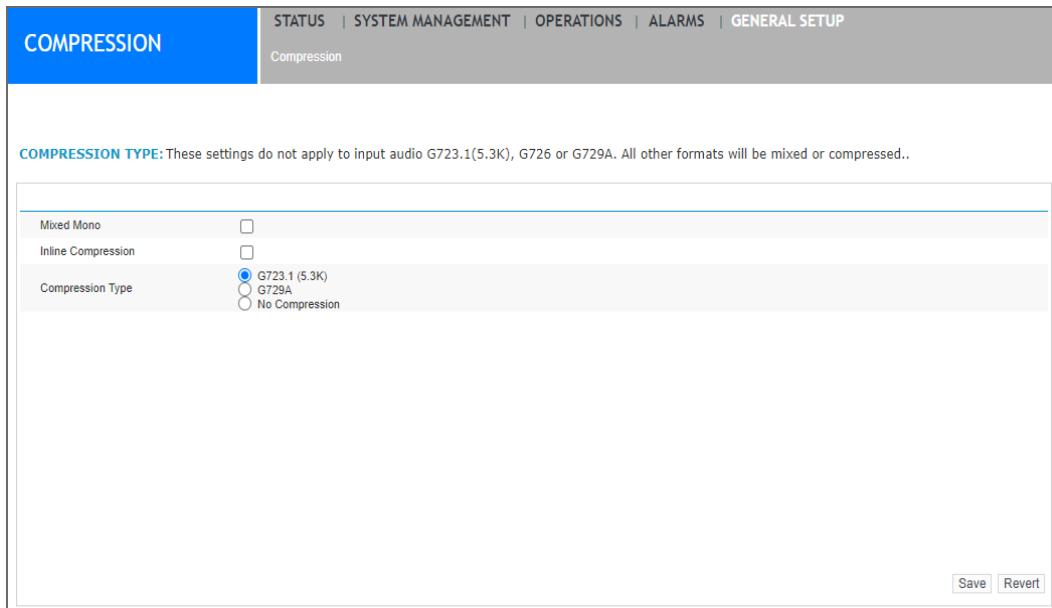
Only uncompressed audio formats will undergo further compression.



Upgrades to version 11 will maintain established compression settings, but new installations will have mixing “off” and G.723.1 (5.3 K) enabled by default.

Procedure

- Under **General Setup > Compression**.



- Specify the type of compression you want, from the following options (all possible combinations will be valid).



Stereo files are produced by IP Recorders if the input audio is stereo (all Interception systems and most Delivery systems), and either the input audio is already compressed, or mixing is disabled. Mono files are produced by all TDM Recorders. Mono files are produced by IP Recorders if either the input format is G.711 or G.722 and mixing is enabled, or (in some Delivery mode systems) the VoIP system mixes the audio before it is delivered to the Recorder. The compression type does not affect whether files are mono or stereo.

Item	Description
Mixed Mono	Select this check box to enable mixing (applies to IP only). This mode mixes one stereo audio file into one mono audio file to save disk space. For G.711 and G.722, it is recommended that files are not mixed. <ul style="list-style-type: none"> • enabling mixing produces one stereo energy file in the format .ene. The audio will be a single mono file. • switching mixing off produces one stereo audio file.

Item	Description
Inline Compression	This setting must always be enabled. The ability to turn this off has been deprecated and is no longer supported in the product. It will be removed in a future version of the product.
Compression Type	
G.723.1 (5.3 K)	This is the recommended audio format. Choose this option to convert audio from the original format to G.723.1 (5.3 K).

See the *Performance and Sizing Guide* for the audio file sizes produced by the settings above.

3. Click **Save**.

Related topics

[Getting started with recorders \(page 26\)](#)

Disk manager setup

Configure the disk manager component to assign call buffer disk settings and logical drives to the contact recording environment. The call buffer, also known as the calls cache, is the local disk space where the contact being recorded is stored. Once on the call buffer, the location of the contact is registered for later search and replay.

Related topics

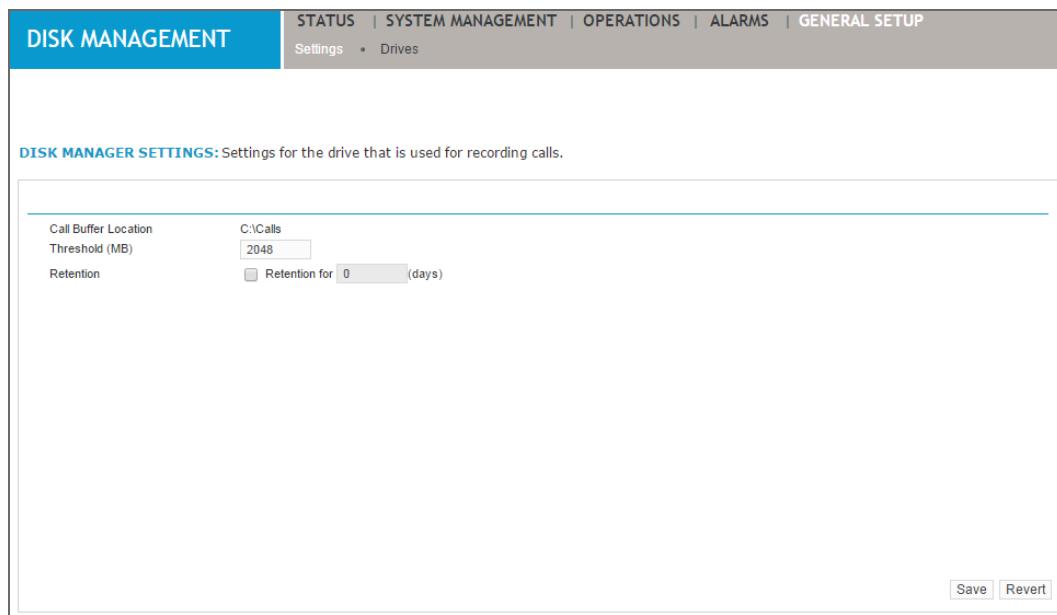
[Monitor disk drives \(page 192\)](#)

Configure disk manager

Use the disk manager settings page to assign drives, folders, and capacity thresholds for the recording of contact details on the local call buffer. Recorded contacts are stored temporarily in the call buffer until the specified disk threshold is reached. Contacts must be archived prior to deletion here, otherwise they are lost (see the *Archive Administration Guide*).

Procedure

1. Click **General Setup > Disk Management > Settings**.



2. Complete the following fields:

- **Threshold (MB)**—Type a size in megabytes for free disk space on the call buffer. Generally, the threshold should be set at 10 percent or 10 GB, whichever is higher, so that amount of hard disk space is always free. This provides a tolerance level for Disk Manager to delete contacts during high-volume recording, when the Call Buffer can fill up faster than contacts can be deleted.



The threshold recommendation for the disk manager in V15.2 accounts for text and video recordings that were not supported in previous releases.

- **Retention**—Select the check box, then type the number of days for which calls should be retained in the Call Buffer. For example, if you want calls to be deleted after 90 days, select the check box and then type 90 in the field. If the disk reaches the threshold calls will be deleted regardless of the retention setting.

3. Click **Save**.

Related topics

[Monitor disk drives \(page 192\)](#)

Monitor disk drives

The Drives screen lists drives managed by disk manager. You can also view thresholds for any alarms (to be triggered, for example, if a drive is running low on space).

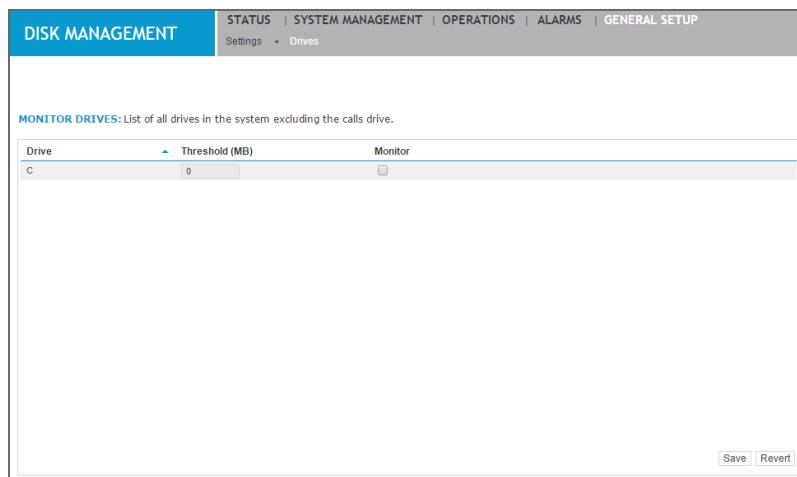


Only one of the listed drives contains the call buffer. The call buffer drive is the only drive from which the disk manager deletes old files. Generally, the threshold should be set at 10 percent or 10 GB, whichever is higher, so that amount of hard disk space is always free.

The threshold recommendation for the disk manager in V15.2 accounts for text and video recordings that were not supported in previous releases.

Procedure

1. Click **General Setup > Disk Management > Drives**.



2. To monitor a drive, select the **Monitor** check box. An alarm is raised when the threshold is reached (enter a value for the **Threshold** as well).
3. Type a threshold (in megabytes) for each drive. When disk space on the drive reaches the threshold size, it triggers an alarm. (Optional.) To edit this field, you must enable the **Monitor**

option.

4. Click **Save**.

Related topics

[Configure disk manager \(page 191\)](#)

Configure database settings

The database settings area provides configuration settings for the connection to the Contact Database Service and the Text Analytics Services.

Related topics

[View database settings \(page 194\)](#)

[Edit a contact database or text analytics database \(page 195\)](#)

[Reprocess call date ranges \(page 196\)](#)

View database settings

Use the following procedure to view database settings.

Procedure

1. Click **General Setup > Databases > Database Settings**.

The screenshot shows the 'Database Settings' page under 'General Setup'. The top navigation bar includes links for STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP. Below the navigation is a sub-header 'Database Settings'. The main content area is titled 'CONFIGURE DATABASES ACCESS: List of all the databases.' It features a table with the following data:

Server Name	Additional Information	Reprocessing	Type
10.165.164.235	N/A	No	Text Analytics Services
cou-raf-con	HTTP Port : 80 HTTPS(SSL) Port : 443	No	Contact Database Service

At the bottom of the page are buttons for 'Edit', 'Start Reprocessing', and 'Stop Reprocessing'. There is also a 'Refresh Rate' dropdown set to '1 Minute' with a refresh icon.

2. Review the following fields:

Field	Description
Server Name	Shows the name of the database server. This name must be unique.
Additional Information	Shows information such as whether this is the Text Analytics database, Calls database and whether it is the Site database (in a Site with Centralized Archiving enabled).

Field	Description
Reprocessing	Shows whether or not one of the following is being reprocessed: <ul style="list-style-type: none"> • Contact database calls • Text Analytics database calls and content For additional information about reprocessing, see Reprocess call date ranges (page 196) .
Type	Shows the type of access: <ul style="list-style-type: none"> • Contact Database Service • Text Analytics Services

3. From this screen you may click **Start Reprocessing** or **Stop Reprocessing** to start or stop the re-upload of call metadata or call metadata and content to the target database, as described in [Reprocess call date ranges \(page 196\)](#).
4. You may also select a database and click **Edit** to make changes to certain settings.

Related topics

[Configure database settings \(page 194\)](#)

[Edit a contact database or text analytics database \(page 195\)](#)

[Reprocess call date ranges \(page 196\)](#)

Edit a contact database or text analytics database

1. Click **General Setup > Databases > Database Settings**.
2. Select Contact Database or Text Analytics, then click **Edit**.
3. Edit the following fields as necessary:

Contact Database fields

Item	Description
Contact Database Service	Read-only name of the database.
Consolidate	Select this check box to allow local and centralized archiving components to archive media information to a single database.
HTTP Port	The port number used by the database to communicate with the Recorder.
HTTPS (TLS)	The default port for TLS communication.
Watermark	The watermark indicates the date and time at which archiving will begin in the next cycle. Select either Do not change the current value or Change the current value to (and then select a date and time).



The Server name, non-TLS port, and TLS port entries are validated by establishing a test connection to the target web service. If unable to connect to the web service, a message advises that the information is invalid.

Text Analytics database fields

Item	Description
Text Analytics Services	Read-only name of the database.
Watermark	The watermark indicates the date and time at which archiving will begin in the next cycle. Select either Do not change the current value or Change the current value to (and then select a date and time).



The Server name is validated by establishing a test connection to the target web service. If unable to connect to the web service, a message advises that the information is invalid.

- Click **Save**, and when prompted, restart the Recorder.

Related topics

[Configure database settings \(page 194\)](#)

[View database settings \(page 194\)](#)

[Reprocess call date ranges \(page 196\)](#)

Reprocess call date ranges

Use the following procedure to reprocess Contact database call date ranges or Text Analytics database call and content date ranges to allow the Recorder to re-execute their tasks on an older set of calls and content specified by date range.

Please note the following:

- Reprocessing should not be performed during normal operation and should not be done without consulting support.
- Centralized Archiving drives do not support the reprocessing feature. (You should use a modified campaign in this instance.)
- For Archive drives only:
 - The archive drive status must be Ready or Writing before beginning reprocessing. If the state is Empty, Faulty, Unknown, Full, Replay, or Reconstructing, you cannot reprocess.
 - The Archive drive status page that already shows the last archived Inum continues to track the last archived Inum while reprocessing.
- You must have “View Workflow Configuration” privileges to use the Start Reprocessing and Stop Reprocessing functions.

Procedure

1. Click **General Setup > Databases > Database Settings**.

The screenshot shows the 'Database Settings' page under 'GENERAL SETUP'. At the top, there are tabs for STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP. Below the tabs, it says 'Database Settings'. A sub-header 'CONFIGURE DATABASES ACCESS: List of all the databases.' is followed by a table. The table has columns: Server Name, Additional Information, Reprocessing, and Type. There are two entries:

Server Name	Additional Information	Reprocessing	Type
10.165.164.235	N/A	No	Text Analytics Services
cou-raf-con	HTTP Port : 80 HTTPS(SSL) Port : 443	No	Contact Database Service

Below the table are buttons for Edit, Start Reprocessing, and Stop Reprocessing. To the right of the table, there is a 'Refresh Rate:' dropdown set to '1 Minute' with a refresh icon.

2. Select a database and click **Start Reprocessing**.
3. Type a start and end date and time to be the date range, observing the following:
 - Date and time formats are automatically converted to the proper format according to local convention. You can also click the Calendar icon (circled) to display a visual representation of dates.
 - The date range indicates the approximate beginning and ending range of call times that will be reprocessed.
 - The start date must always be earlier than the end date.
 - All dates and times are specified in the user's local time zone.
4. Click **Start**. Reprocessing begins. If you attempt to start reprocessing again on a database or Archive drive that is already reprocessing, an error message appears.
5. Click **Stop Reprocessing** to interrupt reprocessing. The target Consolidator database or Archive drive will return to its original progress point before the reprocessing operation began and continue from there.

Related topics

[Configure database settings \(page 194\)](#)

[Edit a contact database or text analytics database \(page 195\)](#)

TDM recording setup

Follow the procedures in this chapter to configure the voice cards for TDM Recording. Voice cards capture the audio portion of calls and forward this information to other components for further processing.



Voice card configuration includes a Maximum Record Time — note that this setting applies only to Audio Recording.

Related topics

- [Supported voice cards \(page 198\)](#)
- [Configure DP voice cards \(page 201\)](#)
- [Configure PCM32 voice cards \(page 205\)](#)
- [Configure DT voice cards \(page 208\)](#)
- [Configure NGX voice cards \(page 213\)](#)
- [Configure LD voice cards \(page 217\)](#)
- [Voice cards and channels \(page 230\)](#)
- [TDM voice card reference \(page 219\)](#)

Supported voice cards

The following voice cards are compatible with the Recorder.



Note the following:

- NGX 800 appears in Windows Device Manager regardless of NGX card model
- -eh refers to PCI express card versions

Analog station side

Ai-Logix model	Description
LD409	Ai-Logix's analog station-side recording voice cards capable of recording 4, 8, 16, and 24 ports respectively.
LD409-eh	
LD809	
LD809-eh	
LD1609	
LD1609-eh	
LD2409	
LD2409-eh	

Digital station side

Ai-Logix model	Description
NGX800 NGX800-eh	Voice card that records eight 2-wire digital phones or four 4-wire digital phones. It is triggered by D-channel events. It can have up to two MX80 daughterboards attached.
NGX1600 NGX1600-eh	Voice card that records sixteen 2-wire digital phone or eight 4-wire digital phones. It is triggered by D-channel events. It can have one MX80 daughterboard attached.
NGX2400 NGX2400-eh	Voice card that records twenty-four 2-wire digital phones or twelve 4-wire digital phones triggered by D-channel events.
MX80	Daughterboard that can be installed on NGX800 and NGX1600 voice cards. This board adds capacity of eight 2-wire digital phones or four 4-wire digital phones.

Digital trunk side

Ai-Logix model	Description
DP3209 DP3209-eh DP6409 DP6409-eh	<p>Voice cards for T1/E1 trunk interception recording. Models are based on the DP3209 (single trunk-span) and the DP6409 (dual trunk-span). Cards are software switchable between E1 and T1 trunk spans.</p> <ul style="list-style-type: none"> • DP3209 model: records 30/24 channels (E1/T1 respectively). • DP6409 model: records 60/48 channels (E1/T1 respectively). • Twisted pair cable terminated with RJ-45 connectors.
PCM3209 PCM3209-eh PCM6409 PCM6409-eh	<p>Voice cards for PCM interception recording. Models are based on the PCM3209 (single trunk-span) and the PCM6409 (dual trunk-span).</p> <ul style="list-style-type: none"> • PCM3209 model: records 32 channels. • PCM6409 model: records 64 channels. • Twisted pair cable terminated with RJ-45 connectors.
DT3209TE DT3209TE-eh DT6409TE DT6409TE-eh	<p>Voice cards for delivery recording. Models are based on the DT3209, which is a single trunk-span card, and the DT6409, which is a dual trunk-span card.</p> <ul style="list-style-type: none"> • DT3209TE model: records 30/24 channels (E1/T1 respectively). • DT6409TE model: records 60/48 channels (E1/T1 respectively). • Twisted pair cable terminated with RJ-45 connectors.

Related topics

- [TDM recording setup \(page 198\)](#)
- [Manage voice cards \(page 230\)](#)
- [Configure voice card channels \(page 236\)](#)

Configure DP voice cards

Configure DP voice cards, including card properties, trunks, and channels, using the procedures in this section.

Related topics

[Supported voice cards \(page 198\)](#)

[Modify DP voice card properties \(page 201\)](#)

[Update DP voice card channels \(page 202\)](#)

[Modify the trunk protocol on a T1 voice card \(page 204\)](#)

[Modify the trunk protocol on an E1 voice card \(page 204\)](#)

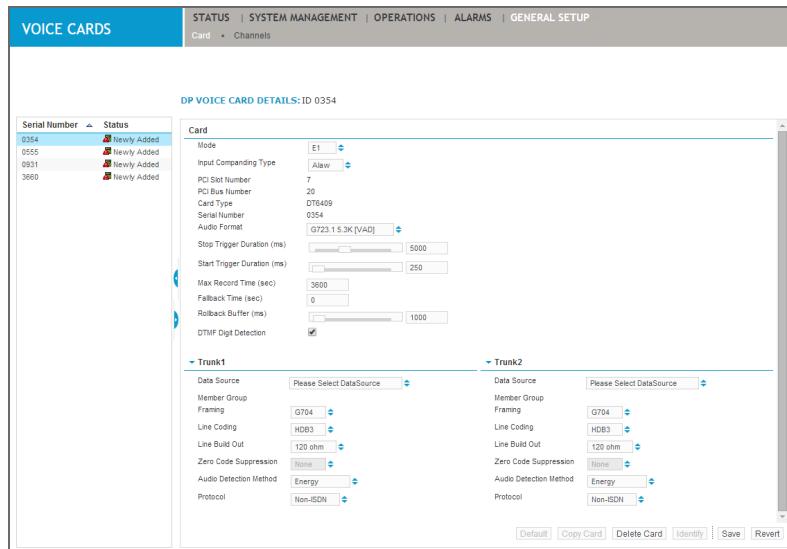
[TDM voice card reference \(page 219\)](#)

Modify DP voice card properties

Use the following procedure to modify the properties of a DP voice card.

Procedure

1. Click **General Setup > Voice Cards > Card**.
2. Select a DP voice card with a status of **Existing** or **Newly Added**.



3. Edit the **Card** properties, as required. Note that some fields you cannot edit.
4. Edit the properties for each trunk.
5. Click **Channels** to configure the channels associated with this card.
6. Do one of the following:

- Click **Save** to complete your changes.
If prompted to restart the Recorder, go to **Operations > Start and Stop > Reboot**. Your changes take effect after the restart.
- Click **Revert** to undo any changes and return to the original settings.

Related topics

[Update DP voice card channels \(page 202\)](#)

[TDM voice card properties reference \(page 219\)](#)

[TDM voice card channel properties reference \(page 225\)](#)

[Configure voice card channels \(page 236\)](#)

Update DP voice card channels

Update channels on the DP voice card to enable individual channels and modify associated recording settings. Channel IDs are created automatically.

The number of channels available depends on the selection of T1 or E1 in the card properties.

- T1 has 23 Channels when configured as a PRI/ISDN and 24 channels when configured as Robbed Bit Signaling (RBS).
- E1 has 30 channels for both ISDN and CAS.

Procedure

- Click **General Setup > Voice Cards** and select a DP card.
- Click **Channels**.

CHANNEL LICENSES AVAILABLE: Channels Configured = 0, Concurrent licenses available = 50

Enabled	Channel #	Channel Name	Channel ID	Monitor Failures	Energy Detect Level	Start On Tap	Stop On Tap	Report Tap Events	AGC
<input checked="" type="checkbox"/>	1		1	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	2		2	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	3		3	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	4		4	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	5		5	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	6		6	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	7		7	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	8		8	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	9		9	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	10		10	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	11		11	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	12		12	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	13		13	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	14		14	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	15		15	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	16		16	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	17		17	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	18		18	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	19		19	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	20		20	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	21		21	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	22		22	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	23		23	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	24		24	<input type="checkbox"/>	-45	Always	Always	Yes	No
<input checked="" type="checkbox"/>	25		25	<input type="checkbox"/>	-45	Always	Always	Yes	No

Select All | Select None | Save | Revert | Configure | Edit Tags | Copy Card

3. Select a channel, and then click **Configure**.

CHANNEL INFORMATION: Channel # : 9, Card Type : DP3209, Serial # : 200

Hardware

Enabled	Yes
Monitor Failures	No
Energy Detect Level (dB)	-45
Start On Tap	InFallBack
Stop On Tap	InFallBack
Report Tap Events	Yes
Automatic Gain Control / AGC	No
Digital Input Gain	0

Channel Identifier

Channel Name	
--------------	--

Set **Default** **Cancel**



To edit multiple channel names at one time, select the channels and click **Edit Tags**. See related topics (below) to learn about configuring channels.

4. Complete the **Hardware** and **Channel Identifier** settings, as required. See related topics (below) to learn about channel properties.
5. Do one of the following:
 - Click **Set** to complete your changes.
 - Click **Default** to undo any changes and return to the default settings.
 - Click **Cancel** to undo any changes and return to the last saved settings.

Related topics

[Modify the trunk protocol on a T1 voice card \(page 204\)](#)

[Modify the trunk protocol on an E1 voice card \(page 204\)](#)

[TDM voice card channel properties reference \(page 225\)](#)

[Configure voice card channels \(page 236\)](#)

Modify the trunk protocol on a T1 voice card

Modify the trunk protocol in a T1 voice card to determine the signalling variant, and therefore the number of channels available, to be used as a line protocol.

Procedure

1. Click **General Setup > Voice Cards > Card**.
2. Select a T1 voice card with a status of **Existing**.
3. In the **Trunk** pane, select the required protocol. Refer to the related topics (below) to learn more about T1 protocols.
4. Click **Channels** to view the number of channels available after the update.
If you have exceeded the number of licensed channels, an alarm triggered as the license limit is approaching will indicate this, and you must obtain additional licenses.
5. Do one of the following:
 - Click **Save** to complete your changes.
If prompted to restart the Recorder, go to **Operations > Start and Stop > Reboot**. Your changes take effect after the restart.
 - Click **Revert** to undo any changes and return to the original settings.

Related topics

[Modify DP voice card properties \(page 201\)](#)

[Modify PCM32 voice card properties \(page 205\)](#)

[Modify DT voice card properties \(page 209\)](#)

[T1 trunk protocols reference \(page 228\)](#)

Modify the trunk protocol on an E1 voice card

Modify the trunk protocol in an E1 Card to determine the signalling variant, and therefore the number of channels available, to be used as a line protocol. See [Modify DP voice card properties \(page 201\)](#) for more information on properties and channels.

Procedure

1. Click **General Setup > Voice Cards > Card**.
2. Select an E1 voice card with a status of **Existing**.
3. In the **Trunk** pane, select the required protocol. Refer to the related topics (below) to learn more about E1 protocols.
4. Click **Channels** to view the number of channels available after the update. If you have exceeded the number of licensed channels, you must obtain additional licenses.



The number of channels vary between the DP3209 card and the DP6409 card. If you use a DP6409 card, two trunks are available; therefore, the number of channels available is doubled.

5. Do one of the following:

- Click **Save** to complete your changes.

If prompted to restart the Recorder, go to **Operations > Start and Stop > Reboot**. Your changes take effect after the restart.

- Click **Revert** to undo any changes and return to the original settings.

Related topics

[Modify DP voice card properties \(page 201\)](#)

[Modify PCM32 voice card properties \(page 205\)](#)

[Modify DT voice card properties \(page 209\)](#)

[E1 trunk protocols reference \(page 229\)](#)

Configure PCM32 voice cards

The PCM32 is trunk-based and is used in trading environments such as stocks, bonds and commodity trading. The PCM32 protocol is similar to E1 in that it is cabled over twisted pair cable and terminated with RJ-45 connectors. The card supports 32 voice channels per trunk span.

Related topics

[Supported voice cards \(page 198\)](#)

[Modify PCM32 voice card properties \(page 205\)](#)

[Update PCM32 voice card channels \(page 206\)](#)

[TDM voice card reference \(page 219\)](#)

Modify PCM32 voice card properties

Most configuration changes take effect dynamically without restarting the capture engine or rebooting the Recorder. Changes to the Input Companding Type require that you restart the system.

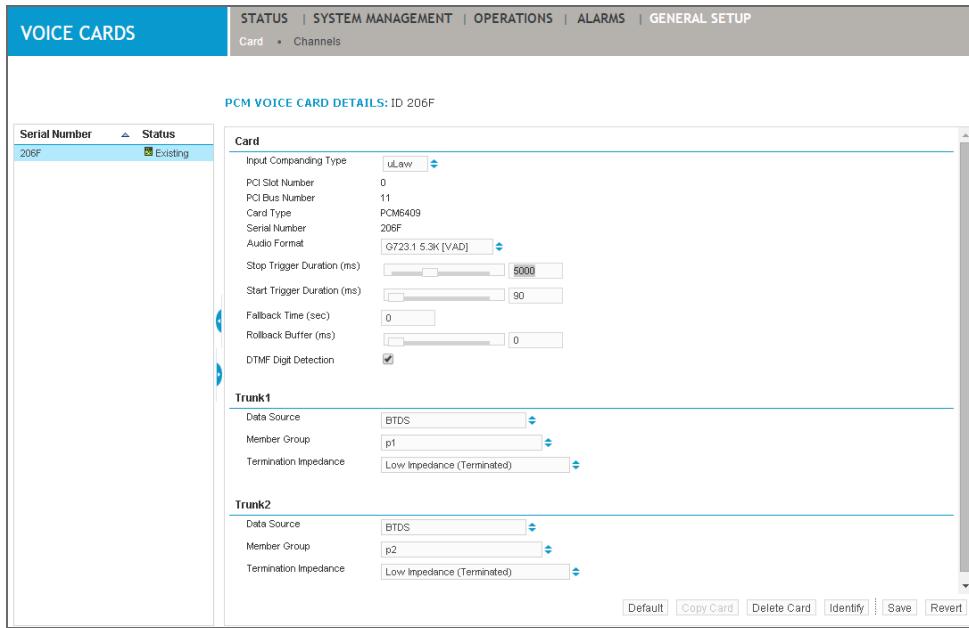
Procedure

1. Click **General Setup > Voice Cards > Card**.

From the voice card list in the left pane, select a PCM32 voice card status of **Existing** or **Newly Added**.



Click **Identify** to illuminate a blinking light on the card for identification.



2. Edit the **Card** properties, as required. Note that some fields you cannot edit.
3. Edit the properties for each trunk.
4. Click **Channels** to configure the channels associated with this card.
5. Do one of the following:
 - Click **Save** to complete your changes.
If prompted to restart the Recorder, go to **Operations > Start and Stop > Reboot**. Your changes take effect after the restart.
 - Click **Revert** to undo any changes and return to the original settings.

Related topics

- [Update PCM32 voice card channels \(page 206\)](#)
[TDM voice card properties reference \(page 219\)](#)
[TDM voice card channel properties reference \(page 225\)](#)
[Configure voice card channels \(page 236\)](#)

Update PCM32 voice card channels

You can enable individual channels on the PCM32 voice card and modify the channel recording settings. Channel IDs are created automatically.

PCM32 cards can have a maximum of 32 channels (for the PCM3209 card) or 64 channels (for the PCM6409 card).

Procedure

1. Click **General Setup > Voice Cards** and select a PCM32 card.
2. Click **Channels**.

VOICE CARDS

STATUS | SYSTEM MANAGEMENT | OPERATIONS | ALARMS | GENERAL SETUP
Card • Channels

CHANNEL LICENSES AVAILABLE: Channels Configured = 64, Concurrent licenses available = 500

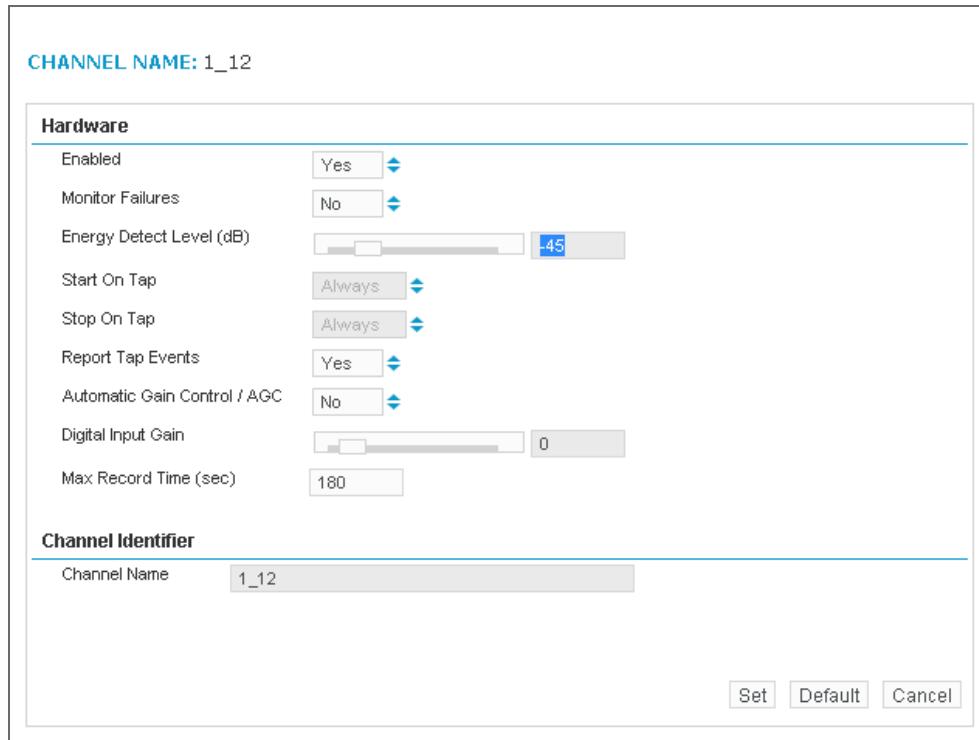
Serial Number	Status	Enabled	Channel #	Channel Name	Channel ID	Monitor Failures	Energy Detect Level	Start On Tap	Stop On Tap	Report Tap Events
206F	Existing	<input checked="" type="checkbox"/>	1	1_1	1	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	2	1_2	2	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	3	1_3	3	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	4	1_4	4	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	5	1_5	5	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	6	1_6	6	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	7	1_7	7	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	8	1_8	8	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	9	1_9	9	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	10	1_10	10	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	11	1_11	11	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	12	1_12	12	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	13	1_13	13	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	14	1_14	14	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	15	1_15	15	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	16	1_16	16	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	17	1_17	17	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	18	1_18	18	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	19	1_19	19	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	20	1_20	20	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	21	1_21	21	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	22	1_22	22	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	23	1_23	23	<input type="checkbox"/>	-45	Always	Always	Yes
		<input checked="" type="checkbox"/>	24	1_24	24	<input type="checkbox"/>	-45	Always	Always	Yes

Select All **Select None** **Save** **Revert** **Configure** **Edit Tags** **Copy Card**

3. Select a channel, and then click **Configure**.



To edit multiple channel names at one time, select the channels and click **Edit Tags**. See related topics (below) to learn about configuring channels.



4. Complete the **Hardware** and **Channel Identifier** settings, as required. See related topics (below) to learn about channel properties.
5. Do one of the following:
 - Click **Set** to complete your changes.
 - Click **Default** to undo any changes and return to the default settings.
 - Click **Cancel** to undo any changes and return to the last saved settings.

Related topics

[TDM voice card channel properties reference \(page 225\)](#)

[Configure voice card channels \(page 236\)](#)

Configure DT voice cards

The following sections describe how to modify properties and channels in the digital terminate (DT) voice card family (which supports the PCM30 type protocol and Active Recording on T1 & E1 mode).

The DT card is trunk-based and can be used in trading environments such as stocks, bonds and commodity trading (apart from active recording support). The DT card is cabled over twisted pair cable and terminated with RJ-45 connectors. The card supports 24 and 30 voice channels per T1 or E1 trunk span respectively.

Related topics

[Supported voice cards \(page 198\)](#)

[Modify DT voice card properties \(page 209\)](#)

[Update DT voice card channels \(page 211\)](#)

[TDM voice card reference \(page 219\)](#)

Modify DT voice card properties

Most configuration changes occur dynamically without restarting the capture engine or rebooting the Recorder. However, framing, protocol, and line coding changes, require that you perform a restart.

Procedure

1. Click **General Setup > Voice Cards > Card**.
2. From the voice card list in the left pane, select a DT voice card status of **Existing** or **Newly Added**.

3. Edit the voice card properties, as required. Note that some fields you cannot edit.
4. Edit the properties for each trunk.
5. Click **Channels** to configure the channels associated with this card.
6. Do one of the following:
 - Click **Save** to complete your changes.
If prompted to restart the Recorder, go to **Operations > Start and Stop > Reboot**. Your changes take effect after the restart.
 - Click **Revert** to undo any changes and return to the original settings.

Related topics

- [Update DT voice card channels \(page 211\)](#)
- [TDM voice card properties reference \(page 219\)](#)
- [Configure voice card channels \(page 236\)](#)

Update DT voice card channels

Channel IDs are created automatically. DT cards can have a maximum of 24/30 channels (DT3200 models) and 48/60 channels (DT6400 models).

Procedure

1. Click **General Setup > Voice Cards** and select a DT card.
2. Click **Channels**.

CHANNEL LICENSES AVAILABLE: Channels Configured = 0, Concurrent licenses available = 50

Serial Number	Status	Enabled	Channel #	Channel Name	Channel ID	Monitor Failures	Energy Detect Level	Start On Tap	Stop On Tap	Report Tap Events	AGC
0354	Newly Added	<input checked="" type="checkbox"/>	1		1	<input type="checkbox"/>	-45	Always	Always	Yes	No
0555	Newly Added	<input checked="" type="checkbox"/>	2		2	<input type="checkbox"/>	-45	Always	Always	Yes	No
0931	Newly Added	<input checked="" type="checkbox"/>	3		3	<input type="checkbox"/>	-45	Always	Always	Yes	No
3660	Newly Added	<input checked="" type="checkbox"/>	4		4	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	5		5	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	6		6	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	7		7	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	8		8	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	9		9	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	10		10	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	11		11	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	12		12	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	13		13	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	14		14	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	15		15	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	16		16	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	17		17	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	18		18	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	19		19	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	20		20	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	21		21	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	22		22	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	23		23	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	24		24	<input type="checkbox"/>	-45	Always	Always	Yes	No
		<input checked="" type="checkbox"/>	25		25	<input type="checkbox"/>	-45	Always	Always	Yes	No

3. Select a channel, and then click **Configure**.

CHANNEL NAME: 1_12

Hardware

Enabled	Yes
Monitor Failures	No
Energy Detect Level (dB)	45
Start On Tap	Always
Stop On Tap	Always
Report Tap Events	Yes
Automatic Gain Control / AGC	No
Digital Input Gain	0
Max Record Time (sec)	180

Channel Identifier

Channel Name	1_12
--------------	------

Set **Default** **Cancel**



To edit multiple channel names at one time, select the channels and click **Edit Tags**. See related topics (below) to learn about configuring channels.

4. Complete the **Hardware** and **Channel Identifier** settings, as required. See related topics (below) to learn about channel properties.
5. Do one of the following:
 - Click **Set** to complete your changes.
 - Click **Default** to undo any changes and return to the default settings.
 - Click **Cancel** to undo any changes and return to the last saved settings.

Related topics

[TDM voice card channel properties reference \(page 225\)](#)

[Configure voice card channels \(page 236\)](#)

Configure NGX voice cards

The NGX card records digital, station-side calls, and uses a combination of connector hardware and punchdown blocks.

Related topics

- [Supported voice cards \(page 198\)](#)
- [Modify NGX voice card properties \(page 213\)](#)
- [Update NGX voice card channels \(page 215\)](#)
- [Configure LD voice cards \(page 217\)](#)
- [TDM voice card properties reference \(page 219\)](#)

Modify NGX voice card properties

NGX cards record digitally on the station-side (extension) of the switch, unlike T1/E1 cards, which record digitally on the trunk (switch) side.

Procedure

1. Click **General Setup > Voice Cards > Card**.
2. Select an NGX voice card status of **Existing** or **Newly Added**.

3. Edit the **Card** properties, as required. Note that some fields you cannot edit.
4. Click **Channels** to configure the channels associated with this card.
5. Do one of the following:
 - Click **Save** to complete your changes.
If prompted to restart the Recorder, click **Operations > Start and Stop**, then select **Recorder** and click **Restart**.
 - Click **Cancel** to undo any changes and return to the last saved settings.

Related topics

[Update NGX voice card channels \(page 215\)](#)

[TDM voice card properties reference \(page 219\)](#)

[Configure voice card channels \(page 236\)](#)

Update NGX voice card channels

Channel IDs are created automatically. The number of channels available depends on the type of card.

Procedure

1. Click **General Setup > Voice Cards** and select an NGX card.
2. Click **Channels**.

Serial Number	Status	Enabled	Channel #	Channel Name	Channel ID	Monitor Failures	Extension	Agent ID	Energy Detect Level	Start On Tap	Stop On Tap	Report Tap Events	AGC
100	Existing	<input checked="" type="checkbox"/>	1	1					-45	InFallBack	InFallBack	Yes	No
200	Existing	<input checked="" type="checkbox"/>	2	2					-45	InFallBack	InFallBack	Yes	No
300	Existing	<input checked="" type="checkbox"/>	3	3					-45	InFallBack	InFallBack	Yes	No
400	Existing	<input checked="" type="checkbox"/>	4	4					-45	InFallBack	InFallBack	Yes	No
600	Existing	<input checked="" type="checkbox"/>	5	5					-45	InFallBack	InFallBack	Yes	No
700	Existing	<input checked="" type="checkbox"/>	6	6					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	7	7					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	8	8					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	9	9					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	10	10					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	11	11					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	12	12					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	13	13					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	14	14					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	15	15					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	16	16					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	17	17					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	18	18					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	19	19					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	20	20					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	21	21					-45	InFallBack	InFallBack	Yes	No
		<input checked="" type="checkbox"/>	22	22					-45	InFallBack	InFallBack	Yes	No

3. Select a channel, and then click **Configure**.

 To edit multiple channel names at one time, select the channels and click **Edit Tags**. See related topics (below) to learn about configuring channels.

CHANNEL INFORMATION: Channel # : 11, Card Type : NGX2400, Serial # : 100

Hardware	
Enabled	Yes
Monitor Failures	No
Energy Detect Level (dB)	-45
Start On Tap	InFallBack
Stop On Tap	InFallBack
Report Tap Events	Yes
Automatic Gain Control / AGC	No
Digital Input Gain	0
Channel Identifier	
Channel Name	
Extension	
Agent ID	
Set Default Cancel	

4. Complete the **Hardware** and **Channel Identifier** settings, as required. See related topics (below) to learn about channel properties.
5. Do one of the following:
 - Click **Set** to complete your changes.
 - Click **Default** to undo any changes and return to the default settings.
 - Click **Cancel** to undo any changes and return to the last saved settings.

Related topics

[Configure LD voice cards \(page 217\)](#)

[TDM voice card channel properties reference \(page 225\)](#)

[Configure voice card channels \(page 236\)](#)

Configure LD voice cards

Use the following procedures to configure any compatible LD (analog) voice card or to change information for the card's channels.

Related topics

- [Supported voice cards \(page 198\)](#)
- [Modify LD voice card properties \(page 217\)](#)
- [Update LD voice card channels \(page 217\)](#)
- [TDM voice card reference \(page 219\)](#)

Modify LD voice card properties

Use the following procedure to modify any LD (analog) card or channel configuration.

Procedure

1. Click **General Setup > Voice Cards > Card**.
2. Select an LD voice card with a status of **Existing** or **Newly Added**.
3. Update the voice card properties.
4. Click **Channel** to configure the channels associated with this card.
5. Do one of the following:
 - Click **Save** to complete your changes.
 - Click **Cancel** to undo any changes and return to the last saved settings.

Related topics

- [Update LD voice card channels \(page 217\)](#)
- [TDM voice card properties reference \(page 219\)](#)
- [Configure voice card channels \(page 236\)](#)

Update LD voice card channels

Compatible LD (analog) voice cards appear in [Supported voice cards \(page 198\)](#).

Procedure

1. Click **General Setup > Voice Cards** and select an LD voice card.
2. Click **Channels**.

CHANNEL NAME: 1_12

Hardware	
Enabled	Yes
Monitor Failures	No
Energy Detect Level (dB)	-45
Start On Tap	Always
Stop On Tap	Always
Report Tap Events	Yes
Automatic Gain Control / AGC	No
Digital Input Gain	0
Max Record Time (sec)	180
Channel Identifier	
Channel Name	1_12
Set Default Cancel	

3. Select a channel and click **Configure**.

CHANNEL INFORMATION: Channel # : 11, Card Type : NGX2400, Serial # : 100

Hardware	
Enabled	Yes
Monitor Failures	No
Energy Detect Level (dB)	-45
Start On Tap	InFallBack
Stop On Tap	InFallBack
Report Tap Events	Yes
Automatic Gain Control / AGC	No
Digital Input Gain	0
Channel Identifier	
Channel Name	
Extension	
Agent ID	
Set Default Cancel	

4. Update the **Hardware** and **Channel Identifier** settings, as required.
5. Do one of the following:
 - Click **Set** to complete your changes.
 - Click **Default** to undo any changes and use the default settings.
 - Click **Cancel** to undo any changes and return to the last saved settings.

Related topics

[TDM voice card channel properties reference \(page 225\)](#)

[Configure voice card channels \(page 236\)](#)

TDM voice card reference

Use the topics in this section to learn about the properties provided for TDM voice cards, including (where applicable) trunk properties, trunk protocols, and channel properties.

Related topics

[TDM recording setup \(page 198\)](#)

[TDM voice card properties reference \(page 219\)](#)

[TDM voice card channel properties reference \(page 225\)](#)

[T1 trunk protocols reference \(page 228\)](#)

[E1 trunk protocols reference \(page 229\)](#)

TDM voice card properties reference

The following properties are provided for voice cards and voice card trunks. Properties are in alphabetical order and identified by card type.

Applicable Cards						
Field	Description	PCM32	DP	DT	NGX	LD
Audio Detection Method	<p>Select Signaling, Energy or Human Voice and set the start/stop time as described under Start Trigger Duration and Stop Trigger Duration.</p> <ul style="list-style-type: none"> • Signaling—Select this option for D-Channel-based recording. • Energy—The recorder will start or stop recording based on detection of any sound, including but not limited to a human voice. • Human Voice—The recorder will start or stop recording based on detection of a human voice (also referred to as VOX recording). <p>Set the start/stop time as described under Start Trigger Duration and Stop Trigger Duration.</p>		✓	✓	✓	✓
Audio Format	<p>Defines the method for encoding the audio data in a .WAV file. This field is editable and required.</p> <p>Options: Alaw [VAD], uLaw [VAD], G.723.1 (5.3 K) [VAD], G726, and G729A</p>	✓	✓	✓	✓	✓

Field	Description	Applicable Cards				
		PCM32	DP	DT	NGX	LD
Card Type	The model number of the voice card. Read-only. Examples: DP3209, DP6409, DP3209, DP6409, NGX800, NGX1600, NGX2400, LD409, LD809. For NGX cards only: You can add an NGX80 daughterboard that increases the channel capacity of the card. In Windows device manager, the card shows as NGX800 .	✓	✓	✓	✓	✓
Data Source	Lists phone switches (data sources) associated with the Recorder (configured in Enterprise Manager). The message Please Select DataSource appears when the Recorder is not associated with any member groups. Optional.	✓	✓	✓	✓	✓
DTMF Digit Detection	Select to enable Dual Tone Multi Frequency (DTMF) digit detection. If deselected, any numbers (for example, a credit card number) entered by a caller using DTMF digits will not be stored with the recording data. Default: Enabled.	✓	✓	✓	✓	✓
Fallback Time (sec)	Maximum elapsed time before the Recorder switches to tap sense mode if there is a loss of CTI feed. Default: 0. Required.	✓	✓	✓	✓	✓
Framing	Framing standard to use. T1 options include: <ul style="list-style-type: none">• ESF (Extended Super Frame): default, a framing standard that includes cyclic redundancy checks (CRC).• SF (D4): Super Frame, also known as D4. E1 options include: <ul style="list-style-type: none">• Basic G.704: default, a frame alignment standard that includes CRC.• CRC-4: a 4-bit, cyclic redundancy check that ensures data integrity.		✓	✓		

Field	Description	Applicable Cards				
		PCM32	DP	DT	NGX	LD
Inbound CAS Idle Code (appears only for non-ISDN protocol)	<p>Defines the four-bit pattern used by the transmitting switch to indicate on-hook for the inbound signal. CAS is an acronym for Channel Associated Signalling.</p> <p>Range: 0000 - 1111. Default: 0.</p> <p>i Applicable only when the protocol is Non-ISDN and the Audio Detection Method is Signaling.</p> <p>T1 itself uses a 2-bit pattern so for T1 lines you would repeat the 2 bit pattern as a 4 bit pattern. For example, 01 becomes 0101.</p>		✓			
Input Companding Type	Choose the format to encode audio on the wire—this must match the switch configuration. Options are Alaw (regions with E-1 circuits) and uLaw (typically North America and Japan).	✓	✓	✓	✓	
Line Build Out	An estimate of the cabling required within the building/facility used by the signal repeater function in the copper line.			✓		
Line Coding	<p>Describes the method used to translate digital data into an electrical signal.</p> <p>T1 options include AMI and B8ZS.</p> <p>E1 options include AMI and HDB3.</p> <ul style="list-style-type: none"> • AMI (Alternate Mark Inversion) specifies that there are three states of the line: no voltage is a zero, positive voltage is a one (or mark), and negative voltage is also a one (or mark). Because of the inversion of the voltage for each ‘mark’ or one, sent, the receiving equipment can easily determine the data rate of the line and not lose synchronization. • B8ZS (Bipolar with 8 Zeros Substitution or Binary Eight Zero Substitution) is a method of line coding used for T1 lines. • HDB3 (High Density Bipolar of order 3 code) is used mainly in Japan, Europe and Australia (for E1 lines) and is based on AMI. It is also very similar to the B8ZS encoding used in T1 lines. 		✓	✓		

Applicable Cards						
Field	Description	PCM32	DP	DT	NGX	LD
Max Record Time (sec)	Maximum record time for a single call segment. Required. Default: 3600.		✓	✓	✓	✓
Member Group	Selected data source's eligible member groups. Configure member groups within the Data Source in Enterprise Manager. You cannot assign a single member group to more than one card. Optional.	✓	✓	✓	✓	✓
Mode	Defines whether the card is operating with the E1 or T1 firmware on it. T1 is used in the United States, Canada, and Japan. E1 is used in most other countries. Default: T1		✓	✓		
NFAS Group (appears only for T1 lines with NFAS protocol)	Identifies the Non-Facility Associated Signalling (NFAS) group of which the span is a member. Applicable only when the protocol is NFAS, at which point this setting is required. Range: 0-31. Default: 0.		✓			
NFAS Index (appears only for T1 lines with NFAS protocol)	Identifies the span within an NFAS group. Required for NFAS protocol. Range: 0-31. Default: 0.		✓			
NFAS Type (appears only for T1 lines with NFAS protocol)	Identifies whether the span is used for voice-only or whether it contains the D-Channel for the group, or the backup D-channel for the group. Required for NFAS protocol. Options: D , Backup , or None . Default: D.		✓			
Outbound CAS Idle Code (appears only for non-ISDN protocol)	Defines the four-bit pattern used by the transmitting switch to indicate on-hook for the outbound signal for Channel Associated Signalling (CAS). Range: 0000 - 1111. Default: 0. i Applicable only when the protocol is Non-ISDN and the Audio Detection Method is Signaling. T1 itself uses a 2-bit pattern so for T1 lines you would repeat the 2 bit pattern as a 4 bit pattern. For example, 01 becomes 0101.		✓			

		Applicable Cards				
Field	Description	PCM32	DP	DT	NGX	LD
PBX Type	Choose from list the type of PBX switch with which the Recorder is interfacing.				✓	
PCI Bus Number	The PCI bus number on the PC motherboard. Read-only.	✓	✓	✓	✓	✓
PCI Slot Number	The PCI card slot number on the PC motherboard. Read-only.	✓	✓	✓	✓	✓
Protocol	<p>Describes the multiplexing protocol used, such as ISDN or NFAS. The protocols available depend on whether you select T1 or E1.</p> <ul style="list-style-type: none"> • T1 protocols: see T1 trunk protocols reference (page 228). • E1 protocols: see E1 trunk protocols reference (page 229). 		✓			
Rollback Buffer (ms)	<p>Interval (milliseconds) to automatically capture voice before the Start Record command begins. The buffer enables the Recorder to compensate for delays in CTI processing and automatically rollback the voice and begin recording before the actual start record request is received.</p> <p>DP and DT default: Enabled? Yes. Default value: 1000. Range: 0 - 99000.</p> <p>PCM32, NGX, and LD default: Enabled? No. Default value: 0. Range: 0 - 99000.</p>	✓	✓	✓	✓	✓
Serial Number	The unique serial number of the voice card. Read-only.	✓	✓	✓	✓	✓
Start Trigger Duration (ms)	<p>Defines the interval (milliseconds) when sound needs to be above the threshold before the VOX method identifies a call. The threshold is configurable on each channel. Change the value in increments of 28 by sliding the bar.</p> <p>Required. Range: 0 to 5000. Default: 250.</p>	✓	✓	✓	✓	✓
Stop Trigger Duration (ms)	<p>Defines the interval (milliseconds) when sound needs to be below the threshold before the VOX method determines a call has ended. The threshold is configurable on each channel. Change the value in increments of 91 by sliding the bar.</p> <p>Required. Range: 0 to 13000. Default: 5000.</p>	✓	✓	✓	✓	✓

Field	Description	Applicable Cards				
		PCM32	DP	DT	NGX	LD
Termination Impedance	Determines whether the span will be terminated with Low Impedance for normal connections, or High Impedance for N+N redundant Recorder configurations. Values are Low Impedance (Terminated) and High Impedance (Non-terminated) . i N+N refers to having one backup Recorder for each Recorder in a system. So if you would normally need 5 Recorders to cover a particular number of channels, you would deploy 10 instead: 5 main and 5 backup Recorders.	✓				
Warn Tone	Warn tone setting that will alert the listener on the call that the call is being recorded. Pre-defined selections are: Europe , US-Canada , Australia , and None . Default is None .					✓
Zero Code Suppression	A technique implemented on T1 lines to ensure density. The density is a requirement imposed by the use of AMI as the line code on a T1. In this line code, a long series of the zeroes (that is, more than 15) leads to loss of clock and loss of synchronization. i This field does not appear if the line coding is B8ZS. If you select the ISDN protocol, then you should TE/NT. If you select RBS (Robbed Bit Signalling), three timers are displayed. For these timers, accept the defaults or type new settings.			✓		

Related topics

- [Modify DP voice card properties \(page 201\)](#)
- [Modify PCM32 voice card properties \(page 205\)](#)
- [Modify DT voice card properties \(page 209\)](#)
- [Modify NGX voice card properties \(page 213\)](#)
- [Modify LD voice card properties \(page 217\)](#)

TDM voice card channel properties reference

The following properties are provided for voice card channels. Properties are in alphabetical order and identified by card type.

		Applicable Cards				
Field	Description	PCM32	DP	DT	NGX	LD
AGC	Auto Gain Control enables a voice card option to amplify automatically the voice on the channel when necessary. It is recommended that you always change the audio level through the AGC setting. Required. Default: No.	✓	✓	✓	✓	✓
Employee ID	The optional identification of the employee. Refer to Extension for information on this field.				✓	✓
Channel #	Number of the channel on the card (for example, 1, 2, or 3), assigned by the voice card auto-detection process. Read-only.	✓	✓	✓	✓	✓
Channel ID	Logical channel ID used by the Integration Service to identify a channel. This is a unique number within the Recorder, generated from the card auto-detect process. Read-only.	✓	✓	✓	✓	✓
Channel Name	Optional, assigned name of the channel. Name channels individually or in blocks, by selecting the channel and clicking Configure or by selecting two or more channels and then clicking Edit Tags.	✓	✓	✓	✓	✓
Digital Input Gain	Level of amplification that can be used on weak channels. Change in increments of 1. Values above 3 can cause high audio clipping audio which may affect Speech Analytics performance; therefore, values of 4 or higher are not recommended. Range: -3 to 24. Default: 0.	✓	✓	✓	✓	✓
Enabled	To enable a channel, select its check box. Selecting a check box subtracts a license channel from the Available License counter (whereas when you deselect a channel check box, one is added to the counter). The default value for check boxes for cards with a status of Newly Added is deselected (disabled). Once you save the Newly Added card, all channels are enabled by default.	✓	✓	✓	✓	✓

Field	Description	Applicable Cards				
		PCM32	DP	DT	NGX	LD
Energy Detect Level (dB)	<p>Threshold, in decibels, when Energy is selected as the Audio Detection Method on the Card tab. Although this option is available when using Human Voice as the Audio Detection Method, it will have no effect. It applies only to the Energy option.</p> <p>For the Smartworks series of boards the adjustable range is -57 to 6, with a default value of -45 (minus 45).</p>	✓	✓	✓	✓	✓
Extension	<p>The optional telephone extension associated with this channel.</p> <p>Name extensions individually or in blocks:</p> <ul style="list-style-type: none"> • Select the channel and click Configure. • Select two or more channels (Ctrl + Click, or Shift + Click or Select All), and then click Edit Tags. <p>If Enterprise Manager controls this Recorder, this field cannot be edited in Recorder Manager. Instead, this field is populated with an extension number configured in the Data Source's Station-side Span Member Group. To edit the extension in Enterprise Manager, go to Data Sources > Member Groups and locate the span containing the extension(s).</p>				✓	✓
Maximum Record Time	This defines the maximum time in seconds that a channel will spend in the Recording state before forcing a break. Maximum is 1200. This is used in trading environments to limit the size of .WAV files on continuously recording channels. This setting has been moved from the card level to the individual channel level to allow more flexibility in trading environments. This field is optional.	✓				
Monitor Failures	Select to specify whether this channel is monitored for failure. If selected, a channel failure indication alarm is sent if the channel fails to record calls. If unchecked, the channel failure does not show as an alarm.	✓	✓	✓	✓	✓

Field	Description	Applicable Cards				
		PCM32	DP	DT	NGX	LD
Report Tap Events	Auto Gain Control enables a voice card option to amplify automatically the voice on the channel when necessary. It is recommended that you always change the audio level through the AGC setting. Required. Default: No.	✓	✓	✓	✓	✓
Start On Tap	This setting is defined by the Fallback Mode setting in the associated member group in Enterprise Manager.	✓	✓	✓	✓	✓
Stop on Tap	This setting is defined by the Fallback Mode setting in the associated member group in Enterprise Manager.	✓	✓	✓	✓	✓

Related topics

- [Update DP voice card channels \(page 202\)](#)
- [Update PCM32 voice card channels \(page 206\)](#)
- [Update DT voice card channels \(page 211\)](#)
- [Update NGX voice card channels \(page 215\)](#)
- [Update LD voice card channels \(page 217\)](#)

T1 trunk protocols reference

The following properties are provided for voice card T1 trunk protocols. Properties are in alphabetical order and identified by card type.



If you use a DP6409 card, two trunks are available with this card; therefore, the total number of channels available will be double the number stated in the supported voice cards section (see related topics below).

			Applicable Cards	
Protocol	Description	Channels Available	DP	DT
ISDN	Integrated Services Digital Network (ISDN) is a signaling variant used with the T1 or E1, reserving a single data channel on each multiplexed line for signaling information.	23	✓	✓
Non-ISDN	Applies to CAS or Robbed Bit Signaling (RBS), which are signalling variants used with the T1 or E1, reserving a single data channel on each multiplexed line for signaling information.	24	✓	✓
NFAS	NFAS D. This is a variant of ISDN used with T1 where a single D-channel is used to service up to 10 x T1 lines. Use NFAS D when the T1 is part of an NFAS group and this T1 contains the D-channel.	23	✓	
	NFAS Backup. This is a variant of ISDN used with T1 where a backup channel, not necessarily the D-channel, is used to service up to 10 x T1 lines. Use NFAS Backup when the T1 is part of an NFAS group and this T1 contains the backup D-channel.	23	✓	
	NFAS None. A non-facility associated signaling variant of ISDN, it is used with T1 lines but does not use a D-channel or Backup channel. Use NFAS None when the T1 is part of an NFAS group but the T1 does not contain either a primary or backup D-channel.	24	✓	

Related topics

[Supported voice cards \(page 198\)](#)

[Modify the trunk protocol on a T1 voice card \(page 204\)](#)

E1 trunk protocols reference

The following properties are provided for voice card E1 trunk protocols. Properties are in alphabetical order and identified by card type.



The number of channels available are for the DP3209 card; if you use a DP6409 card the number of channels available is doubled, as two trunks are available with this card.

			Applicable Cards	
Protocol	Description	Channels Available	DP	DT
ISDN / DASS2	<p>Integrated Services Digital Network (ISDN) is a signalling variant used with the T1 or E1 that reserves a single data channel on each multiplexed line for signaling information.</p> <p> This setting must match the setting on the PBX/phone switch.</p> <p>DASS2 is a predecessor of ISDN.</p>	30 / 60	✓	✓
Non-ISDN / RBS	<p>Applies to CAS or Robbed Bit Signaling (RBS), which are signalling variants used with the T1 or E1, reserving a single data channel on each multiplexed line for signaling information.</p> <p> This setting must match the setting on the PBX/phone switch.</p>	30 / 60	✓	✓
DPNSS	<p>The Digital Private Network Signalling System (DPNSS) is a network protocol used on digital trunk lines for connecting two PBXs. DPNSS supports a defined set of inter-networking facilities.</p> <p> This setting must match the setting on the PBX/phone switch.</p>	30 / 60	✓	

Related topics

[Modify the trunk protocol on an E1 voice card \(page 204\)](#)

Voice cards and channels

General voice card configuration tasks in a TDM recording environment are described. In TDM recording, you can use one of three audio detection methods.

Audio detection methods

- **Signaling**—Select this option for D-Channel-based recording.
- **Energy**—The Recorder will start or stop recording based on detection of any sound, including but not limited to a human voice.
- **Human Voice**—The Recorder will start or stop recording based on detection of a human voice (also referred to as VOX recording).

Viewing available voice cards

The Recorder Manager lists available digital and analog voice cards, along with their properties and available channels. Only T1/E1 cards can record trunk-side (that is, between the switch and PBX), so trunk settings appear for T1/E1 cards only. All other cards record station-side (that is, between the PBX and extensions).

Related topics

[Manage voice cards \(page 230\)](#)

[Manage voice card channels \(page 236\)](#)

Manage voice cards

Use Recorder Manager to view, add and modify settings on an existing or replaced card. Compatible voice cards appear in [Supported voice cards \(page 198\)](#).

Related topics

[View voice cards \(page 230\)](#)

[Copy voice card configuration \(page 232\)](#)

[Identify a voice card \(page 233\)](#)

[Delete a voice card \(page 233\)](#)

[Add a new voice card \(page 234\)](#)

[Replace a voice card \(page 234\)](#)

[Modify an existing voice card \(page 235\)](#)

View voice cards

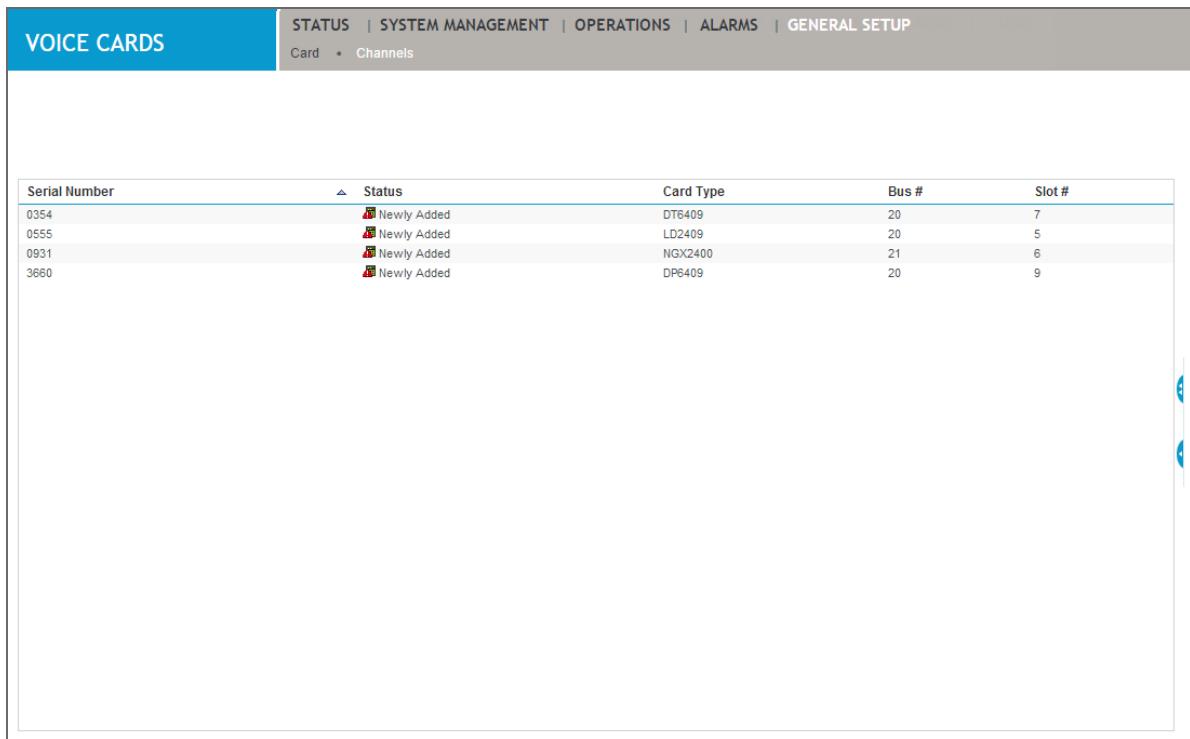
The Card screen lists all voice cards in the Recorder. From this page you can take action on one or more cards, and find out where in the computer the voice card is located.

During the initialization of the Recorder, if there are any faulty Smartworks cards, an alarm is triggered and an alarm message appears. After this message appears, you may disable and replace

the card, or ignore the message. If you ignore the message, the Recorder skips the faulty card and proceeds with the initialization of the other cards.

Procedure

1. Click **General Setup > Voice Cards > Card**.



The screenshot shows a software interface titled 'VOICE CARDS'. At the top, there is a navigation bar with links: STATUS | SYSTEM MANAGEMENT | OPERATIONS | ALARMS | GENERAL SETUP. Below the navigation bar, there are two tabs: 'Card' and 'Channels', with 'Card' being selected. The main area displays a table with the following data:

Serial Number	Status	Card Type	Bus #	Slot #
0354	Newly Added	DT6409	20	7
0555	Newly Added	LD2409	20	5
0931	Newly Added	NGX2400	21	6
3660	Newly Added	DP6409	20	9

2. The following information appears for each card:

Field	Description
Serial Number	The unique serial number of the voice card.
Status	<p>Shows the status of the card as one of either Existing, Replaced, Newly Added, and Removed.</p> <ul style="list-style-type: none"> • Existing is a previously existing card that can be configured. • Replaced is a card that has taken the position of an Existing card and may or may not require configuration. • Newly Added is a new voice card that is physically located in the PC but awaits configuration. • Removed refers to an empty slot representing a card that was removed from the PC.
Card Type	Shows the model number and type of the card.

Field	Description
Bus #	Shows a read-only number of the data bus on which the card is located in the PC.
Slot #	Shows a read-only number of the slot on the computer's motherboard on which the card is located.

- When finished, click the left pointing arrow on the right side of the window to expose the voice card details window.

Related topics

[Copy voice card configuration \(page 232\)](#)

[Identify a voice card \(page 233\)](#)

[Delete a voice card \(page 233\)](#)

[Add a new voice card \(page 234\)](#)

[Replace a voice card \(page 234\)](#)

[Modify an existing voice card \(page 235\)](#)

Copy voice card configuration

Copy the configuration of a voice card with a status of Existing to one or more other voice cards of the same type, regardless of their status. The card's model number and all pertinent configuration information is copied. Bus numbers and slot numbers are not copied.

Procedure

- Click **General Setup > Voice Cards > Card**.
- Select a voice card with a status of **Existing** or **Removed**.
- Click **Copy Card**. A list of installed voice cards appears.
- Select one or more cards, and then click **Copy Config**.

You can copy cards only of the same family. For example, if you select an NGX card as the source, the destination cards must be of type NGX.

- Click **Operations > Start and Stop** and reboot if requested.



If you use an expansion chassis with your Recorder and you need to restart the Recorder, you must stop and restart the expansion chassis, wait 30 seconds, and then restart the Recorder so that all capture cards can be detected in the bus scan.

Related topics

[View voice cards \(page 230\)](#)

[Identify a voice card \(page 233\)](#)

[Delete a voice card \(page 233\)](#)

[Add a new voice card \(page 234\)](#)

[Replace a voice card \(page 234\)](#)

[Modify an existing voice card \(page 235\)](#)

Identify a voice card

To locate a specific voice card, you can select the card in the Recorder Manager list and click **Identify**. A light blinks on the back of the hardware indicating where the card is physically located. You can have as many cards as there are available card slots on the PC (typically maximum 15), so that when you click the **Identify** button, the light on the corresponding card appears.



A card's light cannot be seen from the back of the computer/server; the light is on the board.

Procedure

1. Click **General Setup > Voice Cards > Card** and select a card.
The **Identify** function works for all card statuses except Removed.
2. Click **Identify**. A light blinks on the card. If the light does not illuminate, check connections (card seating and wire connectors) and retest. If the light still does not appear, the card may be defective and require replacing.

Related topics

- [View voice cards \(page 230\)](#)
- [Copy voice card configuration \(page 232\)](#)
- [Delete a voice card \(page 233\)](#)
- [Add a new voice card \(page 234\)](#)
- [Replace a voice card \(page 234\)](#)
- [Modify an existing voice card \(page 235\)](#)

Delete a voice card

Delete a voice card to remove a selected card from the configuration window. All cards, regardless of status, are eligible for deletion. For example, a voice card may be removed from one Recorder and relocated in a different Recorder.

Procedure

1. Click **General Setup > Voice Cards > Card**.
2. Select a voice card, regardless of status.
3. Click **Delete**.

Related topics

- [View voice cards \(page 230\)](#)
- [Copy voice card configuration \(page 232\)](#)
- [Identify a voice card \(page 233\)](#)
- [Add a new voice card \(page 234\)](#)
- [Replace a voice card \(page 234\)](#)
- [Modify an existing voice card \(page 235\)](#)

Add a new voice card

Add a new voice card to install and configure a new compatible voice card into a Recorder.

Procedure

1. Insert a compatible voice card (see [Supported voice cards \(page 198\)](#)) into an empty slot on the bus of the Recorder PC.

 Extreme care should be taken when inserting voice cards or any other component into a PC. Tools with magnetic tips should be used with extreme caution. Wearing an anti-static cuff is strongly recommended to prevent static electricity.
2. Click **Operations > Start and Stop** and click **Reboot** to reboot the system. The Recorder detects and displays the new card's slot number, serial number, and other metadata.
3. Click **General Setup > Voice Cards > Card**. The card you added appears in the left pane with a status of **Newly Added**.
4. Configure the voice card as necessary or leave all settings at their defaults and click **Save**. If an unsupported card is detected, its factory default information may display. However the card cannot be configured and you should replace the unsupported card with a supported one.
5. Click **Channels** to review channels available, as described in [Configure voice card channels \(page 236\)](#).
6. Click **Save**. The status of the voice card changes from **Newly Added** to **Existing**.
7. If prompted, restart services by choosing **Operations > Start and Stop**.

Related topics

[View voice cards \(page 230\)](#)

[Copy voice card configuration \(page 232\)](#)

[Identify a voice card \(page 233\)](#)

[Delete a voice card \(page 233\)](#)

[Replace a voice card \(page 234\)](#)

[Modify an existing voice card \(page 235\)](#)

Replace a voice card

Replace a voice card as a replacement for a broken voice card in the same bus slot. The replacement card must be the same type, must be in the same slot, and must have a status of Replaced. You then update and save the setting. The fields on the voice cards vary according to card type selected.

Procedure

1. Click **General Setup > Voice Cards > Card**.
2. Select the replacement card. This card has a status of **Replaced**. You cannot edit the card until the card is saved and the status is **Existing**.

3. Click **Save**. The status of the card is changed from **Replaced** to **Existing**. You can now edit the card.
4. Complete the Voice Card Details screen fields for the card type by referring to one of the following:
 - [Modify DP voice card properties \(page 201\)](#)
 - [Modify PCM32 voice card properties \(page 205\)](#)
 - [Modify NGX voice card properties \(page 213\)](#)
 - [Modify LD voice card properties \(page 217\)](#)

Related topics

[View voice cards \(page 230\)](#)

[Copy voice card configuration \(page 232\)](#)

[Identify a voice card \(page 233\)](#)

[Delete a voice card \(page 233\)](#)

[Add a new voice card \(page 234\)](#)

[Modify an existing voice card \(page 235\)](#)

Modify an existing voice card

Modify properties of an existing card to implement any card or channel configuration changes. In modifying an existing card, you select the card, make changes, save the changes, and the new settings take place upon restart of the Recorder.

Procedure

1. Complete the steps as described in [Add a new voice card \(page 234\)](#), and then click **General Setup > Voice Cards > Card**.
2. In the Voice Card List box (left pane), select the card (with the status of **Existing**) to be modified and type the new settings for the card type as by referring to one of the following:
 - [Modify DP voice card properties \(page 201\)](#)
 - [Modify PCM32 voice card properties \(page 205\)](#)
 - [Modify NGX voice card properties \(page 213\)](#)
 - [Modify LD voice card properties \(page 217\)](#)
3. Click **Channels**, and review channel details if necessary, as described in [Configure voice card channels \(page 236\)](#).
4. Click **Save** and reboot the system by clicking **Operations > Start and Stop** if prompted for the new settings to take effect.



If you make changes to any speed or duplex settings for the voice card, always restart the Recorder, as directed in Step .

Related topics

[View voice cards \(page 230\)](#)

[Copy voice card configuration \(page 232\)](#)

[Identify a voice card \(page 233\)](#)

[Delete a voice card \(page 233\)](#)

[Add a new voice card \(page 234\)](#)

[Replace a voice card \(page 234\)](#)

Manage voice card channels

The following sections describe how to view and configure voice card channels:

- [View voice card channels \(page 236\)](#)
- [Configure voice card channels \(page 236\)](#)
- [Edit voice card channels \(page 237\)](#)
- [Copy voice card configuration from the Channels screen \(page 237\)](#)
- [Revert channel settings \(page 238\)](#)
- [Edit tags for voice card channels \(page 238\)](#)

View voice card channels

View voice card channels to review summary information of licensed channels corresponding to a selected voice card. Although channel configurations vary for each card type you can perform the same types of actions by clicking the action buttons to select, save, revert, configure, and identify cards.



To configure a channel, select any displayed channel and click **Configure**. To copy a voice card configuration, select the card instead of the channel and then click **Copy Card**.

Procedure

1. Click **General Setup > Voice Cards > Card**.
2. Select a voice card, and then click **Channels**.
3. Configure channels as described in the related topics section.

Related topics

[Configure voice card channels \(page 236\)](#)

[Edit voice card channels \(page 237\)](#)

Configure voice card channels

Configure voice card channels to change editable settings on one or more channels, such as **AGC** and **Energy Detect Level**.

You can configure a single Channel Name using the Configure command. Except for T1/E1 and PCM cards, you can also configure Extension and Employee ID using the Configure command. However, for a large number of channels, doing so can be a laborious task. To edit multiple Channel Name, Extension and Employee ID fields, use the Edit Tags command, as described in [Edit tags for voice card channels \(page 238\)](#).



If the Recorder is associated with the Enterprise Manager, Extension and Employee ID fields are controlled from the Enterprise Manager.

Procedure

1. Click **General Setup > Voice Cards > Card**.
2. Select a voice card, and then click **Channels**. Select a voice card, and then click **Channels**. To edit all channels at once, click **Select All** (click **Select None** to de-select.)
3. Click **Configure**.
4. Complete the channel details screen for the type of voice card selected.
5. Click **Save**.

Related topics

- [Update DP voice card channels \(page 202\)](#)
[Update PCM32 voice card channels \(page 206\)](#)
[Update DT voice card channels \(page 211\)](#)
[Update NGX voice card channels \(page 215\)](#)
[Update LD voice card channels \(page 217\)](#)

Edit voice card channels

Procedure

1. Click **General Setup > Voice Cards > Card**.
2. Select a voice card, and then click **Channels**.
3. To edit all channels at once, click **Select All** (click **Select None** to de-select).
4. Click **Configure**.
5. Complete the channel details screen according to the type of voice card selected.
6. Click **Save**.

Related topics

- [Update DP voice card channels \(page 202\)](#)
[Update PCM32 voice card channels \(page 206\)](#)
[Update DT voice card channels \(page 211\)](#)
[Update NGX voice card channels \(page 215\)](#)
[Update LD voice card channels \(page 217\)](#)

Copy voice card configuration from the Channels screen

From the Channels screen, you have the option to copy an associated card. See [Copy voice card configuration \(page 232\)](#).

Related topics

- [Configure voice card channels \(page 236\)](#)

[Edit voice card channels \(page 237\)](#)

Revert channel settings

If you are editing channel settings, but decide before saving that you want to discard the changes, you can click the **Revert** button to restore the settings that were last saved.

Related topics

[Configure voice card channels \(page 236\)](#)

[Edit voice card channels \(page 237\)](#)

Edit tags for voice card channels

Edit voice card channel tags to assign a name to channels and, for some voice cards, identification for the extensions and employees associated with channels.

Using the Edit Tags option, you can select one or more channels and apply settings without having to cycle through individual channels. Editing tags is distinct from using the Configure command on channels, where you can configure all settings except read-only fields, as described in [Configure voice card channels \(page 236\)](#).

- If the Recorder is associated with the Enterprise Manager, Extension and Employee ID fields are controlled from the Enterprise Manager.
- It is recommended that you always change the audio level through the AGC setting. If you change the accompanying Digital Input Gain setting, values higher than 3 may result in high clipping in audio which may affect Speech Analytics performance; therefore values of 4 or higher are not recommended. See the instructions for updating voice card channels for your particular card (under [TDM recording setup \(page 198\)](#)).

Procedure

1. Click **General Setup > Voice Cards > Card**.
2. Select a voice card, and then click **Channels**.
3. Select two or more channels.
4. Click **Edit Tags**. The channel details screen appears, allowing you to edit the Channel Name and, for all but T1/E1 and PCM cards, the Extension and Employee ID settings for the selected channels.

Channel #	Channel ID	Channel Name	Extension	Agent ID
10	10			
11	11			
12	12			
13	13			
14	14			
15	15			

Set Cancel

5. Complete the channel details screen:

Item	Description
Channel#	Number of the channel on the card (for example, 1, 2, or 3), assigned by the voice card auto-detection process. Read-only.
Channel ID	ID of the channel. Read-only.
Channel Name	Name of the channel.
Extension	<p>The optional telephone extension associated with this channel. Name Extensions individually or in blocks:</p> <ul style="list-style-type: none"> • Select the channel and click Configure. • Select two or more channels (Ctrl + Click, or Shift + Click or Select All), and then click Edit Tags. <p>If Enterprise Manager controls this Recorder, this field cannot be edited in Recorder Manager. Instead, this field is populated with an extension number configured in the Data Source's Station-side Span Member Group. To edit the extension in Enterprise Manager, go to Data Sources > Member Groups and locate the span containing the extension(s).</p>
Employee ID	Optional Employee ID associated with this channel. This field may be populated from the Enterprise Manager, in which case it will be read-only.

6. Click **Set**.

Related topics

[Configure voice card channels \(page 236\)](#)

[Edit voice card channels \(page 237\)](#)

IP Recorder and IP Recorder Video configuration

If you are using IP recording for audio or video, follow these procedures to configure the network interface card (NIC) configuration.

- [Update BIOS settings for Windows 2012 R2 \(page 240\)](#)
- [Configure network interface cards \(page 240\)](#)
- [Configure network cards and filters \(page 243\)](#)
- [Configure network protocols \(page 247\)](#)
- [Configure IP recording settings \(page 249\)](#)

Update BIOS settings for Windows 2012 R2

IP Recording on Windows 2012 R2 servers requires a change to the BIOS to prevent recording loss due to dropped network packets. Change the power mode to high performance/maximum performance.

Before you begin

If you require additional guidance changing BIOS settings, consult the documentation provided when you acquired the server from the manufacturer.

Procedure

1. Enter the BIOS setup utility on the server during the boot sequence, as directed by the manufacturer.
2. In the setup utility, locate the power management options.
3. Set the power profile to high performance or maximum performance.
4. Save changes to the BIOS and restart the server.

Related topics

[IP Recorder and IP Recorder Video configuration \(page 240\)](#)

[Configure network interface cards \(page 240\)](#)

Configure network interface cards

The following sections describe the process of setting up network cards, filters and protocols. Detection of standard NICs for IP recording is an automatic process. After installing the NIC, the Windows operating system automatically detects the new hardware and acts accordingly.

 In Interception recording mode the recording system will support up to eight NICs. In Delivery recording mode only one NIC is supported.

You can however have one NIC for Delivery and others for Interception. In this type of scenario, ensure that the same call does not exist on both NIC cards (for example, if an extension is monitored in Delivery mode, the RTP payload for this extension should not exist on the Interception NIC card).



If you make any system-level changes to a NIC using Windows, you must restart that server on which the NIC resides, otherwise errors may occur.

Related topics

- [Configure capture settings for NICs \(page 241\)](#)
- [NIC settings for interception recording \(page 242\)](#)
- [Configure network cards and filters \(page 243\)](#)
- [Configure network protocols \(page 247\)](#)
- [Configure IP recording settings \(page 249\)](#)

Configure capture settings for NICs

Configure capture settings to setup NICs and filters, and to assign communication protocols for extensions and devices.

Related topics

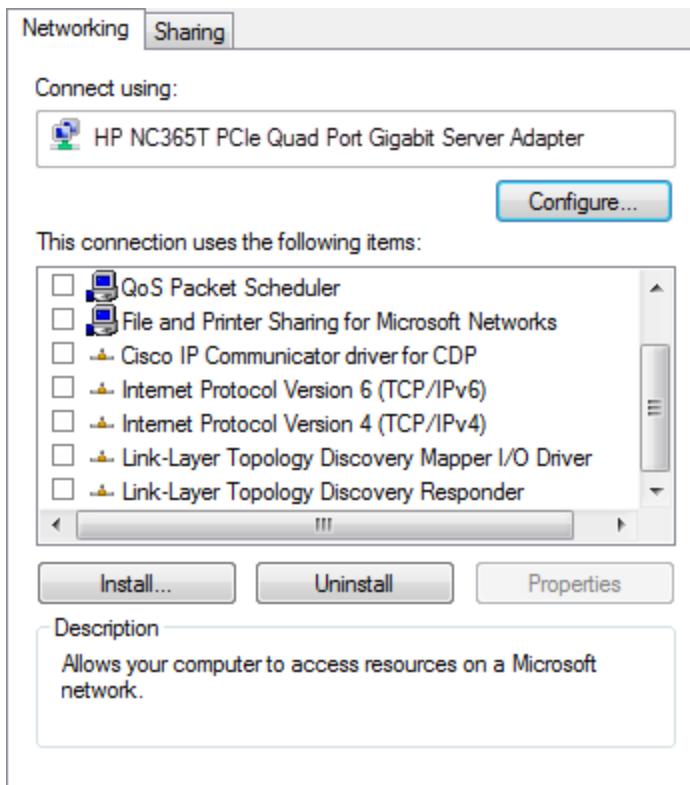
- [NIC settings for interception recording \(page 242\)](#)
- [Configure network cards and filters \(page 243\)](#)
- [Configure network protocols \(page 247\)](#)
- [Configure IP recording settings \(page 249\)](#)

NIC settings for interception recording

For interception recording, use Windows to configure the NIC properties for all cards by means of the **Networking** tab of the adapter properties.

Procedure

1. Clear all protocols listed.



2. Click **Configure**, and then go to the **Advanced** tab.
 - Set the Transmit Buffers (Tx) to zero or the lowest value allowed.
 - Set the Receive Buffers (Rx) to the maximum value allowed.
3. Click **OK** to save your changes to the NIC settings.
4. Restart the server.

Related topics

[Configure capture settings for NICs \(page 241\)](#)

[Configure network cards and filters \(page 243\)](#)

[Configure network protocols \(page 247\)](#)

[Configure IP recording settings \(page 249\)](#)

Configure network cards and filters

You can apply filters to IP traffic to increase performance when recording in Interception mode; do not apply filters in Delivery mode.

Only Interception mode is supported when recording IP video.

Filters can:

- Prevent the Recorder from receiving excessive, unneeded packets.
- Repress packets that the Recorder cannot process.
- Remove specific IP address ranges and traffic.

You can also configure the (Network Interface Cards (NICs) in some TDM Recorders to create settings needed by the IP emulation of pseudo wire emulation protocols (PWE3).

Choosing the starting and ending ports for delivery recording

Before making configuration changes, note the following: When using delivery recording, the UDP port range assigned to the **Recorder Analytics Framework** server role to receive audio from the IP Capture Engine must be separate from the port range configured in Recorder Manager on the same recorder by **IP Capture** to receive RTP from the telephony system being captured.

The port ranges, by default, are empty and must always be configured on a new Recorder Server using delivery recording. The entire range of ports must be opened in any firewalls that would otherwise block the RTP traffic to the recorder. To learn about the default port ranges by server role, see the *Firewall Ports Configuration Guide*.

Since a single RTP stream uses an even port number, the next (odd) port number is reserved for any associated RTCP stream. Stereo recording uses two streams per recording. Therefore, four UDP ports are required for each concurrent channel. You can calculate the minimum size of the port range required based on the number of concurrent channels used with a 25% buffer added:

$$((\text{Number of concurrent channels}) * 4) * 1.25$$

Before you begin



Before making configuration changes, note the following:

- Obtain filter expressions from your system architect or by visiting <http://www.winpcap.org> for filter expressions.
- IP Analyzer is only used in interception environments; it has no role in delivery environments.

Procedure

1. In an IP Recorder, choose **General Setup > Capture Settings > Cards and Filters**.

CONFIGURE CARDS AND FILTERS: List of available network interface cards.

Name	Device Name	Recording Type	Starting Port	Ending Port	Filter Expression	Subnet Mask	Destination Subnet	Next Hop Router
Application NIC	Intel(R) PRO/1000 MT Network Connection	Interception	0	0		0.0.0.0	0.0.0.0	0.0.0.0

Save Revert

2. Complete any editable settings:

Item	Description
Name	Shows a read-only description of the Network Interface Card. Card names must use the Latin alphabet. Non-Latin characters are not supported.
Device Name	Shows the read-only network connection name associated with the NIC.

Item	Description
Recording Type	<p>Choose one of the following (the default is None)</p> <ul style="list-style-type: none"> • Delivery—The Starting Port, Ending Port, and Filter Expression fields are enabled, allowing selective recording based on the ports specified, and the filter expression. You cannot use this option with more than one NIC card. You cannot use this option to record IP video calls. • Interception—Recording is based on the Filter Expression field (all other fields are unavailable). Select this option when recording IP video calls. • RFC 2003 Interception—Recording is based on the Filter Expression field (all other fields are unavailable). Acme Packet SBC Session Replication allows a copy of specific calls to be delivered to a recording device on the network. Use the RFC 2003 Interception recording type if you are recording Acme Packet SBC-replicated traffic. You cannot use this option to record IP video calls. See the Avaya or Genesys <i>Integration Guide</i> for more information. • RTP Proxy—Select RTP Proxy for V15.2 HFR3 and lower Lync environments where the Recorder acts as an RTP proxy to record calls. In this mode, the Recorder is placed in the RTP (audio) path between the endpoints in the call, and forwards audio between those two devices. You cannot use this option to record IP video calls. • None—Starting Port, Ending Port and Filter Expression are unavailable and no recording takes place. <p>Also note:</p> <ul style="list-style-type: none"> • If you expect the need for more channels in the future, start with a higher end NIC card. You cannot change the on-board NIC later. • For all Recording Types, after disabling/enabling the NIC card you must return to this screen, save the configuration, then restart the IP Capture Service. • For Skype environments, you do not need to configure a Recording type. IP Capture directly connects to the Verba Proxy/Media Collector to receive both signaling and audio on the connection.
Starting Port	Starting port specific to the Protocol. Only numerals separated by a comma are acceptable. The Starting Port number must be less than the Ending Port number. This field is enabled only if the Delivery recording type is selected.
Ending Port	Ending port specific to the Protocol. Only numerals separated by a comma are acceptable. The Ending Port number must be greater than the Starting Port number. This field is enabled only if the Delivery recording type is selected.
Filter Expression	Shows the name of the protocol or just the protocols that are specific to the card. This value is an expression such as TCP (transmission control protocol). The value is also the filter expression being used for this NIC. The actual filter expression is the logical sum (that is, the operator AND) of the filter on each card and the filter specified at the system level. See also Configure network protocols (page 247) .

Item	Description
Subnet Mask	Type the subnet mask. The subnet mask is used to determine what subnet an IP address belongs to. An IP address has two components: the network address, and the host (workstation) address. For example, consider the IP address 150.215.017.009. The first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host (workstation) on this network.
Destination Subnet	Type the IP address of the host (workstation) address, as described in the Subnet Mask field.
Next Hop Router	Type the IP address of the next logical router device in the network.

3. Click **Save**.

Example: Filter Expression for RTP-based IP Recorders

You can reduce the amount of traffic that IP Recorders and Analyzers need to monitor by creating and applying network filters. A filter screens network traffic, allowing through only traffic that meets the conditions specified in the filter. Since a well-constructed filter can reduce or eliminate unnecessary traffic, it can improve your system performance.

Filters are applied at the Network Interface Card (NIC) level. If a Recorder has more than one NIC, a system-level filter applies to all of them. If you also apply NIC-level filters, the system appends these filters to the system-level filter. (Make certain that your system-level and NIC-level filters do not contradict or otherwise interfere with each other.) The Recorder uses WinPcap for network filtering. You can find information on their standardized filter syntax at <http://www.winpcap.org>.

The most typical filters would be:

(tcp port 2000) or (udp and not udp port 0) Use this filter in a standard Cisco SCCP environment. It tells the driver to let packets of port 2000 through; these are the SCCP packets, and also to let UDP packets through, which contain the RTP and therefore the audio.

(tcp port 5060) or (udp and not udp port 0) Use this filter in standard SIP environments. This filter lets the SIP control protocol through on port 5060 and the UDP, which contains the RTP and therefore the audio.

At a minimum, use the following standard pcap filters:

- For Recorders that use SIP: **(tcp port 5060) or (udp and not udp port 0)**. This filter lets the SIP control protocol through on ports 2000 and 5060 and the UDP, which contains the RTP and therefore the audio.
- For Recorders that use SCCP: **(tcp port 2000) or (udp and not udp port 0)**.

Because port numbers change according to customer environment, check with your system architect that the port numbers configured correctly reflect your environment.

Related topics

[Configure capture settings for NICs \(page 241\)](#)

[NIC settings for interception recording \(page 242\)](#)

[Configure network protocols \(page 247\)](#)

[Configure IP recording settings \(page 249\)](#)**Related information**

Recorder Analytics Framework server role settings (*Enterprise Manager Configuration and Administration*)

Configure network protocols

Configure call control protocols in the network to identify which IP communication protocol is used for Recorder Controlled extension management, including Analyzer if installed. The Remote Analyzer protocol can also be used. If your Extension Recorder Control Type is CTI Controlled (configured in the Enterprise Manager), do not configure SCCP or SIP, as these will trigger recordings and override existing CTI Controlled settings.



Please note that RTP detection is independent of protocol configuration. Please see [Configure IP recording settings \(page 249\)](#).

Procedure

1. Choose **General Setup > Capture Settings > Protocols**.

The screenshot shows the 'Capture Settings' interface with the 'Protocols' tab selected. The top navigation bar includes links for STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP. Below the navigation bar, there are links for Cards and Filters, Protocols, and IP Recording. The main content area is titled 'CONFIGURE PROTOCOLS: List of Call Control Protocols.' It displays a table with columns for Name, Configured (with checkboxes), and Listen Port. The table rows are:

Name	Configured	Listen Port
H.323	<input checked="" type="checkbox"/>	
Remote Analyzer	<input type="checkbox"/>	29510
SCCP	<input checked="" type="checkbox"/>	
SIP	<input type="checkbox"/>	
Unify (Siemens) H.323	<input type="checkbox"/>	

At the bottom right of the interface are 'Save' and 'Revert' buttons.

2. Complete the following settings:

Item	Description
Name	<p>Shows the name of the protocol.</p> <ul style="list-style-type: none"> • H.323 is a common multimedia communications protocol used in packet-based networks (and in particular, in some Avaya environments). • Remote Analyzer is the name of the proprietary protocol used for call control in IP Analyzer. • SCCP (Skinny Call Control Protocol) is used with either Cisco IP phones or Cisco Call Managers. Select this option to record video for phones that support SCCP. • SIP (Session Initiated Protocol) is a common IETF non-proprietary call control protocol. Select this option to record video for phones that support SIP. • Unify (Siemens) H.323 is used exclusively with Siemens.
Configured	Select a protocol (see above for descriptions) to be used if the Extension Recorder Control Type (configured in the Enterprise Manager) is Recorder Controlled . If the Extension Recorder Control Type is NOT Recorder Controlled (that is, extensions are CTI Controlled), leave these fields unchecked. If you check Remote Analyzer as the protocol, you must also type in a port number under Listen Port .
Listen Port	Only if Remote Analyzer is checked, type the number of the port on which the Recorder <i>listens</i> to (that is, communicates with) the IP Analyzer. The Port field is available only for the Remote Analyzer protocol. The port number specified should match the port in the Analyzer Call Control Protocol configuration as described in Create a Call Control Recorder Group (page 259) .

3. Click **Save**.

Related topics

[Configure capture settings for NICs \(page 241\)](#)

[NIC settings for interception recording \(page 242\)](#)

[Configure network cards and filters \(page 243\)](#)

[Configure IP recording settings \(page 249\)](#)

Configure IP recording settings

Configure IP recording settings to tell the Recorder the settings to be used on NICs for the capture of calls. These settings include timing parameters, VOX detection, RTP, and extension mapping settings.

Procedure

- Click **General Setup >Capture Settings > IP Recording**.

CAPTURE SETTINGS

STATUS | SYSTEM MANAGEMENT | OPERATIONS | ALARMS | GENERAL SETUP
Cards and Filters • Protocols • IP Recording

IP RECORDING SETTINGS: Configure Settings for IP Capture

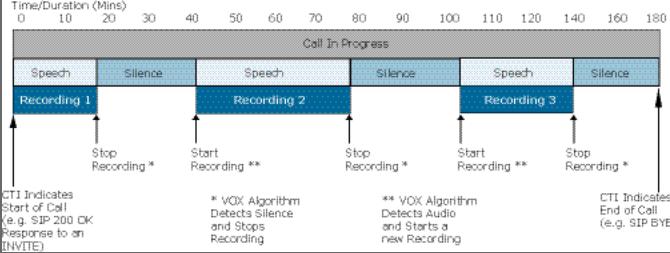
- Timing Parameters**
 - Call Timeout (seconds): 60
 - Long Call Timeout (seconds): 2000
 - Max Record Time (seconds): 3600
 - Long Call Max Record Time (seconds): 600
 - Skinny No Audio Timeout (seconds): 7200
 - SIP No Audio Timeout (seconds): 7200
 - H323 No Audio Timeout (seconds): 7200
- Suppress Silence Recording**
 - Silence Detection: Long Calls
 - VOX Detection: Enabled
 - VOX Detect Level (dB): -45
 - Start Trigger Duration (milliseconds): 250
 - Stop Trigger Duration (milliseconds): 5000
- RTP Detection**
 - Detect RTP: System Default
- Extension to IP Mapping**
 - Static Mapping: Enabled
 - Persist Dynamic Mapping: Disabled
 - Persist Interval (minutes): 0

Save Revert

- Complete the following fields:

Item	Description
Timing Parameters	
Call Timeout (seconds)	Type the number of seconds after which call recording will time out. This setting determines how long, after seeing the first RTP packet, that the IP capture engine will keep a call active before timing out. The call is timed out only if all streams involved in the call do not detect RTP for this duration.

Item	Description
Long Call Timeout (seconds)	Type the number of seconds representing how long the IP capture engine must keep a Speaker Call/Turret Call active, when no audio is detected, before timing out. Long Calls will be timed out only if all the streams involved in the call do not detect RTP for this duration.
Max Record Time (seconds)	<p>This is the maximum time for which any given call should be recorded. Type a value in seconds.</p> <p>This setting does not apply to IP video recording. For IP video recording, specify the maximum video recording time from the settings screen of the IP Recorder Video server role. To access this settings screen, select System Management > Enterprise > Settings, and select the IP Recorder Video server role.</p>
Long Call Max Record Time (seconds)	<p>This is how long the IP capture engine will record a call before it breaks recordings into segments. See the <i>Call Flow Guide</i> for more information. Type a value in seconds.</p> <p>This setting does not apply to IP video recording. For IP video recording, specify the maximum size that a video recording can reach before it is broken into segments from the settings screen of the IP Recorder Video server role. To access this settings screen, select System Management > Enterprise > Settings, and select the IP Recorder Video server role.</p>
Skinny No Audio Timeout (seconds)	Type the maximum number of seconds representing how long, from the Call Start message to the first Real Time Protocol (RTP) packet, that the IP Capture Engine keeps a call active before timing out. The call is timed out only if all the streams involved in the call do not detect RTP for this duration.
SIP No Audio Timeout (seconds)	Type the maximum number of seconds representing how long, from the Call Start message to the first Real Time Protocol (RTP) packet, that the IP Capture Engine keeps a call active before timing out. The call is timed out only if all the streams involved in the call do not detect RTP for this duration.
H.323 No Audio Timeout (seconds)	Type the maximum number of seconds representing how long, from the Call Start message to the first Real Time Protocol (RTP) packet, that the IP Capture Engine keeps a call active before timing out. The call is timed out only if all the streams involved in the call do not detect RTP for this duration.
Suppress Silence Recording	

Item	Description
Silence Detection	<p>The Suppress Silence Recording feature identifies periods of silence in order to prevent the recording of long periods of silence on speaker channels, allowing a reduction in the amount of storage space utilized. It is only intended for use in specific trading environments.</p> <p>Set the type of calls to which Silence Detection should apply.</p> <ul style="list-style-type: none"> • Long Calls—Silence Detection is only used for speaker calls. This should be used in production. • All Calls—Silence Detection is used for all calls. This should be used only for testing purposes. • Disabled—Silence Detection will not be used.
VOX Detection	<p>Select this check box to use VOX as the method of detecting silence on the phone line. This setting should be used together with the Silence Detection parameter (above).</p>  <p>G.711 VOX Detection is supported.</p> <p>i VOX Detection should be enabled only when Silence Suppression is not enabled in the VOIP environment, and the audio codec in use is G.711.</p>
Vox Detect Level (dB)	<p>Move the slider to the left or right to reach the desired level of decibels for VOX detection. Default -45. This setting determines the sensitivity of the VOX detection algorithm in determining whether a sound should be considered audio, or simply low-level background noise and effectively rated as silence.</p> <p>VOX Detection must be enabled in order to use this setting.</p>

Item	Description
Start Trigger Duration (milliseconds)	<p>Defines the interval (milliseconds) when sound needs to be above the threshold before the VOX method identifies a call. The threshold is configurable on each channel. Change the value in increments of 28 by sliding the bar.</p> <p>Required. Range: 0 to 5000. Default: 250.</p> <p>Setting this value too low can cause occasional clicks or background noise to trigger recording. Setting the value too high can cause some audio not be recorded after a period of silence. This setting is similar to the Turn On time in TDM recording. VOX Detection must be enabled to use this setting.</p>
Stop Trigger Duration (milliseconds)	<p>Type a value in milliseconds to determine how long a continuous period of silence must be detected for before recording stops. Setting this value too low can result in the call being stopped after even a small pause in audio. VOX Detection must be enabled in order to use this setting.</p>
RTP Detection	
Detect RTP	<p>Choose a method to determine when to use Real-Time Protocol (RTP) detection to record calls. RTP detection works together with Recorder call control protocols and CTI. Options are:</p> <ul style="list-style-type: none"> • Always—RTP detection is enabled irrespective of any associated member group's Recorder Fallback Type configuration. • System Default—Behavior will be dependent on the associated member group's Recorder Fallback Type configuration (set in Enterprise Manager). If any associated member group's Recorder Fallback Type is set to "On CTI Disconnection (Performance)" or "Always (Liability)," RTP detection is enabled. • Never—RTP detection is not enabled.
Extension to IP Mapping	
Static Mapping	<p>Select this check box to enable static extension to IP mapping—this will retrieve mapping from a static file within the system.</p> <p>i If you want to stop recording on an extension removed from mapping, you must restart the capture engine.</p> <p>A Static Mapping should be used only if specifically documented as required for the integration (check the appropriate integration guide) or under direct Product House guidance.</p>
Persist Dynamic Mapping	<p>Select this check box to stipulate that IP Capture update mapping dynamically. By default this is disabled.</p>

Item	Description
Persist Interval (minutes)	Type a number representing the frequency in minutes at which to persist Dynamic Extension to IP mapping into the system. Typing 0 (zero) means this will occur as soon as an update is available. Typing 5, for example, means that the persist will occur once every 5 minutes.

3. Click **Save**.

Related topics

- [Configure capture settings for NICs \(page 241\)](#)
- [NIC settings for interception recording \(page 242\)](#)
- [Configure network cards and filters \(page 243\)](#)
- [Configure network protocols \(page 247\)](#)

IP Analyzer configuration

The IP Analyzer is used to span control traffic in a remote location to the Recorders such that it can provide call control data (call metadata) that the Recorders would not see otherwise. This process enables Recorders to record audio from one area of the network and the call control protocol from a different area.

Related topics

- [View Analyzer \(page 254\)](#)
- [Manage Analyzer \(page 255\)](#)
- [Analyzer setup \(page 256\)](#)
- [Configure Call Control \(page 257\)](#)
- [View Call Control information \(page 258\)](#)
- [Create a Call Control Recorder Group \(page 259\)](#)
- [Edit a Call Control Recorder Group \(page 260\)](#)

View Analyzer



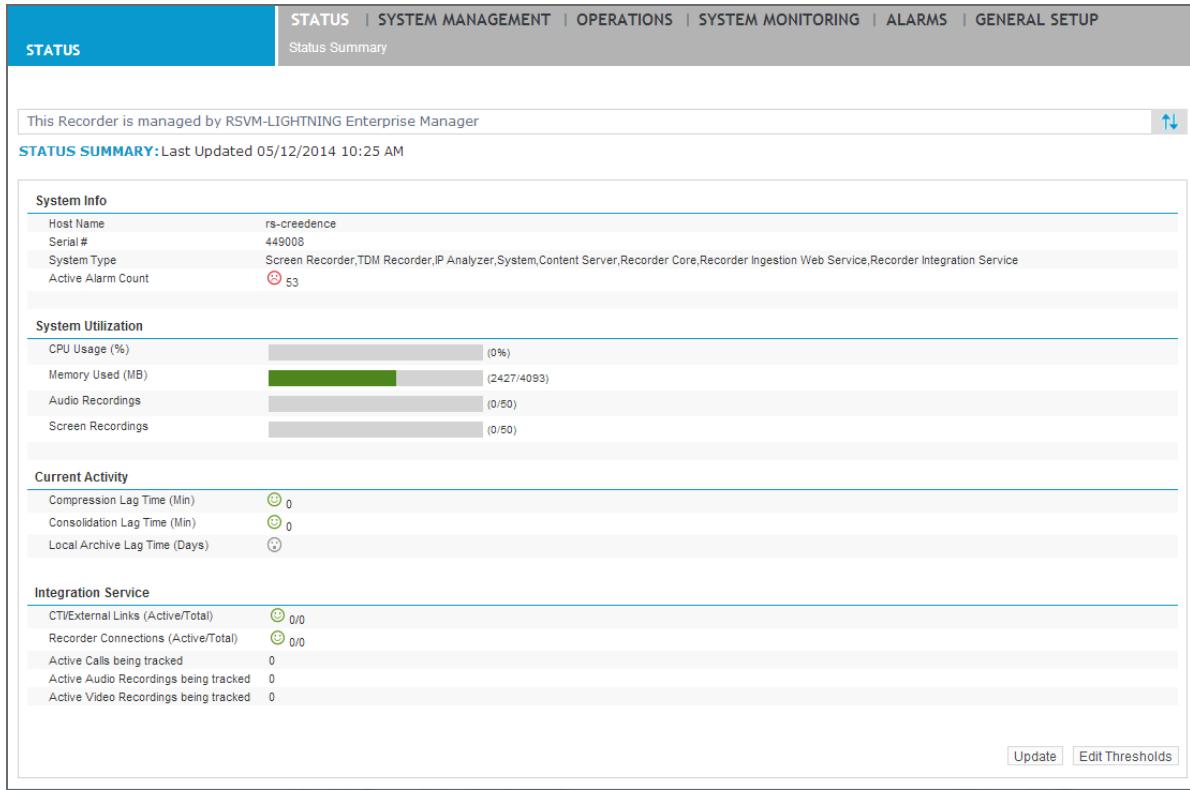
IP Analyzer cannot run with IP Capture; therefore, you cannot have both the IP Recorder and IP Analyzer roles enabled on the same Recorder server.

Access Analyzer

1. In Enterprise Manager, click **System Management > Settings**. Select a Recorder Server and then click **Server Roles**.
2. Enable the **IP Analyzer** role and click **Save**.
3. Launch **Recorder Manager**. This instance of Recorder Manager will now function as an IP Analyzer.

View Analyzer Status

1. On the Analyzer server, in Recorder Manager, click **Status > Status Summary**.



Related topics

- [View Analyzer Status \(page 255\)](#)
- [Manage Analyzer \(page 255\)](#)
- [Analyzer setup \(page 256\)](#)
- [Configure Call Control \(page 257\)](#)
- [View Call Control information \(page 258\)](#)
- [Create a Call Control Recorder Group \(page 259\)](#)
- [Edit a Call Control Recorder Group \(page 260\)](#)

Manage Analyzer

Use Recorder Manager to perform analyzer management functions that enable Analyzer, an optional component in the recording system, to integrate with the IP Recorder. This includes all the familiar tasks you can perform in Recorder Manager, such as managing alarms and users, except that all tasks relate only to the Analyzer.

If your recording system is controlled by the Enterprise Manager, permissions can be assigned to the Analyzer, which is another form of an Installation, limiting who can access this server. You must

therefore have the requisite security authorization to access Analyzer. See:

- [Start and Stop Analyzer Services \(page 256\)](#)
- [Analyzer setup \(page 256\)](#)

Start and Stop Analyzer Services

Use the following procedure to start and stop analyzer services.

1. On the Analyzer server, in Recorder Manager, click **Operations > Start and Stop**.
2. Do one of the following:
 - Select one or more components or click **Select All**, and then click **Start** or **Stop** to start or stop the selected component(s). The Start or Stop operation does not execute for the **Disabled** Start Type. Start, Stop, and Edit options are not available for components that require a restart.
 - With a running component selected, click **Edit** to change to the startup type.
 - For components that cannot be started or stopped, such as Tomcat Services, click **Restart** to restart that component.
3. Click **Reboot** to reboot the server.



To configure notification for Analyzer alarms, start Recorder Manager and click **Alarms**.

Related topics

[View Analyzer \(page 254\)](#)

[Analyzer setup \(page 256\)](#)

[Configure Call Control \(page 257\)](#)

[View Call Control information \(page 258\)](#)

[Create a Call Control Recorder Group \(page 259\)](#)

[Edit a Call Control Recorder Group \(page 260\)](#)

Analyzer setup

You can view Analyzer settings, save and export the analyzer's configuration file, import files from other sources, and type call control and network settings.

To view Analyzer settings

1. On the Analyzer server, in Recorder Manager, click **General Setup > Recorder Settings**.

To add Analyzer Recorder groups and IP addresses

Add Recorder groups and IP addresses using Recorder Manager to identify groups of Recorders within the network, to indicate the IP Gateway switch that supplies IP traffic to the group, and to type the IP addresses of the Recorders within the group.

1. On the Analyzer server, in Recorder Manager, click **General Setup > Call Control**.
2. Follow procedures as described in [Configure Call Control \(page 257\)](#).

To create Analyzer network settings

Add Recorder groups and IP addresses using Recorder Manager to identify groups of Recorders within the network, to indicate the IP Gateway switch that supplies IP traffic to the group, and to type the IP addresses of the Recorders within the group.

1. On the Analyzer server, in Recorder Manager, click **General Setup > Capture Settings > Cards and Filters**.
2. Follow procedures as described in [Configure capture settings for NICs \(page 241\)](#).

Related topics

[View Analyzer \(page 254\)](#)

[Manage Analyzer \(page 255\)](#)

[Configure Call Control \(page 257\)](#)

[View Call Control information \(page 258\)](#)

[Create a Call Control Recorder Group \(page 259\)](#)

[Edit a Call Control Recorder Group \(page 260\)](#)

Configure Call Control

Configure Call Control in Analyzer to set up call control parameters so that the call control messages for IP calls are routed to the Recorders associated with the voice gateways where the calls will go through. Call Control is available only if an Analyzer is installed. Analyzer forwards SCCP/SIP/Avaya (H.323), based upon the IP address of the gateway, to the Recorder specified by its IP address.

Before configuring Call Control, you should have a network diagram showing all Gateway IP addresses and Server names and Ports.

Related topics

[View Call Control information \(page 258\)](#)

[Create a Call Control Recorder Group \(page 259\)](#)

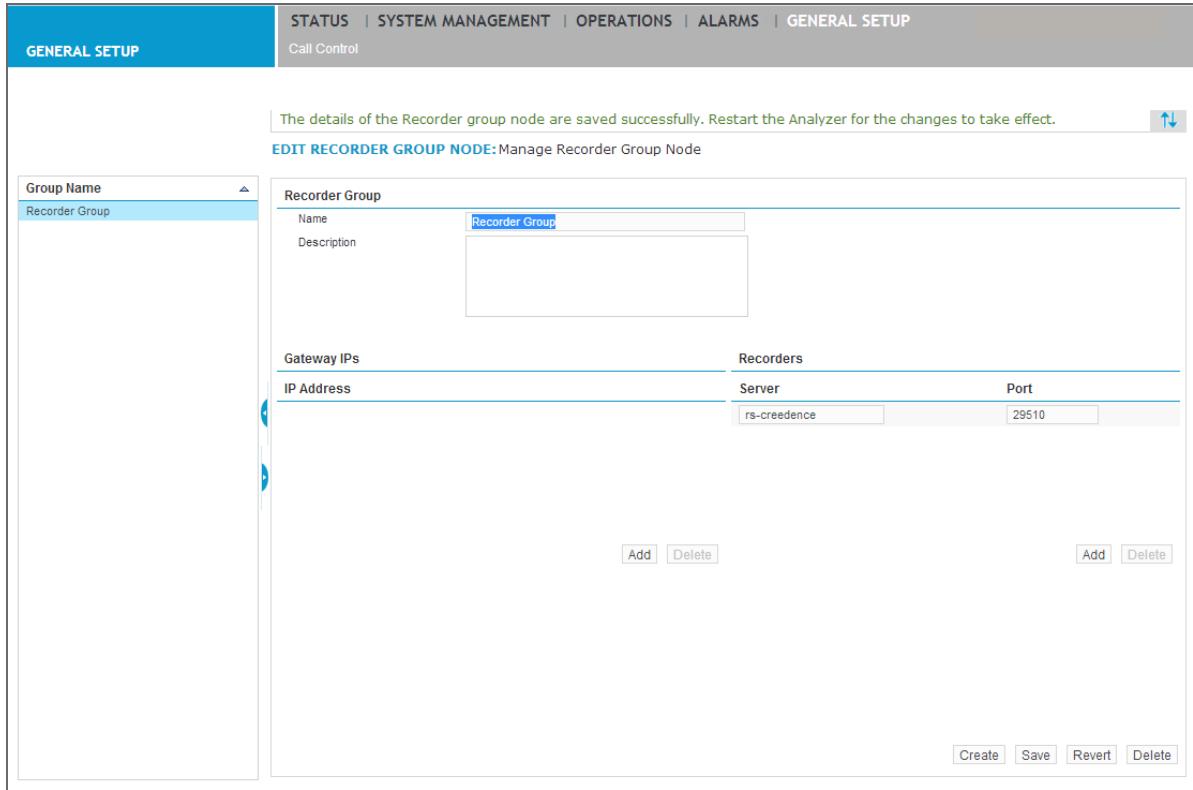
[Edit a Call Control Recorder Group \(page 260\)](#)

View Call Control information

View call control information in Recorder Manager to obtain a summary of recording groups and Gateways in your IP recording environment. You can also view details of each Recorder group, which includes IP Addresses of the targeted Gateway, and IP addresses of the Recorders in the group.

Procedure

1. On the Analyzer server, in Recorder Manager, click **General Setup > Call Control**.



2. Click a group to display editable details of that group, described in [Create a Call Control Recorder Group \(page 259\)](#).

Related topics

- [View Analyzer \(page 254\)](#)
- [Manage Analyzer \(page 255\)](#)
- [Analyzer setup \(page 256\)](#)
- [Configure Call Control \(page 257\)](#)
- [Create a Call Control Recorder Group \(page 259\)](#)
- [Edit a Call Control Recorder Group \(page 260\)](#)

Create a Call Control Recorder Group

Create a Call Control Recorder Group to identify gateway IP addresses and Recorders that are associated with the recording of IP calls within the group.

Procedure

1. On the Analyzer server, in Recorder Manager, click **General Setup > Call Control**. The Call Control window appears.
2. Click **Create**.

The screenshot shows the 'CREATE RECORDER GROUP NODE' dialog box. At the top, there's a header bar with tabs: STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP. The GENERAL SETUP tab is selected. Below the header, the title 'CREATE RECORDER GROUP NODE: ⚠' is displayed. To the left is a sidebar titled 'Group Name' containing a single item: 'Recorder Group'. The main area is divided into two sections: 'Recorder Group' and 'Gateway IPs'. The 'Recorder Group' section contains fields for 'Name' (with an empty input field) and 'Description' (with an empty input field). The 'Gateway IPs' section has a table with columns: 'IP Address', 'Recorders', 'Server', and 'Port'. There are 'Add' and 'Delete' buttons at the bottom of each column. At the very bottom right of the dialog are 'Save', 'Cancel', and 'Revert' buttons.

3. Complete the Recorder Group fields as follows:

Item	Description
Name	Type a name for the Recorder group.
Description	Type a description (optional) of the Recorder group.

Item	Description
Gateway IPs	<p>Click Add, and type the IP address of the Gateway whose SCCP, SIP, or Avaya (H.323) traffic you want forwarded to the remote Recorder, as in the following example: 10 . 3 . 4 . 5. Click Add after each entry to create a new line that will accept a new IP address. The Gateway is the endpoint that the Recorder Group will see RTP traffic for.</p> <p>To delete Gateway information, select it, then click Delete.</p>
Recorders	<p>Click Add, and type the IP address of the Recorder that is to receive that Gateway's SCCP/SIP/Avaya (H.323) traffic, along with the port number, as in the following example: 10 . 3 . 5 . 62 : 3030. Click Add after each entry to create a new line that will accept new information.</p> <p> The port number must be a numeric value between 1024 and 65355.</p> <p>To delete Recorder information, select it, then click Delete.</p>

4. Click **Save**

The Recorder group is added to the Group Name pane on the left.

Related topics

[View Analyzer \(page 254\)](#)

[Manage Analyzer \(page 255\)](#)

[Analyzer setup \(page 256\)](#)

[Configure Call Control \(page 257\)](#)

[View Call Control information \(page 258\)](#)

[Edit a Call Control Recorder Group \(page 260\)](#)

Edit a Call Control Recorder Group

Edit Recorder Group information to change a Recorder group name or description, or to type new call control gateway or Recorder information. All editing is done in real time and there is no Edit button.

Procedure

1. Click **General Setup > Call Control** and in the Recorder Group pane on the left, select a Recorder group.

The screenshot shows the 'Edit Recorder Group Node' screen in the IP Analyzer configuration. The top navigation bar includes links for STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP, with 'GENERAL SETUP' being the active tab. Below the navigation is a 'Call Control' section. A success message at the top right states, 'The details of the Recorder group node are saved successfully. Restart the Analyzer for the changes to take effect.' The main content area is titled 'EDIT RECORDER GROUP NODE: Manage Recorder Group Node'. It contains two tabs: 'Recorder Group' and 'Recorders'. The 'Recorder Group' tab is selected, showing fields for 'Name' (set to 'Recorder Group') and 'Description'. The 'Recorders' tab shows a table with one row, where 'IP Address' is 'rs-creedence' and 'Port' is '29510'. At the bottom are 'Add' and 'Delete' buttons for the recorders, and 'Create', 'Save', 'Revert', and 'Delete' buttons for the group.

2. Edit any displayed information.
3. Click **Save**.

Related topics

- [View Analyzer \(page 254\)](#)
- [Manage Analyzer \(page 255\)](#)
- [Analyzer setup \(page 256\)](#)
- [Configure Call Control \(page 257\)](#)
- [View Call Control information \(page 258\)](#)
- [Create a Call Control Recorder Group \(page 259\)](#)

Backup and recover for recorder configuration

The following sections describe how to:

- backup the recorder system configuration by exporting it
- recover the system after a failure by importing a backed-up configuration

The components for which configuration settings are included in a backup are as follows:

- Archiver
- TDM Capture
- Compressor
- Consolidator
- Disk Manager
- General Recorder
- IP Capture
- IP Analyzer
- Screen Capture
- Integration Service
- Recorder Manager
- Enterprise Manager Agent

Related topics

[Back up the Recorder configuration \(page 262\)](#)

[Recover the Recorder configuration \(page 263\)](#)

Back up the Recorder configuration

Use the following procedure to export the configuration of an individual recorder to an external location.

Procedure

1. Click **System Management**.
2. Under **Export/Import**, click **Export**.

The screenshot shows the 'EXPORT/IMPORT' tab selected in a top navigation bar. The main content area displays the following information:

EXPORT: Saves the Recorder configuration to a file as a backup.

Current Configurations

System Name	rs-ce
Serial Number	449008

Export

3. Using the name and serial number, confirm that this is the recorder you want to back up, then click **Export**.
4. Click **Save** when prompted to download the configuration as a zip file.
5. Navigate to the location in which to save the backup file.
6. Click **Save**.

Related topics

[Recover the Recorder configuration \(page 263\)](#)

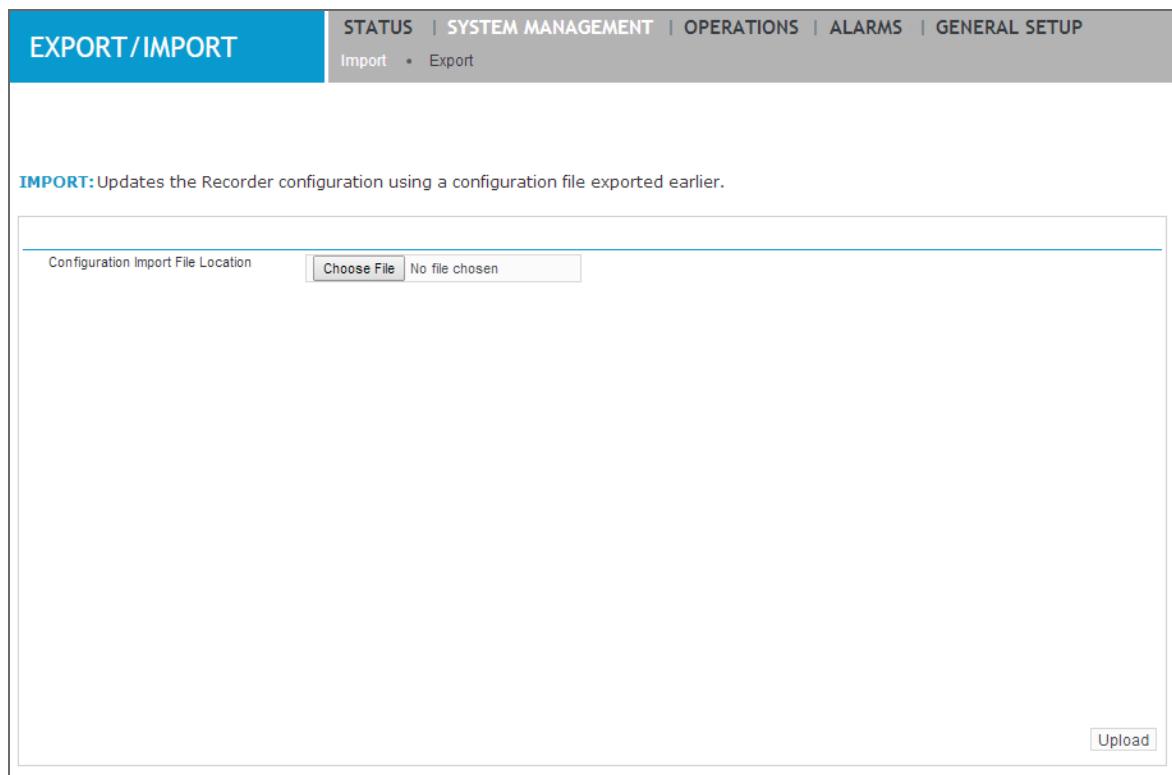
Recover the Recorder configuration

If you have created a backup of your recorder configuration, you can restore it at any time using the following procedure, rather than recreate the configuration manually.

In this procedure, you import a file containing the backed up recorder configuration. The maximum size of the file you can import is 5 MB.

Procedure

1. Click **System Management**.
2. Under **Export/Import**, click **Import**.



3. Click **Browse**, then navigate to the location of the backup configuration zip file.
4. Select the file and click **Open**.
5. Click **Import**.
6. If prompted by the system, reboot recorder.

Related topics

[Back up the Recorder configuration \(page 262\)](#)

Start and stop Recorder components

You may need to start and stop components after a shutdown or to allow a configuration change to take effect. Recorder Manager displays all software components and their current status, and providing tools for working with these settings.

Related topics

- [Start and stop components \(page 265\)](#)
- [Edit component start and stop settings \(page 266\)](#)
- [Restart web services \(page 268\)](#)

Start and stop components

Starting and stopping via the Recorder Manager allows you to:

- start and stop components without interrupting communication with a server
- reestablish communication after a temporary interruption (for example, with a service such as Tomcat)

Procedure

1. Click **Operations > Start and Stop**. The Component Services page appears.

Component Name	Status	Startup Type
Recorder Agent Server	Started	Automatic
Recorder Alarm Service	Started	Automatic
Recorder Archiver Service	Started	Automatic
Recorder Compressor Service	Started	Automatic
Recorder Consolidator Service	Started	Automatic
Recorder Content Server	Started	Automatic
Recorder DiskManager Service	Started	Automatic
Recorder Import Export Engine	Started	Automatic
Recorder Integration Service	Started	Automatic
Recorder IP CaptureEngine	Started	Automatic
Recorder Redundancy Controller	Started	Automatic
Recorder Screen CaptureEngine	Started	Automatic
RecorderTomcat(Restart Only)	Started	Automatic
Recorder Workflow Service	Started	Automatic
WatchDog	Started	Automatic

2. Review the following settings:

Item	Description
Component Name	The name of the installed software component.
Status	The current operational status of the components, either Started or Stopped .
Startup Type	<p>The type of start/stop setting applied to the named software service or component. Can be Automatic (services start automatically whenever the PC is started), Manual, (services start only when the Start button is clicked by a user) or Disabled (services are disabled at startup, requiring that they be edited to change the Start Type before the service can be started).</p> <p>i When the Tomcat Service restarts, it automatically starts services associated with all configured suite server roles, even if the service is disabled. This is a fail-safe feature to ensure the required services are running.</p>

3. Do one of the following:

- Select a component, and then click **Start** or **Stop** to start or stop the selected component. The Start or Stop operation does not execute for the **Disabled** Start Type. Start, Stop, and Edit options are not available for components that require a restart.
- With a running component selected, click **Edit** to change to the startup type. For more information, refer to [Edit component start and stop settings \(page 266\)](#).
- For components that cannot be started or stopped, such as Tomcat Services, click **Restart** to restart that component.
- Click **Reboot** to reboot the server.



You should only reboot the server as an absolute last resort, as calls being recorded or other unfinished processes may be lost.

Related topics

[Edit component start and stop settings \(page 266\)](#)

[Restart web services \(page 268\)](#)

Edit component start and stop settings

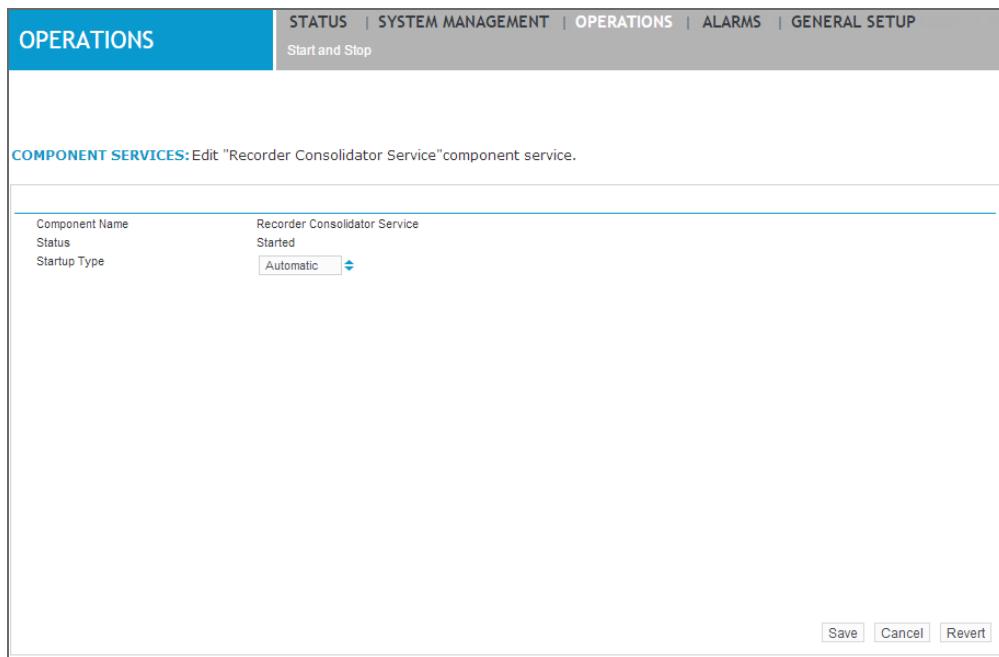
Use the Edit Component option to change Startup Type of individual components. Possible values are Automatic, Manual, or Disabled. Tomcat Service is a Restart only component. Restart only components cannot be edited.

If you are working from Enterprise Manager, verify that your security permissions include editing individual Recorder components within the Recorder Manager.

Procedure

1. Choose **Operations > Start and Stop**, and then select a component.
2. Click **Edit**. The Component Service details page appears.

If the Edit button is disabled, then the component cannot be edited or you do not have sufficient security privileges. For example if you are logged in from Enterprise Manager and you do not have Edit privileges, the Edit button is disabled.



3. For **Startup Type**, select one of the following:

Item	Description
Automatic	The service of the component starts automatically when the system is started. For example, if the system is rebooted, service to the component starts automatically upon the reboot.
Manual	The service of the component must be started manually by selecting the component in the Start and Stop/component window and clicking Start .
Disabled	The service of the component cannot be started either automatically or manually. The component remains disabled until the Start Type is changed to Automatic or Manual .

i When the Tomcat Service restarts, it automatically starts services associated with all configured suite server roles, even if the service is disabled. This is a fail-safe feature to ensure the required services are running.

4. Click **Save**.

Related topics

[Start and stop components \(page 265\)](#)

[Restart web services \(page 268\)](#)

Restart web services

Restart web services manually when the Recorder Manager or Tomcat Service fails to connect automatically to web services.

Procedure

1. Launch Recorder Manager. (If the Recorder Manager or Tomcat start but cannot connect to the web service, the Server Roles error window appears.)
2. Click **Operations > Start and Stop**. The Recorder Component Services window appears.

The screenshot shows the 'OPERATIONS' tab selected in the top navigation bar. Below it, a sub-menu bar includes 'STATUS', 'SYSTEM MANAGEMENT', 'OPERATIONS', 'SYSTEM MONITORING', 'ALARMS', and 'GENERAL SETUP'. The main content area is titled 'COMPONENT SERVICES: List of Component Services and Status on rs-creedence'. It displays a table with three columns: 'Component Name', 'Status', and 'Startup Type'. The table lists various Recorder services, all of which are currently started except for 'WatchDog' which is stopped. At the bottom of the table are buttons for 'Select All', 'Select None', 'Edit', 'Start', 'Stop', 'Restart', and 'Reboot'.

Component Name	Status	Startup Type
Recorder Agent Server	Started	Automatic
Recorder Alarm Service	Started	Automatic
Recorder Archiver Service	Started	Automatic
Recorder Compressor Service	Started	Automatic
Recorder Consolidator Service	Started	Automatic
Recorder Content Server	Started	Automatic
Recorder DiskManager Service	Started	Automatic
Recorder Ingestion Web Service	Started	Automatic
Recorder Integration Service	Started	Automatic
Recorder IP CaptureEngine	Started	Automatic
Recorder Redundancy Controller	Started	Automatic
Recorder Screen CaptureEngine	Started	Automatic
Recorder TDM CaptureEngine	Started	Automatic
RecorderTomcat(Restart Only)	Started	Automatic
Recorder Workflow Service	Started	Automatic
WatchDog	Stopped	Manual

3. Click the **Recorder Tomcat** component, and then click **Restart**.

Related topics

[Start and stop components \(page 265\)](#)

[Edit component start and stop settings \(page 266\)](#)

Set up attributes, tagging, and recording rules

The following sections describe how to set up attributes and custom data for use in tagging and recording rules.

Topics

Attributes configuration workflow	270
Attributes	271
CTI tagging	282
Recording rules	303

Attributes configuration workflow

Use the following procedure to guide you through configuration of recording and tagging on the basis of a business logic that reflects the goals of your enterprise. This workflow is optional.

Workflow sequence

[Workflow: IP-based voice and video recording \(page 33\)](#): Task 7 of 8

Task List

1. For CTI tagging, complete the following procedures:
 - a. [Identify CTI data \(page 282\)](#)
 - b. [Create Custom Data fields \(page 291\)](#)
 - c. [Map Custom Data to an attribute \(page 292\)](#)
 - d. [Map attributes to an adapter \(page 294\)](#)
2. Complete the [Recording rules configuration workflow \(page 303\)](#).

What to do next

Voice recording: [Install and configure Archive \(page 41\)](#)

Attributes

Attributes are used to capture and retrieve interactions based on real criteria associated with employees (such as an Employee ID), contacts (such as number of holds), devices (including extensions) and CTI events (such as a call ID). You can use them to establish the conditions that trigger captures, using recording rules, and to tag interactions, by mapping them to custom data.

There are both standard attributes, which are predefined and have specific values or behaviors, and custom attributes, which are created to serve specific business needs using data present in a particular environment.

Values for standard attributes are pulled from different places. For example, Employee attributes are obtained from the Employee configuration, Contact attributes are collected from information in the contacts, and CTI attributes are received or derived from CTI.

In certain cases attributes won't have values. This can be because configuration is incomplete, there are third-party limitations, or the attributes are simply not applicable to a given environment. If the standard attributes don't contain the data need, you can create new ones.

Error message on the Attributes screen

After a system upgrade, the following error message can display on the Attributes screen:

"The extended custom data migration has not run successfully yet. This migration will run every three minutes until it succeeds. You cannot configure custom data mapping until the migration succeeds."

When the migration succeeds, the error message above is cleared from the screen and you can configure custom data mapping.

If the migration fails continuously, note the following.

The migration is done in two places:

1. In the QM database, which migrates the custom data.
2. In Enterprise Manager, which migrates the custom data to attribute mapping.

Step 2 has a dependency on step 1. In a Level 4 deployment, where the QM/Contact database migration is run later, step 2 cannot complete. Also, if the BPMAINDB and WFO migration runs before the QM and QM database migration, step 2 cannot complete. In both of these cases, the error message displays on the screen. Once step 1 is complete, step 2 is retried in Enterprise Manager, and when the migration is complete, the error message is cleared from the screen.

In the event of an unrecoverable error, you must examine the logs to determine the problem.

Related topics

[Standard attributes \(page 272\)](#)

[Create, edit or delete an attribute \(page 278\)](#)

Standard attributes

The following table lists the standard default attributes used in capturing. You can view the current list of attributes—including both standard and custom—in Enterprise Manager under **Recording Management > Custom Data > Attributes**.

In this release, the character limit for each field for these attributes is 256. If you had previously mapped an attribute to a custom data field because the field length was insufficient in a previous release, you can now remove the mapping and use the custom data field for something else.

- i** While the system evaluates most recording rules on an on-going basis, those attributes in the Contact category are treated differently. Each of these attributes represents a duration or amount, and if a rule is set up to check whether they are less than a specified value, the system does not evaluate the contact on this basis until the contact ends.

Example: If the condition “Time On Hold” is set to “less than 30 seconds”, the system only checks for this value at the end of the interaction, when it is certain there is no more time on hold remaining.

The availability of certain attributes (Call Direction, Called Number, and so on) depends on the following factors,

- For the NFAS protocol (supported on DP cards), all the trunks for a specific NFAS group must be on the same Recorder to process signaling properly.
- For all protocols, certain attributes are available provided they are present on the trunk bearer channel, and that the trunk span is configured to deliver this information.

See the “Recorder” section in the *Technical Overview* for more details.

Category	Attribute	Description
Employee	Employee Group	The group to which the employee belongs.
	Employee ID	The Windows login id used by the employee on the workstation.
	Employee Name	The name of an employee involved in a contact.
	Logged On Duration (seconds)	The amount of time during which an employee is logged on.
	Network ID	The user's network logon ID.
	Organization	The organization of the employee involved in the interaction.
	Skill	The employee skill defined on the switch.
	Supervisor Name	The name of the supervisor associated with a contact.

Category	Attribute	Description
Contact	Contact Duration (seconds)	The duration of the contact in seconds.
	Content Type	The type of media captured. Supported formats are audio (audio/vnd.verint.wav) and screen (screen/vnd.verint.capb).
	Event Type	An event in an interaction, at the Employee, System, or CTI level.
	Exception Reason	You can create a recording rule that marks an interaction meeting the rule criteria as an exception. The Exception Reason field identifies the reason that it is considered an exception.
	Fired Business Rules	Lists recording rules that have been triggered.
	Interaction Type	The type of interaction captured. Valid types "Phone" and "Desktop."
	Number of Conferences	Total number of conferences in the contact.
	Number of Holds	Total number of times that the interaction started tracking a held connection for the user. Overlapping, concurrent held connections count as a single continuous hold.
	Number of Transfers	Total number of transfers that occur over the course of the contact.
	Parties	All parties involved in the current interaction.
	Pause Duration (seconds)	The Pause Duration for the contact.
	Time On Hold (seconds)	The total amount of time, in seconds, that the interaction tracked one or more held connections for the user.
	Wrapup Time	Indicates how much time the employee spent doing work related to the interaction after the interaction ends.

Category	Attribute	Description
CTI	ANI	Automatic number identification or Caller ID.
	Call Direction	The direction of the interaction.
	Call ID	Unique interaction identifier on the switch.
	Call Reference	A reference (any string) sent by the Recorder.
	Call Type	The type of interaction.
	Called Party	Number of the line to which the interaction was directed.
	Called Party Name	Employee name associated to the called party or value provided from the switch in the case of Cisco UCM.
	Calling Party	Number of the line from which the interaction is made.
	Calling Party Name	Employee name associated to the calling party, or value provided from the switch in the case of Cisco UCM.
	DNIS	Dialed number identification service (DNIS). The DNIS identifies the number that the caller dialed, which is useful in call centers to which interactions to multiple numbers may be directed.
	Extended Call History	Provides a history of the interaction states through which the contact has gone.
	Global Call ID	Globally unique call identifier. This is populated in most environments if the switch or CTI infrastructure supports it.
	Module Number	The serial number of the Recorder that captured a contact. When used in recording rules, this attribute will contain the serial numbers of all the different captures in an interaction/session.
	Number Dialed	The actual number dialed by the calling party.
	Queue	The queues configured on the switch.
	Source Platform	The source platform (such as Facebook, WhatsApp, Instagram) from which an Interaction originated. This attribute is populated by integrations with systems that supply interactions from multiple different platforms, such as Conversocial. For this tagging to be available in a database, a Custom Data field must be mapped to the attribute.

Category	Attribute	Description
Device	Data Source Name	The name of the switch from which the contact information originates.
	Device Name	The name of either the primary extension or workstation.
	Extension	The extension of an employee involved in a contact.
	Primary Extension	The primary extension of the phone associated with the capture.
	Serial Number	The serial number of the Recorder for the primary capture of an interaction.
	Workstation	The name of the employee workstation.
Import Export	Extraction Job Name	The name of the extraction job that extracted the interaction.
	Source Call Identifier	The unique identifier provided to the interaction by the source capturing system. This identifier is mapped to ensure that the source identifier of each interaction is maintained when the interaction is extracted.
	Source QM Database Server	Not supported.

Category	Attribute	Description
Public Safety	ALI	The Automatic Location Identifier (ALI) contains the location information, such as the street address or GPS coordinates of the caller.
	CAD ID	The emergency ID supplied by the Computer Aided Dispatch (CAD) software.
	Callback Number	Phone number for calling back the caller.
	Caller Name	The name of the caller.
	Caller Number	The telephone number of the caller.
	Class of Service	One byte Class of Service characters include: V = VoIP Services default Class of Service (preferably with VOIP being displayed at the PSAP) C = VoIP Residential (preferably with VRES being displayed at the PSAP) D = VoIP Business (preferably with VBUS being displayed at the PSAP) E = VoIP Coin/Pay Phone (preferably with VPAY being displayed at the PSAP) F = VoIP Wireless (preferably with VMBL being displayed at the PSAP) J = VoIP Nomadic (preferably with VNOM being displayed at the PSAP) K = VoIP Enterprise Solutions - Centrex and PBX (preferably with VENT being displayed at the PSAP)
	Emergency Service Number	Emergency Service Number (ESN) associated with the house number of the street name of the caller.
	GPS Elevation	GPS elevation coordinate of the mobile caller.
	Latitude	The latitude coordinate of the mobile caller.
	Local Exchange Carrier	The Local Exchange Carrier of the caller.
	Longitude	The longitude coordinate of the mobile caller.
	PSAP ID	The identifier of the Public Safety Answering Point (PSAP) that handled the referenced call.
	PSAP Name	The name of the PSAP that handled the referenced call.
	State Province	The state or province in which the caller is located.
	Street Address	The street address of the caller.

Category	Attribute	Description
Radio	ZIP Code	The zip code of the location of the caller.
	Emergency Call	If the call is an emergency call.
	Radio ID	The ID of the individual radio device on the call.
	Radio Name	The alias of the individual radio device on the call.
	Radio Network ID	Unique network identifier of a radio subsystem.
	Radio System ID	Unique system identifier of a radio subsystem.
	Site	The radio site ID.
	Talk Group ID	The ID of the talk group in a group call.
	Talk Group Name	The alias of the talk group in a group call.
TDM	Zone ID	The radio zone ID.
	Channel Name	Name of the channel on which the call appears. Used for tagging but not in recording rules.
	Channel Number	The channel number on which the call appears.
	DTMF Digits	Dual Tone Multi Frequency (DTMF) Digits apply to the TDM Recorder. DTMF refers to voice-frequency band telephone signaling to call switching centers.
		 The DTMF Digits attribute arrives after the call is completed, and as such will not be effective when used in a recording rule.
	First Message	The first message sent by the Recorder.
	Last Message	The last message sent by the Recorder.
	Third Party	A message sent by the Recorder in some TDM environments.
	Trunk	The trunk that the call is on.
	Trunk Group	The trunk group that the call is on.

Category	Attribute	Description
Trading	Turret Name	The name of a trading turret on a call.
	Turret ID	The unique identifier of a trading turret on a call.
	Trader Group Name	The name of the group to which the trader belongs.
	Trader Group ID	The unique identifier of the group to which the trader belongs.
	Line Name	The name of the line from which the call is made.
	Line ID	The unique identifier of the line from which the call is made.
	Destination Appearance Number	The appearance number of the dialed destination.
	Destination Label	The label of the called destination.
	Recording Reference	A reference to a recording channel.
	Is Mute	Is true if part of the call is not supposed to be captured.

Related topics

[Attributes \(page 271\)](#)

[Create, edit or delete an attribute \(page 278\)](#)

Create, edit or delete an attribute

The Attributes screen in Enterprise Manager lists a set of standard attributes. You can create custom attributes and edit existing attributes for use in both recording rules and tagging. Complete the following procedure to support external attributes in use by a third-party device (such as a CTI switch).

Procedure

1. In Enterprise Manager, go to **Recording Management**.
2. Under **Custom Data**, select **Attributes**.

Name	Description	Tagging Level	Stored	Data Type	Status
Employee Group	Contact Center agent	Session	First value	String64	Enabled
Employee ID	Group of the agent involved in the call	Session	First value	String256	Enabled
Employee Name	Agent identifier who takes call	Session	First value	String128	Enabled
Logged On Duration (seconds)	The agent involved in the call	Session	Last Value	Integer	Enabled
Network ID	Agent logged on duration in seconds on switch	Session	First value	String256	Enabled
Organization	Users network logon id	Session	First value	String128	Enabled
Skill	Organization of the agent involved in the call	Session	First value	String32	Enabled
Supervisor Name	The agent skill defined on the switch configuration	Session	First value	String128	Enabled
Contact	Supervisor of the agent involved in the call	Session	First value	String64	Enabled
Contact Duration (seconds)	Contact	Session	Last Value	Integer	Enabled
Content Type	The contact duration in seconds	Session	Last Value	String100	Enabled
Event Type	Content Type	Session	Last Value	String16	Enabled
Exception Reason	Event in a call (Agent Level/ System Level/ CTI level)	Session	Integer	Enabled	
Fired Business Rules	Indicates the reason the contact is an exception.	Session	Last Value	String128	Enabled
Interaction Type	Contains a list of all business rules that fired for this contact.	Session	Last Value	String100	Enabled
Number Of Conferences	Interaction Type	Session	Last Value	Integer	Enabled
Number Of Holds	Total number of conference in the contact	Session	Last Value	Integer	Enabled
	Total number of holds in the call	Session	Last Value	Integer	Enabled

[Create](#) [Edit](#) [Delete](#)

3. Do one of the following:

- Click **Create** to create a new attribute.
- Select an existing attribute and click **Edit**.

 Existing *custom* attributes appear under the heading **Custom**.

4. Type a unique **Name** (required) and a **Description** (optional) for the attribute. If you are mapping attributes to custom data fields for CTI tagging, you can use the same name for the sake of simplicity. An example of "MyCallId" is used throughout this documentation, as the name of both a Custom Data Field and an Attribute.



The attribute name must not contain any spaces or special characters, and must be limited to US-ASCII characters (that is, the numbers 0 through 9, and the 26 letters of the English alphabet).

In addition, an = (equals sign) is a delimiter that separates a name from its value, and as such should not be used as part of the attribute name.

5. From the drop-down list, select a **Data Type** of Boolean, Integer, or String.

Note that the list of options includes a "DateTime" setting that is not supported for Recording Rules used by the Recorder/Recorder Integration Service. In the context of tagging the DateTime value is treated the same as a String.

- Type a maximum **Size** (that is, number of characters) for the value of the attribute.
- Select the **Enabled** check box to make this attribute available for use.
- Use the **Stored** dropdown box to specify whether you want to store, as the attribute, the first value received during the contact or the last unique value received during the contact. For example, if

you select Last value and the set of values received for CD1 are: AAA, BBB, the last tagged value for CD1 in this interaction will be BBB.

9. Use the **Tagging Level** dropdown box to specify how you want this attribute tagged to an interaction. Tagging Level applies only to custom attributes and certain statistical attributes. The statistical attributes are:
 - Number Of Conferences
 - Number Of Holds
 - Number Of Transfers
 - Pause Duration (seconds)
 - Time On Hold (seconds)



The Tagging Level option is unavailable if it does not apply to a given attribute.

Tagging level options are:

- **Session** — The interaction (also referred to as a session) is tagged with the attribute value that applies only to that interaction. If an attribute is not present in an interaction, the interaction is not tagged with the attribute.
- **Contact** — All interactions (past, present, and future) of a contact are tagged with the same custom attribute value based on the selection of the **Stored** value (first or last).

Tagging Level options control how statistical information is tagged to interactions, and can affect how contacts are located in searches.

The Tagging Level options determine whether the attribute tagged to each interaction contains statistics for the individual interaction or for the entire contact.

If the **Session** value is selected, the CD1 field tagged to Interaction 1 has a value of 30 seconds, and the CD1 field tagged to Interaction 2 has a value of 45 seconds.

If the **Contact** value is selected, the CD 1 field tagged to Interaction 1 has a value of 75 seconds, and the CD 1 field tagged to Interaction 2 also has a value of 75 seconds.

The Tagging Level options can also affect how contacts are located in searches.

To illustrate, assume that a customer account number is stored in the custom attribute, and the following scenario occurs:

- a. A customer calls the contact center and tells Agent 1 their customer account number.
- b. Agent 1 transfers the interaction to Agent 2 (which creates interaction 2 of the interaction). The customer does not mention the customer account number to Agent 2.

In this example, the custom attribute occurred in interaction 1 of the contact, but not in interaction 2.

If the **Session** value is selected, the custom attribute is tagged only to interaction 1. In this case, if the supervisor of Agent 2 can access only the interactions handled by Agent 2, the supervisor cannot find the interaction using the account number as the search criteria.

If the **Contact** value is selected, the custom attribute is tagged to all interactions (both interaction 1 and interaction 2 in this example). In this case, the supervisor of Agent 2 can find the interaction using the account number, even though the account number was never spoken to Agent 2 during interaction 2.

Specifying the **Contact** value ensures that users who do not have privileges to all interactions of an interaction tagged with the custom attribute can locate the interaction when using the attribute as the search criteria.

-  In the case of interactions that are already closed, if Agent 1 takes a call, then transfers it to Agent 2, resulting in data being tagged to the interaction, when the Tagging Level is "Contact," any interactions associated with the contact that are already closed will be updated as well.
 -  If an attribute has a Tagging Level of Session, you can view related statistics for contacts in the Interactions application. See the Interactions documentation for more information.
10. If the Data Type is an Integer or String, you can set up lookup mapping. Lookup mapping allows you to associate internal fields with meaningful terms that can be used in recording rules or elsewhere. For example, if you have fields that are represented by numeric codes, you may want to map them to names that convey what each field actually represents.
You could map the numeric value of a resolution code to the name of the issue it represents (such as "Agent Hangup" or "Wrong Department").
- a. Click **Add LookupMapping**.
 - b. In the **Field Value** field, type the internal name of the field. See [Identify CTI data \(page 282\)](#) for information on how to determine what these internal names are.
 - c. In the **Lookup Value** field, type a name that conveys what the internal name represents (for example, the actual name of a company rather than a numeric code that represents that company).
11. Click **Save**.

To delete an attribute

You can only delete custom attributes.

In Enterprise Manager, click **Recording Management > Custom Data > Attributes**.

Select an existing attribute and click **Delete**.

Related topics

[Standard attributes \(page 272\)](#)

[Attributes \(page 271\)](#)

CTI tagging

CTI tagging allows you to take call data and turn it into actionable information within applications such as Interactions.

Complete the following procedures in sequence in order to:

- Identify CTI events and bring them into the system as custom data.
- Link this custom data to attributes.
- Map the attributes to the Integration Service adapter so that it may tag call recordings based on events.



Third-party fields may be case-sensitive, and at a minimum must match those in use character-for-character, so always use caution when working with these values.

Related topics

[Identify CTI data \(page 282\)](#)

[Create Custom Data fields \(page 291\)](#)

[Map Custom Data to an attribute \(page 292\)](#)

[Map attributes to an adapter \(page 294\)](#)

Identify CTI data

Third-party CTI fields are based on events received from the switch. You can identify the third-party CTI attributes available for use by examining the Integration Service logs.

Before you begin

Configure the Recorder and an Integration Service adapter.

Procedure

1. Ensure that the log Trace Level is set to DebugHigh:
 - a. On the server where the Integration Service is installed, go to **<install software dir>\ContactStore\LogManager.exe**.
 - b. Run the Log Manager.
 - c. Select the IntegrationService component and set **Trace Level** to **DebugHigh**.
2. Go to **<datadir>/logs** and open the Integration Service log file.
3. Locate the CTI event in question.

Events from the integration target a destination of "CallTracker" within the system. To find CallTracker events, filter the log for lines that look like:

--> <CallTracker>

If there are multiple adapters configured in the system, the source information (for example, the "si.1" field from the **<si.1> --> <CallTracker>** log line) can be used for additional filtering.

4. Locate the desired data from within the message.

All data within a message is held within a named Field. Each Field is tracked within either a Folder or an Array. To extract data from a Field, the entire path to that Field must be defined.



The names of fields, folders, and arrays are case-sensitive when defining a mapping.

Example 1: CTI events

The following is an example CTI event from Adapter 2 sent into the CallTracker for processing. In this case, the customer wants to extract the call id and the calling party display name.

```

1 Dispatching Event CTI Event<si.2> --> <CallTracker> Size<2>Int<AdapterId> = 2 ;
Str<AdapterName> = JTAPI ; Int<SwitchId> = 304 ; Str<SwitchName> = Cisco ;
Int<eventId> = 116

2 Str<description> = TermConnCreatedEv SEP68BDABA4568B

3 Folder<event>

4 Int<ciscoCause> = 100 ; Str<ciscoCauseStr> = CAUSE_INVALIDIECONTENTS ;
Int<ciscoFeatureReason> = 12 ; Str<ciscoFeatureReasonStr> = REASON_NORMAL

5 Int<callId> = 16865573

6 Folder<ciscoCallIdentifiers>

7 Int<ciscoCallId> = 16865573 ; Int<ciscoCallManagerId> = 1 ;
Int<ciscoGlobalCallId> = 88357

8 Folder<calledPartyInfo>

9 Str<displayName> = ; Str<unicodeDisplayName> =

10 Folder<callingPartyInfo>

11 Str<address> = 8614 ; Str<displayName> = 8614 SCCP Tier3 DMS ;
Str<unicodeDisplayName> = 8614 SCCP Tier3 DMS

12 Folder<terminalConnection>

13 Int<termConnState> = 67 ; Int<callControlTermState> = 98 ; Int<connState> = 51
; Int<callControlState> = 84 ; Str<terminalAddress> = 8614/SEP68BDABA4568B

14 Array<connections> [1]

15 [0]: Str<terminalAddress> = 8614/SEP68BDABA4568B ; Int<callControlState> = 84 ;
Int<termConnState> = 67 ; Int<connState> = 51 ; Int<callControlTermState> = 98

```

In the CTI Event example, the following fields were identified for extraction:

On Line 7: **Int<ciscoCallId> = 16865573**

On Line 11: ; **Str<unicodeDisplayName> = 8614 SCCP Tier3 DMS**

- Identify the full path to the **ciscoCallId** field. To find the path, work up from the **ciscoCallId** field and identify all of the folders and arrays above it. In the example, the **ciscoCallId** field is within the **ciscoCallIdentifiers** folder, which is contained within the **event** folder. There is no folder above the **event** folder. So, to access this field, the mapping is **event.ciscoCallIdentifiers.ciscoCallId**.
- Identify the full path to the **unicodeDisplayName** field. To find the path, work up from the **unicodeDisplayName** field and identify all of the folders and arrays above it. **unicodeDisplayName** is within a folder named **callingPartyInfo**, which is within the **event** folder. To extract this name, the mapping is **event.callingPartyInfo.unicodeDisplayName**.

Example 2: CTI events in unknown array index

The following CTI event from Verint Adapter 2 was sent to the CallTracker service for processing. In this case, our customer wants to identify the agent and the customer in a call. Although there are several tags that could be used, the agent's email address and the customer's telephone number offer unique values.

```
1 [IEMessage |295C|H] 2024-07-17 13:23:30.261-04:00 Dispatching <Event>
  CTIEvent<si.2> --> <CallTracker> Size<0>

2   Int<AdapterId> = 2 ; Str<AdapterName> = Genesys Cloud CX API Adapter ;
   Int<SwitchId> = 201 ; Str<SwitchName> = Genesys_TenantB_QA ;
   Str<MonitoredDevice> = Agent01@myContactCenter.com ; Str<version> = 2

3   Str<topicName> = v2.users.443c901d-5406-405d-8ca3-f0041da44613.conversations

4   Folder<eventBody>

5     Str<id> = 51123a71-1f50-490d-b79c-ab18f506b755 ; Str<recordingState> =
active ; Str<address> = tel:+18881231234 ; Str<utilizationLabelId> = 631f0939-
be32-495a-baf9-970abb039192 ; Bool<securePause> = false

6     Array<participants> [4]

7       [0]: Folder<attributes>

8         [0]: Str<id> = b4434aed-a6ff-458c-b6b7-79312041e850 ; Str<connectedTime> =
2024-07-17T17:23:11.103Z ; Str<endTime> = 2024-07-17T17:23:24.976Z ; Str<name> =
Agent01 call flow ; Str<purpose> = ivr ; Bool<wrapupRequired> = false

9         [0]: Str<address> = sip:a1b8db7d-9e3d-4dbd-a8b2-
47d3eeef1630@127.0.0.1;language=en-US;user=ivr ; Bool<wrapupExpected> = false

10        [0]: Array<calls> [1]
```

```

11      [0]: [0]: Str<id> = 652d297b-1cc1-475d-85e1-436c3675f634 ; Str<state> =
terminated ; Str<initialState> = offering ; Bool<recording> = false ;
Str<recordingState> = none ; Bool<muted> = false ; Bool<confined> = false ;
Bool<held> = false

12      [0]: [0]: Bool<securePause> = false ; Str<disconnectType> = transfer ;
Str<direction> = inbound ; Str<provider> = Edge ; Str<peerId> = 517bc150-72d9-
4359-9118-e4e0360c3dfe ; Str<connectedTime> = 2024-07-17T17:23:11.103Z

13      [0]: [0]: Str<disconnectedTime> = 2024-07-17T17:23:24.976Z ;
Bool<afterCallWorkRequired> = false

14      [0]: [0]: Folder<self>

15      [0]: [0]: Str<name> = Hasbrouck Heights NJ ; Str<nameRaw> = Hasbrouck
Heights NJ ; Str<addressNormalized> = sip:a1b8db7d-9e3d-4dbd-a8b2-
47d3eeef1630@127.0.0.1;language=en-US;user=ivr ; Str<addressDisplayable> =
unavailable

16      [0]: [0]: Str<addressRaw> = sip:a1b8db7d-9e3d-4dbd-a8b2-
47d3eeef1630@127.0.0.1;language=en-US;user=ivr

17      [0]: [0]: Folder<other>

18      [0]: [0]: Str<name> = Robert Smith ; Str<nameRaw> = Robert Smith ;
Str<addressNormalized> = tel:+15551231234 ; Str<addressRaw> =
sip:+15551231234@10.87.6.151;user=phone ; Str<addressDisplayable> = unavailable

19      [0]: Folder<workflow>

20      [0]: Str<workflowId> = 44f92b9f-0524-469c-805d-58924c24feef

21      [1]: Folder<attributes>

22      [1]: Str<id> = 01d6aa4d-8259-4373-be8b-4f8eac6b27f4 ; Str<connectedTime> =
2024-07-17T17:23:11.280Z ; Str<externalContactId> = 7287af43-0211-4652-9caa-
d989c7b1a3f7 ; Str<name> = Robert Smith ; Str<purpose> = customer

23      [1]: Str<queueId> = 25d389d7-30ac-46d0-8284-432acf0c7b4a ; Str<address> =
tel:+15551231234 ; Bool<wrapupRequired> = false ; Bool<wrapupExpected> = false

24      [1]: Array<mediaRoles> [1]

25      [1]: [0]: Str<mediaRoles> = full

26      [1]: Array<calls> [1]

27      [1]: [0]: Str<id> = 517bc150-72d9-4359-9118-e4e0360c3dfe ; Str<state> =
connected ; Str<initialState> = offering ; Bool<recording> = true ;
Str<recordingState> = active ; Bool<muted> = false ; Bool<confined> = false ;
Bool<held> = false

```

```
28      [1]: [0]: Bool<securePause> = false ; Str<direction> = inbound ;
Str<provider> = Edge ; Str<connectedTime> = 2024-07-17T17:23:11.280Z ;
Bool<afterCallWorkRequired> = false
29      [1]: [0]: Folder<self>
30      [1]: [0]: Str<name> = Robert Smith ; Str<nameRaw> = ;
Str<addressNormalized> = tel:+15551231234 ; Str<addressRaw> =
sip:+15551231234@10.87.225.68 ; Str<addressDisplayable> = unavailable
31      [1]: [0]: Folder<other>
32      [1]: [0]: Str<name> = Hasbrouck Heights NJ ; Str<nameRaw> = ;
Str<addressNormalized> = tel:+18881231234 ; Str<addressRaw> =
sip:+18881231234@10.87.6.151:8140;transport=tcp ; Str<addressDisplayable> =
unavailable
33      [2]: Folder<attributes>
34      [2]: Str<id> = 88365632-9039-4a32-acbe-26ef398cbbbd ; Str<connectedTime> =
2024-07-17T17:23:25.032Z ; Str<name> = Agent01 queue ; Str<queueId> = 25d389d7-
30ac-46d0-8284-432acf0c7b4a ; Str<purpose> = acd ; Bool<wrapupRequired> = false
35      [2]: Str<address> = sip:25d389d7-30ac-46d0-8284-
432acf0c7b4a@127.0.0.1;language=en-US;user=acd ; Bool<wrapupExpected> = false
36      [2]: Folder<conversationRoutingData>
37      [2]: Folder<language>
38      [2]: Byte<priority> = 0
39      [2]: Folder<queue>
40      [2]: Str<id> = 25d389d7-30ac-46d0-8284-432acf0c7b4a
41      [2]: Array<calls> [1]
42      [2]: [0]: Str<id> = 8a62f071-98cb-48c3-aa5f-9b917a597af1 ; Str<state> =
connected ; Str<initialState> = offering ; Bool<recording> = false ;
Str<recordingState> = none ; Bool<muted> = false ; Bool<confined> = false ;
Bool<held> = false
43      [2]: [0]: Bool<securePause> = false ; Str<direction> = inbound ;
Str<provider> = Edge ; Str<peerId> = 517bc150-72d9-4359-9118-e4e0360c3dfe ;
Str<connectedTime> = 2024-07-17T17:23:25.032Z ; Bool<afterCallWorkRequired> =
false
44      [2]: [0]: Folder<self>
```

```
45      [2]: [0]: Str<name> = Agent01 queue ; Str<nameRaw> = Agent01 queue ;
Str<addressNormalized> = sip:25d389d7-30ac-46d0-8284-
432acf0c7b4a@127.0.0.1;language=en-US;user=acd ; Str<addressDisplayable> =
unavailable
46      [2]: [0]: Str<addressRaw> = sip:25d389d7-30ac-46d0-8284-
432acf0c7b4a@127.0.0.1;language=en-US;user=acd
47      [2]: [0]: Folder<other>
48      [2]: [0]: Str<name> = Robert Smith ; Str<nameRaw> = Robert Smith ;
Str<addressNormalized> = tel:+15551231234 ; Str<addressRaw> =
sip:+15551231234@10.87.6.151;user=phone ; Str<addressDisplayable> = unavailable
49      [3]: Folder<attributes>
50      [3]: Str<id> = 92a2c0a1-575d-4ba7-8bf1-9b4da987cfb9 ; Str<userId> =
443c901d-5406-405d-8ca3-f0041da44613 ; Str<queueId> = 25d389d7-30ac-46d0-8284-
432acf0c7b4a ; Str<purpose> = agent ; Bool<wrapupRequired> = false ;
Bool<wrapupExpected> = true
51      [3]: Str<address> =
sip:62d0249013bd2d1d8f86bf1f+mycontactcenterBYOC.orgspan.com;tgrp=6a5d2b81-ba49-
42f7-bbdd-c6aecda5af17;trunk-context=mycontactcenterBYOC@localhost ;
Str<wrapupPrompt> = optional ; Shrt<alertingTimeoutMs> = 8000
52      [3]: Str<device> = Agent01@myContactCenter.com
53      [3]: Array<mediaRoles> [1]
54      [3]: [0]: Str<mediaRoles> = full
55      [3]: Array<calls> [1]
56      [3]: [0]: Str<id> = ebdb1e0b-442a-4131-8f91-eaee94e79cbe ; Str<state> =
alerting ; Str<initialState> = alerting ; Bool<recording> = false ;
Str<recordingState> = none ; Bool<muted> = false ; Bool<confined> = false ;
Bool<held> = false
57      [3]: [0]: Bool<securePause> = false ; Str<direction> = inbound ;
Str<provider> = Edge ; Str<peerId> = 517bc150-72d9-4359-9118-e4e0360c3dfe ;
Bool<afterCallWorkRequired> = false
58      [3]: [0]: Folder<self>
59      [3]: [0]: Str<nameRaw> = Agent01@myContactCenter.com ;
Str<addressNormalized> =
sip:62d0249013bd2d1d8f86bf1f+mycontactcenterBYOC.orgspan.com;tgrp=6a5d2b81-ba49-
42f7-bbdd-c6aecda5af17;trunk-context=mycontactcenterBYOC@localhost ;
Str<addressDisplayable> = unavailable
```

```
50      [3]: [0]: Str<addressRaw> =
sip:62d0249013bd2d1d8f86bf1f+mycontactcenterBYOC.orgspan.com@10.87.6.151;language=en-US;user=station
51      [3]: [0]: Folder<other>
52          [3]: [0]: Str<name> = Robert Smith ; Str<nameRaw> = Robert Smith ;
Str<addressNormalized> = sip:+15551231234@10.87.6.151;user=phone ;
Str<addressRaw> = sip:+15551231234@10.87.6.151;user=phone
53          [3]: [0]: Str<addressDisplayable> = unavailable
54          [3]: [0]: Folder<queueMediaSettings>
55              [3]: [0]: Byte<alertingTimeoutSeconds> = 8
56              Array<recentTransfers> [1]
57                  [0]: Folder<initiator>
58                  [0]: Folder<modifiedBy>
59                      [0]: Str<id> = b44b6635-bbfff-4b57-92e7-c66df8180561 ; Str<state> = active
; Str<dateIssued> = 2024-07-17T17:23:25.267Z ; Str<transferType> = attended
70                  [0]: Folder<destination>
71                      [0]: Str<userId> = 443c901d-5406-405d-8ca3-f0041da44613 ; Str<address> =
sip:tuananh.pham(missing param)overint.com@localhost
72          Folder<metadata>
73              Str<CorrelationId> = cd31f7ab-275d-4c38-b69d-156f4f5212f5
```

To get a mapping, identify the full path to the required data. To find the path, work up from the required field and identify all of the folders and arrays above it.

In the CTI event, the required data is the customer's phone number, which is found within the path:

```
Line 4: Folder<eventBody>
Line 6: Array<participants>
Line 22: Str<purpose> = customer
Line 23: Str<address> = tel:+15551231234
```

The agent's email address is within:

```
Line 4: Folder<eventBody>
Line 6: Array<participants>
Line 50: Str<purpose> = agent
Line 52: Str<device> = Agent01@myContactCenter.com
```

For this external system, we cannot predict in which array index (0, 1, 2, etc.) the customer and agent participants might be found. For this reason we use the **Selector** option, which provides a more flexible method to tag a data value within an array. The format to use is:

```
FolderName.arrayName (selector:PropertyName=PropertyValue).DesiredValue.
```

To map the desired values on the adapter, use the following mappings:

- eventBody.participants (selector:purpose=customer).address
- eventBody.participants (selector:purpose=agent).device

Example 3: SIPREC events

This is an example SIPREC recording event from the internal SIP Proxy sent into the CallTracker for processing. In this case, the customer wants to extract the UCID and the second participant name.

```
1 Dispatching Event recording<SIProxy> --> <CallTracker> Size<0>Int<AdapterId> =
1 ; Str<AdapterName> = SIPREC SBC Avaya ; Int<SwitchId> = 751 ; Str<SwitchName>
= SIPREC_SBC ; Str<datemode> = complete
2 Str<rSessionId> = 786562_54473663@xx.xx.254.70
3 Array<group> [1]
4 [0]: Str<group_id> = OGM3MTkzMDATMThiNy0xMA== ; Str<associate-time> = 2017-05-
11T20:37:18Z
5 [0]: Folder<callData>
6 [0]: Str<fromhdr> = sip:+114045555678@xx.xx.138.36:5060;user=phone ;
Str<callid> = 1258564145_113685498@xx.xx.135.12 ; Str<gcid> = 786562
```

```

7 [0]: Str<tohdr> = "UUID-00FA080045C69E5914CB7E"
  <sip:+18885551234@xx.xx.135.71;user=phone>;tag=gK0c80b638
8 Array<session> [1]
9 [0]: Str<session_id> = OGM3MTkzMDEtMThiNy0xMA== ; Str<group-ref> =
  OGM3MTkzMDAtMThiNy0xMA== ; Str<start-time> = 2017-05-11T20:37:18Z
10 [0]: Str<avayaUCID> = 00FA080045C69E5914CB7E
11 Array<participant> [2]
12 [0]: Str<participant_id> = OGM3MTkzMDItMThiNy0xMA==
13 [0]: Folder<nameID>
14 [0]: Str<aor> = +18885551234@xx.xx.138.36:5060
15 [0]: Folder<name>
16 [0]: Str<lang> = en
17 [1]: Str<participant_id> = OGM3MTkzMDMtMThiNy0xMA==
18 [1]: Folder<nameID>
19 [1]: Str<aor> = +14045555678@xx.xx.135.71
20 [1]: Folder<name>
21 [1]: Str<lang> = en
22 Array<stream> [2]
23 [0]: Str<stream_id> = OGM3MTkzMDQtMThiNy0xMA== ; Str<session_id> =
  OGM3MTkzMDEtMThiNy0xMA== ; Str<associate-time> = 2017-05-11T20:37:18Z
24 [0]: Array<label> [1]
25 [0]: [0]: Str<label> = 1
26 [1]: Str<stream_id> = OGM3MTkzMDUtMThiNy0xMA== ; Str<session_id> =
  OGM3MTkzMDEtMThiNy0xMA== ; Str<associate-time> = 2017-05-11T20:37:18Z
27 [1]: Array<label> [1]
28 [1]: [0]: Str<label> = 2

```

In the SIPREC event example, the following fields were identified for extraction:

On Line 10: [0]: **Str<avayaUCID> = 00FA080045C69E5914CB7E**

On Line 19: [1]: **Str<aor> = +14045555678@xx.xx.135.71**

- “**avayaUCID**” field. Working up from the “**avayaUCID**” field, we need to identify all of the folders /arrays above it. In this particular example message, the “**avayaUCID**” field exists in the “**session**” array. There is no folder above the “**session**” array in this example. The formatting of the Array tells us there is one (1) entry in the array (that is “[0] : **Array<session> [1]**”) and the desired field is in the zeroth index of the array (that is “[0] : **Str<avayaUCID>**”). To access this field, the mapping would be “**session(0) . avayaUCID**”.
- “**aor**” field. Extracting the display name is done in a similar manner. The “**aor**” field is held within a folder named “**nameID**”, which is contained within a different array named “**participant**”. To extract this name, the mapping is “**participant(1) . nameID . aor**”.

Related topics

[CTI tagging \(page 282\)](#)

[Create Custom Data fields \(page 291\)](#)

[Map Custom Data to an attribute \(page 292\)](#)

[Map attributes to an adapter \(page 294\)](#)

Create Custom Data fields

The Custom Data application in Interactions allows you to identify CTI fields to the system.

The Integration Service only evaluates CCDs at the beginning and end of the interaction/session, so if there is post-call tagging, the post-call tags are not used to evaluate CCDs.

Procedure

1. Go to **Interactions > Custom Data**.
2. Edit the custom data fields, following the instructions in the "Custom Data" chapter in the *Interactions and Analytics Administration Guide*.
Example: In keeping with the example in the procedure in "Identify CTI data," you could create a custom data field for the Call Id, name it "MyCallId" and assign a Data Source of "CTI".
3. To assign the custom data to the relevant roles and organizations or groups, go to **Interactions > Assignment Manager**.



If expanding the range of Custom Data fields in use in your system beyond the number of physical fields available by default, it is important that you do not use the same physical field twice for the same contact.

Related topics

[CTI tagging \(page 282\)](#)

[Identify CTI data \(page 282\)](#)

[Map Custom Data to an attribute \(page 292\)](#)

[Map attributes to an adapter \(page 294\)](#)

Related information

"Custom Data" (*Interactions and Analytics Administration Guide*)

What to do next

[Map Custom Data to an attribute \(page 292\)](#)

Map Custom Data to an attribute

Map each Custom Data field created above to an Attribute. You can use one of the existing standard attributes, or create a new one.

If an error message displays on the Custom Data Mapping screen, see [Error message on the Custom Data Mapping screen \(page 292\)](#).

Procedure

1. In Enterprise Manager, go to **Recording Management**.
2. Under **Custom Data**, click **Custom Data Mapping**.
3. Locate the Custom Data field created in the previous procedure ("MyCallId" in our example). Then, under **Attribute Mapping**, select a custom attribute to map to the Custom Data field.
All attributes (excluding those considered standard for the Contact Database) appear in the Attribute Mapping list box, regardless of whether they apply to the data type of the Custom Data in question. When you click Save, if there is a mismatch between the data type and the attribute, an error message appears.



Use the **Find** field in the upper right corner of the screen to search the **Display Name** and **Description** fields to locate specific Custom Data entries. If the text you type in the **Find** field matches text in the **Display Name** or **Description** field for a Custom Data entry, the matching Custom Data entry is highlighted. If there is no match, the **Find** field turns red. The text in the **Find** field can be a partial match. For example, if you type "Cust" in the **Find** field, the search finds entries with the text "Custom Data" under the **Display Name** column. Select the next arrow to the right of the **Find** field, or press the Enter key, to go to the next matching Custom Data entry. Select the previous arrow to the right of the **Find** field to go to the previous matching Custom Data entry.

4. Click **Save**.

The value of the custom attribute (or attribute mapping if configured) is populated into the Custom Data field.

Error message on the Custom Data Mapping screen

After a system upgrade, the following message can display on the Custom Data Mapping screen:

"The extended custom data migration has not run successfully yet. This migration will run every three minutes until it succeeds. You cannot configure custom data mapping until the migration succeeds."

When the migration succeeds, the error message above is cleared from the screen and you can configure custom data mapping.

If the migration fails continuously, note the following.

The migration is done in two places:

1. In the QM database, which migrates the custom data.
2. In Enterprise Manager, which migrates the custom data to attribute mapping.

Step 2 has a dependency on step 1. In a Level 4 deployment, where the QM/Contact database migration is run later, step 2 cannot complete. Also, if the BPMAINDB and WFO migration runs before the QM and QM database migration, step 2 cannot complete. In both of these cases, the error message displays on the screen. Once step 1 is complete, step 2 is retried in Enterprise Manager, and when the migration is complete, the error message is cleared from the screen.

In the event of an unrecoverable error, you must examine the logs to determine the problem.

Related topics

[CTI tagging \(page 282\)](#)

[Identify CTI data \(page 282\)](#)

[Create Custom Data fields \(page 291\)](#)

[Map attributes to an adapter \(page 294\)](#)

What to do next

[Map attributes to an adapter \(page 294\)](#)

Map attributes to an adapter

Mapping attributes to an adapter identifies, to the Integration Service, which CTI fields should be tagged.

Before you begin

[Create an adapter \(page 322\)](#)

[Identify CTI data \(page 282\)](#)

Procedure

1. Go to **System Management**. Under **Enterprise**, select **Settings**.
2. In the Installation Tree, select the relevant Recorder server.
3. Click **Launch** and select **Recorder Manager** to open the Recorder Manager application.
4. In **Recorder Manager**, click **General Setup**.
5. Under **Integration Adapters**, select **Settings**.
6. In the left-hand pane, select the CTI adapter to map the CTI field to the custom attribute.
7. Click **Attributes**. The attributes created in the Enterprise Manager appear in the list.

The screenshot shows the 'General Setup' interface for the 'Recorder Manager'. The top navigation bar includes links for STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP. Below this, a sub-navigation bar shows 'Settings' and 'Attributes'. The main content area is titled 'ADAPTER: CTI API Adapter'. On the left, a table lists the 'Adapter Name' (CTI API Adapter), 'Status' (Started), and 'Target Sta' (Start). To the right, a large table maps 'Attribute' names to 'External Name' fields. The attributes listed include AgentID, AgentName, ALI, ANI, CADid, CallDirection, CalledParty, CalledPartyName, CallId, CallingParty, CallingPartyName, CallRef, CallType, ChannelName, ChannelNumber, ContactDuration, DataSourceName, DeviceName, DNIS, DTMFDigits, EmergencyCall, EmployeeGroup, and EventType. Each attribute has a corresponding input field for its external name. A 'Save' button is located at the bottom right of the mapping table.

- For each attribute, in the **External Name** field, enter the name of the CTI data supplied by the third-party device (see [Identify CTI data \(page 282\)](#)).
8. Locate the custom attribute created in Recording Management, and type the CTI field's External Name as extracted from the Recorder Integration Service logs.

For example, if you have an attribute named "MyCallId", you would map the attribute to the External Name "**event.call.callId**".

You can find external names in the Recorder Integration Service logs. See "Identify CTI data" in the *Recorder Configuration and Administration Guide* for more information. For all of the rules governing the External Name field, including cases where the external attribute consists of a list of values, see [Attribute external name syntax \(page 295\)](#).



- When creating the external name, use only custom attributes. Do not associate standard attributes with custom values.
- Custom attributes are created in the task [Create, edit or delete an attribute \(page 278\)](#).
 - Standard attributes are listed in the topic [Standard attributes \(page 272\)](#).

9. Click **Save**.

Related topics

[CTI tagging \(page 282\)](#)

[Attribute external name syntax \(page 295\)](#)

[Concatenate field values into an attribute \(page 301\)](#)

[Limitations of attribute mapping \(page 302\)](#)

Attribute external name syntax

An attribute is a value that falls within the maximum length set by the string size in the Custom Data field—in such cases you can enter this value in the External Name field. (Note that this may be a single field value, or several field values concatenated into a single attribute as described in [Concatenate field values into an attribute \(page 301\)](#).)

A number of options allow you to handle instances where the External Name represents more than a single value from which you want to extract just one for use as an attribute, or in which the length of the value must be shortened.



- You can only use ASCII values in External Names. This means that you cannot use the following characters:

[] { } < > “ & ! ? |

The following special characters are allowed if you prefix each with an escape character (\):

* ?

For example, to use an escape character with an asterisk, use syntax such as:

```
event.my_list{delimiter: \*}{index:2}{indexbase:0}
```

Example:

Consider a situation in which the external attribute consists of a list of values, from which you want to select the third item for use as an attribute in Recording. By entering the following in the External Name field for the appropriate attribute in Recorder Manager,

```
event.my_list{delimiter:_}{index:2}{indexbase:0}
```

you are asking that the third item be extracted from a list delimited by the underscore symbol, attached to the event "my_list". The indexbase is used to indicate whether the first item in the list is considered item 0 or 1, so in a list that starts at "0", "2" refers to the third item. Each option must be enclosed in braces ({}) and be followed by a colon (:), which separates the option from its value.

Option	Description
delimiter	<p>A character, or list of characters, may be used as a delimiter to separate values in a list (excluding [] { } < > & ! ?).</p> <p>When specifying the delimiter in the context of the External Attribute field, use the following format:</p> <pre>{delimiter: }</pre> <p>Everything between the colon (:) and the end brace will be considered the delimiter.</p> <p>Example:</p> <pre>{delimiter: ; }</pre> <p>In this example, a semi-colon (;) separates the values in the list, representing a list such as:</p> <pre>123 ; 456 ; 789</pre>
keydelimiter	<p>This option allows you to specify the delimiter used to separate a list of key-value pairs. As above, this may be any character, or list of characters (excluding [] { } < > & ! ?).</p> <pre>{keydelimiter: }</pre> <p>Example:</p> <pre>{keydelimiter: : }</pre> <p>In this example, a colon (:) separates the key and value in a key-value pair. For example, if the key is "custid" and the value is "4215", the pair would be represented as follows:</p> <pre>custid: 4215</pre>
Notes:	The delimiter and key delimiter are case-sensitive. If specifying both, the order in which they appear does not matter.
index	The index allows you to indicate which value in a sequence you want to use. See indexbase, below.

Option	Description
indexbase	<p>Use the indexbase to indicate whether the first item in the list is considered item 0 or 1, so in a list that starts at "0", "2" refers to the third item.</p> <p>If you don't specify an indexbase, an indexbase of 1 is assumed.</p> <p>Example:</p> <p><code>{index:5}</code> — selects the 5th item</p> <p><code>{index:3}{indexbase:0}</code> — selects the 4th item</p>
key	<p>Use the key option to select a key element from a key-value pair. If the specified key is not present, no value will be extracted.</p> <p>Example:</p> <p><code>{key:custid}</code></p> <p>If the key "custid" is present, the associated value will be extracted.</p>
keyvalueorder	<p>Use the keyvalueorder option to specify whether the order of a key-value pair is key first or value first.</p> <p>Specify K for key first, or V for value first. The default is "key first".</p> <p>Example:</p> <p>For a key-value pair "flavor:vanilla",</p> <p><code>{keyvalueorder:K}</code> would consider "flavor" the key and vanilla the value.</p> <p><code>{keyvalueorder:V}</code> would consider "vanilla" the key and flavor the value.</p>
Note:	<p>Keys are case-sensitive.</p> <p>When dealing with a list of values, you must specify a key or an index, but not both. In this instance, the key will be used first. If the key does not exist, the specified index will be used to extract a value.</p>
Substring selection	
	<p>Substring selection options allow you to further refine the attribute extracted by means of the options described above. You may use the substring options in combination.</p>
length	<p>Allows you to specify a maximum length for the extracted value. Enter any positive integer, or 0 (zero). 0 is the default.</p> <p>Example:</p> <p>A length option set as follows,</p> <p><code>{length:4}</code></p> <p>with no additional substring options, would turn "1234567890" into "1234".</p>
offset	<p>Use this option to begin extraction of the value at a certain digit. The default is no offset.</p> <p>Example:</p> <p>The following offset,</p> <p><code>{offset:2}</code></p> <p>with no additional substring options, would turn "1234567890" into "34567890".</p>

Option	Description
justify	<p>Use this option to begin extraction from the left or right side of the attribute. Values are L (for left) and R (for right). The default is left.</p> <p>Example: Starting from the left, extract first 5 characters</p> <pre>{justify:L}{length:5}</pre> <p>would turn "1234567890" into "12345"</p> <p>Example: Starting from the right, skip first 2 characters and extract next 4 characters</p> <pre>{justify:R}{length:4}{offset:2}</pre> <p>would turn "1234567890" into "5678"</p> <p>Example: Starting on the right, extract first 2 characters</p> <pre>{justify:R}{length:2}</pre> <p>would turn "1234567890" into "90"</p> <p>Example: Starting on the right, skip first 2 characters and extract remaining characters</p> <pre>{justify:R}{offset:2}</pre> <p>would turn "1234567890" into "12345678"</p> <p>i For right justification, the offset determines the number of characters from the right to be the last character; the length determines the number of characters toward the left to include.</p>

Consider the following scenarios. Each example represents the string you would enter in the External Name field in Recorder Manager for that situation.

Scenario	Solution
External attribute is a list of values	<p>Specify the delimiter used to separate the values, and which value from among those in the list to map to the internal attribute.</p> <p>Example:</p> <pre>event.userlist{delimiter:,}{index:3}</pre> <p>This example would extract the third item from a list of values separated by commas. In:</p> <pre>red,green,blue,yellow</pre> <p>the resulting value will be blue.</p>

Scenario	Solution
External attribute is a list of key-value pairs	<p>Specify the delimiter used to separate the key-value pairs and the specific key associated with the data you want to use as an attribute.</p> <p>Example:</p> <pre>event.test{delimiter:;} {keydelimiter:=}{key:custid}</pre> <p>This example would look for a match to the "custid" key in the following: custname=Sheena ; custid=7719 and extract "7719" as the attribute.</p>
The desired external attribute starts at the fifth character from the end of a string, and must not exceed a length of 100 characters.	<p>Use the justify, length, and offset substring selection options.</p> <p>Example:</p> <pre>event.someevent{justify:r}{length:100}{offset:4}</pre>

Related topics

[Identify CTI data \(page 282\)](#)

[Create Custom Data fields \(page 291\)](#)

[Map Custom Data to an attribute \(page 292\)](#)

[Map attributes to an adapter \(page 294\)](#)

Concatenate field values into an attribute

You can concatenate multiple field values into a single attribute.

For example, take a case where you want to make use of three separate fields in an event, but need them combined into a single attribute. If a CTI event for an adapter is expected to include,

```
someUserField1 = 111  
someUserField2 = 222  
someUserField3 = 333
```

you would typically create a custom attribute for each one, as in:

```
MyAttr1 = event.someUserField1  
MyAttr2 = event.someUserField2  
MyAttr3 = event.someUserField3
```

This would produce the following:

```
MyAttr1 = 111  
MyAttr2 = 222  
MyAttr3 = 333
```

To combine these three values into one attribute, you can use the characters {+} to concatenate them, using the following format:

```
MyAttr = event.someUserField1 {+} event.someUserField2 {+} event.someUserField3
```

or

```
MyAttr = MyAttr1 {+} MyAttr2 {+} MyAttr3
```

To produce the same result in each case of:

```
MyAttr = 111222333
```

Unidentified values

If only a portion of the requested concatenation exists, a partial value will be provided. For example:

```
MyAttr = MyAttr1 {} MyAttr4 {} MyAttr3
```

or

```
MyAttr = event.someUserField1 {} event.someUserField4 {} event.someUserField3
```

Will result will in `MyAttr = 111333`, because `MyAttr4/event.someUserField4` was not identified. If none of the referenced fields contain any data, then the attribute will not be tagged. This behavior works even if a fixed string is included as part of the concatenation.

Fixed strings

You can use a constant string in an attribute mapping, whether as part of a concatenation or as a standalone value. The former is useful for cases where one or more characters are needed between pieces of data in received events. In this instance you will use {{}} to enclose the string. For example:

```
Attribute1 = event.clientIP {+} {':'} {+} event.clientPort
```

If a CTI message from the switch contains `clientIP = 10.156.7.7` and `clientPort = 9999`, then Attribute1 will be mapped to the value `10.156.7.7:9999`.

You may also create an attribute mapping such as the following:

```
Attribute2 = { 'ABCD' }
```

In this case the static value of `ABCD` will be used, rather than a dynamic value from CTI.

Related topics

[Map attributes to an adapter \(page 294\)](#)

[Attribute external name syntax \(page 295\)](#)

[Limitations of attribute mapping \(page 302\)](#)

Limitations of attribute mapping

Mixed mapping

You may only map attributes to other attributes *or* to IEMessage fields, but not a mix of the two. So the following is not supported, because it includes both:

```
MyAttr = event.someUserField1 {+} MyAttr2
```

Recursive mapping

Recursive mapping is not supported. This means that you may do the following:

```
MyAttr1 = event.someUserField1  
MyAttr2 = event.someUserField2  
MyAttr3 = event.someUserField3  
MyAttr4 = MyAttr1 {+} MyAttr2  
MyAttr5 = MyAttr3 {+} MyAttr2
```

But you may not then take the created attributes `MyAttr4` and `MyAttr5` and concatenate them further into yet another field, as in:

```
MyAttr6 = MyAttr4 {+} MyAttr5
```

Related topics

[Map attributes to an adapter \(page 294\)](#)

[Attribute external name syntax \(page 295\)](#)

Recording rules

Recording rules extend the functionality of your recording system by allowing you to implement recording on the basis of a business logic that reflects the goals of your enterprise. Each rule consists of one or more conditions, and an action to perform if the conditions are met. You can also create a schedule that specifies when to apply all rules.

Recording rules are optional for voice recording. To trigger screen recording, the easiest method is a recording rule. Alternatively, you can use AIM or external commands by means of the Integration Service.

Related topics

[Set up recording rules \(page 303\)](#)

Set up recording rules

You can apply individual recording rules to specific Integration Service servers, entire sites, or across the enterprise. There are also settings at the server-level that impact the way all recording rules are carried out.

Before you begin

Set up any [Attributes \(page 271\)](#) specific to your system.

Related topics

[Configure server-level settings for recording rules \(page 304\)](#)

[Create a recording rule \(page 305\)](#)

[Create conditions for a recording rule \(page 311\)](#)

[Create a schedule for recording rules \(page 312\)](#)

Recording rules configuration workflow

Complete the following tasks to configure each recording rule you require.

Workflow sequence

[Workflow: Screen recording \(page 38\)](#): Task 6 of 8

Before you begin

[Configure server-level settings for recording rules \(page 304\)](#)

Procedure

1. [Create a recording rule \(page 305\)](#)
2. [Create conditions for a recording rule \(page 311\)](#)
3. [Create a schedule for recording rules \(page 312\)](#)

What to do next

Screen recording: [Install and configure Archive \(page 41\)](#)

Related topics

[Conditions in a rule \(page 310\)](#)

[Validate regular expressions \(page 313\)](#)

[Delete a rule \(page 319\)](#)

Configure server-level settings for recording rules

Settings for the Integration Service Role establish baseline behavior for recording rules that apply across the server (that is, for all Recorders associated with a particular Integration Service).

This includes,

- How the Integration Service behaves when it receives a Delete/Block command. It can either delete all recordings in a contact, only those for active interactions/sessions or all recordings from that point forward.
- Whether the Integration Service applies recording rules per interaction/session, contact, or current and new interactions/sessions of the contact.

Procedure

1. In Enterprise Manager, click **System Management > Enterprise Settings**, and then select a server node on the left side.
2. Click the triangle beside the name of the server to reveal all of the roles with which it is associated.
3. Click **Recorder Integration Service**.
4. Specify the **Delete/Block Behavior** for the system.

This feature allows you to delete all or a portion of a call. It applies to all delete or block commands within the system. This includes Business Rule Block, Delete on Demand functionality, AIM Block commands, and Block commands from Connect or other external APIs.

- **Delete entire contact completely:** All recordings (past, present, and future) in a contact are deleted.
- **Delete active sessions completely:** All recordings (past, present, and future) for all active interactions at the time of the block are deleted. Past interactions in the contact are not affected. Future interactions in the contact are not affected.
- **Delete all future recordings in a contact:** All current and future interactions in a contact are affected. Any active recording is segmented at the time that the block is processed. Any recording prior to the block for the current interaction is not affected and is kept or discarded according to its current state. Any recording after the block and future interactions in the contact are deleted. Past interactions in the contact are not affected.
- **Delete all future recordings in currently active sessions:** All future recordings for all active interactions at the time of the block are deleted. Any active recording is segmented at the time that the block is processed. Any recording prior to the block for the current interaction is not affected and is kept or discarded according to its current state. Any recording after the block are

deleted for the affected interactions. Past interactions in the contact are not affected. Future interactions in the contact are not affected.

5. Specify the portion of a contact or interaction/session to which rules should apply using the **Process Business Rule on** setting. Options are to run the rules against each,
 - **Contact, then apply action to every session**— Evaluates rules on the contact level (and will only fire once per contact) and the action will affect all sessions/interactions in that contact.
 - **Session, then apply action to that session only**— Evaluates rules on the session/interaction level and the action will only affect that session/interaction.
6. Click **Save**.

Related topics

[Set up recording rules \(page 303\)](#)

[Create a recording rule \(page 305\)](#)

[Create conditions for a recording rule \(page 311\)](#)

[Create a schedule for recording rules \(page 312\)](#)

Create a recording rule

A recording rule defines, the action the Integration Service must take when it encounters a contact or part of a contact that matches the rule's conditions, the amount of audio to record, how to apply the rule across a pool of employees, whether to record the screen activity of an employee after a call. In addition, you can configure a rule to trigger on a schedule and for specific conditions.

Procedure

1. In Enterprise Manager, click **Recording Management > Recording Rules > Settings**, then click **Create**.

The settings page displays with a new rule for you to configure.

Rule

Name	<input type="text"/> LegacyRuleToValidateMultipleExtensions_Migrate_OR
Description	<input type="text"/> Created by EM_Gate1_TenantManagedCaptureRules_Workflow
Status	<input checked="" type="checkbox"/> Enabled
Actions	
Audio Content	<input checked="" type="checkbox"/> <input type="range"/> 11
Screen Content	<input checked="" type="checkbox"/> <input type="range"/> 22
Video Content	<input checked="" type="checkbox"/> <input type="range"/> 33
Block Content	<input type="checkbox"/>
Tag Only/No Action	<input type="checkbox"/>
Use Person Level Recording Percentages	<input checked="" type="checkbox"/>
Randomizer on Individual Person	<input checked="" type="checkbox"/>
After Call Work	<input checked="" type="checkbox"/> Record after call work <input type="text"/> 99 Recording time after call work (Seconds)
Redaction	<input type="checkbox"/>
Morphing	<input type="text"/> Do Not Morph

2. **Name and Description** - Type a name (required) for the rule, and a description (optional).
3. **Status** - Select the **Enabled** check box if you want the rule to take effect right away. If this check box is not selected, the rule never takes effect.
4. **Audio Content** - Select this check box to record audio content.
Use the slider to the right of the check box to specify the percentage of audio contacts to be recorded and saved. For example, move the slider all the way to the right to record 100% of audio contacts. Optionally, you can type a percentage value in the text box to the right of the slider to specify the percent of the audio contacts that are recorded and saved.
The **Block** and **Tag Only / No Action** check boxes are unavailable when this check box is selected.
5. **Screen Content** - Select this check box to record screen content.
Use the slider to the right of the check box to specify the percentage of contacts for which to record and save the associated screen activity. For example, move the slider to the half-way point to record screen activity for 50% of all contacts. Optionally, you can type a percentage value in the text box to the right of the slider to specify the percentage of contacts for which associated screen activity is recorded and saved.
The **Block** and **Tag Only / No Action** check boxes are unavailable when this check box is selected.
6. **Video Content** - Select this check box to record video content.
Use the slider to the right of the check box to specify the percentage of video contacts to be recorded and saved. For example, move the slider to the three-quarters point to record 75% of all

video contacts. Optionally, you can type a percentage value in the text box to the right of the slider to determine the percentage of video contacts that are recorded and saved.

The **Block** and **Tag Only / No Action** check boxes are unavailable when this check box is selected.

7. **Block Content**—Select this option to block the content. The Integration Service server role contains additional settings that define its behavior upon receipt of a block command. Block commands take precedence over Record commands. When you select this option, 100% of calls are blocked.

This option is unavailable if either the **Audio Content**, **Screen Content**, **Video Content**, or **Tag Only / No Action** check boxes are selected. To select this option, you must clear all check marks from the **Audio Content**, **Screen Content**, **Video Content**, and **Tag Only / No Action** check boxes.

8. **Tag Only / No Action**—Select this option to tag other actions on the call. This option can be used with after call work (ACW) and tagging functionality. When you select this option, 100% of calls are only tagged.

This option is unavailable if either the **Audio Content**, **Screen Content**, **Video Content**, or **Block** check boxes are selected. To select this option, you must clear all check marks from the **Audio Content**, **Screen Content**, **Video Content**, and **Block** check boxes.

9. **Use Person Level Recording Percentages** - Select this check box to use the recording percentages set for employees.

Person level percentages can be set for individual employees or for all employees in an organization. Percentages set for individual employees, or for all employees in an organization, will override any percentages set under **Recording Rules** in Recording Management.

Change either the person level percentages for individual employees or the person level percentages for all employees in an organization, as described below:

Change the person level percentages settings for individual employees:

- a. Navigate to **User Management > Employees > Interactions**.
- b. Make sure that **Inherit Settings from Current Organization** is not selected.
- c. In the left pane, select the specific employee for whom you want to specify a person level percentage.
- d. Under **Recording Properties**, for each of Audio, Video, and Screen Recording (as applicable), select **Percentage**, and specify a number in the field. Please note that if you specify a percentage here, but do not select the **Use Person Level Recording Percentages** check box, the system will use the percentage from the **Recording Rules** page in Recording Management.



If you select **System Defined**, the system uses the percentages set under **Recording Rules** in Recording Management in Steps 4 - 6. In this situation, the system will use this setting, even if on Recording Rules page you have selected the **Use Person Level Recording Percentages** check box.

- e. Click **Save**.
- f. Repeat steps c. through e. for each employee for whom you want to specify a person level

percentage.

- g. Continue to step 10.

Change the person level percentages settings for all employees in an organization:

- a. Navigate to **User Management > Employees > Interactions**.
- b. Make sure that **Inherit Settings from Current Organization** is selected.
- c. Navigate to **Interactions > Administration > Interaction Settings**.
- d. In the left pane, select the organization for which you want to specify person level percentages for all persons in the organization.
- e. Under **Recording Properties**, for each of Audio, Video, and Screen Recording (as applicable), select **Percentage**, and specify a number in the field. Please note that if you specify a percentage here, but do not select the **Use Person Level Recording Percentages** check box, the system will use the percentage from the **Recording Rules** page in Recording Management.



If you select **System Defined**, the system uses the percentages set under **Recording Rules** in Recording Management in Steps 4 - 6. In this situation, the system will use this setting, even if on the Recording Rules page you have selected the **Use Person Level Recording Percentages** check box.

- f. Click **Save**.
- g. Repeat steps d. through f. for each organization for which you want to specify person-level percentages.
- h. Continue to step 10.

This option is unavailable if either the **Block** or **Tag Only / No Action** options are selected.

10. **Randomizer on Individual Person** - Select this check box to ensure that, within the calls that meet the criteria, calls are recorded for a random sampling of employees when available.

If the percentage of calls to save is less than 100, and the rule conditions include more than one employee or supervisor, the random check can be applied to each individual or for the group as a whole. For example, there are 100 calls for 10 employees, and you have specified that 10 percent of calls be recorded. If **Randomiser on Individual Person** is not enabled, any number of the 10 recorded calls may be for just one employee. If **Randomiser on Individual Person** is enabled, each employee will be given equal treatment when the rule is triggered. So if each employee gets 10 calls, then the supervisor is assured that he can expect 10 percent, or 1 call per employee, to be recorded.

11. **After Call Work** - To record an employee's activity after a call:

- a. Select the **After Call Work** check box.
- b. Beside **Recording time after call work (Seconds)**, specify a time in seconds for which to record the employee's work after the call terminates.

The After Call Work feature:

- tags the call with an attribute (Wrapup Time) that indicates how much time the employee spent doing after call work. (Even if there is no recording.)
- records after call screen activity after the call terminates, if screens were being recorded.

See the *Recorder Call Flow Guide* for information about the scenarios to which this applies.



- The employee's after call work time is tracked until any one of the following occurs:
- The amount of time entered in the **Recording time after call work** field elapses.
 - The employee receives a new call.
 - A switch event indicates the employee is no longer in the After Call Work state.

12. **Redaction:** Select to hide sensitive customer information in the call audio and transcriptions. Redaction must be enabled on your system for this option to work.
13. **Morphing:** Protects people's identity by changing the voice heard during replay, so it is intelligible but anonymous. Choose one of the following options:
 - **Agent:** Only the voice of the agent channel is morphed during interaction replay. The voice on the customer channel is the original captured voice.
 - **Agent and customer:** The voice of the agent channel and the customer channel are morphed during interaction replay.
 - **Do not morph:** Original voices are preserved.Morphing must be enabled on your system for this option to work.
14. *For Trading environments only*, optionally configure the User-Defined field (UDF) populated when the rule triggers:
 - **Tag stored in:** select which UDF field to use to store a value.
 - **Tag value:** provide the value to store in the UDF field. The default value is the rule **Name**. You can enter any value. This field is only used when a UDF field is selected in the **Tag stored in** setting.
15. **Mark As Exception** - Select this check box to have contacts that meet the criteria of this rule marked as exceptions, allowing you to further distinguish certain types of contacts from the rest. (For example, you may need to identify calls with a number of transfers above a certain threshold.)
16. **Installations** - Specify where you want this rule to apply. You can apply the rule to individual Integration Services, entire sites, or across the enterprise.
17. Click **Save**.

Related topics

[Set up recording rules \(page 303\)](#)

[Configure server-level settings for recording rules \(page 304\)](#)

[Create a schedule for recording rules \(page 312\)](#)

What to do next

Learn about [Conditions in a rule \(page 310\)](#) and [Create conditions for a recording rule \(page 311\)](#).

Conditions in a rule

Each recording rule consists of a set of conditions (such as "extension starts with") and actions (record, block, and so on). A rule will trigger the specified action when contacts between employees and customers meet the specified criteria. You can combine rules in multiple ways to meet your requirements.

Examples:

Consider the following:

- You could create a rule stipulating that "if Contact Duration is **Greater Than 20 minutes** (1200 seconds), then Record Audio, at a level of 25% of all contacts (with Randomize on Individual member enabled)," the call should be recorded. This will provide a sample of contacts lasting longer than 20 minutes, and handled by a range of employees. You could use the results to examine whether certain factors may be contributing to lengthy resolution times in a support center.
- If you have an employee within your organization who is particularly successful at finding resolutions to customer issues, without placing the caller on hold to seek additional help or resources. You could create a rule that specifies "if **Employee Name** is Equal to AgentABC and Time on Hold is Equal to 0 (zero), then Record Audio and Screen at a level of 100%." You could use the captured data to analyze whether the employee uses strategies that are repeatable.
- You are running a specific campaign, and you want to determine whether specific supervisors were successful in communicating to employees the key goals of the campaign. Assume all calls for this campaign are to a special promotional number. You may create a rule such as "if Number Dialed Equals **1-800-555-5555**, then Record Audio, at a level of 10% of all contacts, where the Supervisor Name is Equal to Supervisor A Or Supervisor B (with Randomize on Individual member enabled)." This will record a random sampling of campaign-related calls to employees working for Supervisors A and B.
- You want to monitor calls received during particular time periods. In this case you can create a rule that runs on a specific schedule, triggering contact recording on certain days or during defined time periods.

Related topics

[Configure server-level settings for recording rules \(page 304\)](#)

[Create a recording rule \(page 305\)](#)

[Create a schedule for recording rules \(page 312\)](#)

What to do next

[Create conditions for a recording rule \(page 311\)](#)

Create conditions for a recording rule

In addition to a schedule and rule settings, you must create conditions for your recording rules. While the settings and schedule define what action to take and when, conditions define the criteria that will trigger the rule.

Procedure

1. In Enterprise Manager, click **Recording Management > Recording Rules >Conditions**.
2. Click **Add** to specify the conditions under which the recording rule should be triggered.
3. For each condition, select an **Attribute** and a **Condition**. In the field beside the condition, type a value or click the pencil icon to select a value from the list.



You may enter multiple values for some conditions. These must be separated by a semi-colon (;).

4. If you are creating only one condition for this rule, select **End** from the **Terminator** drop-down list. If you are creating more than one condition, use the parentheses check boxes and the **And** and **Or** terminators group parts of the condition together logically.

Example:

The following rule triggers recording when the supervisor is either John Doe or Jane Doe, the call is placed on hold more than three times, and the entire call is longer than 20 minutes (1200 seconds). If you are creating only one condition for this rule, select **End** from the **Terminator** drop-down list. If you are creating more than one condition, use parentheses (by clicking the * in each line) and the **And** and **Or** terminators group parts of the condition together logically.

Compare the first rule with the following rule, which triggers recording when the Supervisor is John Doe, OR the Supervisor is Jane Doe, the call is placed on hold more than three times, and the entire call is longer than 20 minutes (1200 seconds). Note how only the placement of parentheses has changed, but the rules will produce different results: the first rule will record only those calls where John Doe or Jane Doe are the supervisor, *and* the other criteria are met, while the second rule will record *all* calls where John Doe is the Supervisor, and only some where Jane Doe is the Supervisor.

5. At the end of your condition, select the **End** terminator.
6. Click **Add**.
7. Click **Save**.

Usability issue with the In List and Not In List condition settings

A recording rule condition includes an attribute setting, a condition setting, and a condition box where you enter a value for the condition setting.

The condition box field has a length limitation of 256 characters. A usability issue can occur when the "In List" or "Not In List" condition setting is used and there are a large number of items to be entered in the condition box field. To overcome this limitation, you must split the condition into multiple rows using the "Or"/"And" terminator.

For example, assume you want to split the condition below into two or more rows:

Attribute setting = **ANI** Condition setting = **In List** Condition box field values = **1,2,3,4,5,6,7,8,9,0** so that you have that you basically have this condition:

ANI "In List" "1,2,3,4,5,6,7,8,9,0,"

You can change the condition into a condition consisting of three rows, like this:

(ANI "In List" "1,2,3" OR
ANI "In List" "4,5,6" OR
ANI "In List" "7,8,9,0")

Here is another example using the "Not In List" condition setting. Assume you have the condition:

ANI "Not In List" "1,2,3,4,5,6,7,8,9,0"

You can split the condition into three rows like this:

(ANI "Not In List" "1,2,3" AND
ANI "Not In List" "4,5,6" AND
ANI "Not In List" "7,8,9,0")

Related topics

[Configure server-level settings for recording rules \(page 304\)](#)

[Create a recording rule \(page 305\)](#)

What to do next

[Create a schedule for recording rules \(page 312\)](#)

Create a schedule for recording rules

A schedule defines when a given rule should be applied to the recording of the contact or part of the contact.

Example: Using a schedule to trigger a recording rule

- **on every** day of the week **between the** hours of 12:00am and 12 pm UST **beginning** immediately and **ending** on 06/27/2006.
- **on every** Sunday of the week **between the** hours of 12:00am and 12 pm UST **beginning** on 06/23/2006 and **ending** on 06/27/2006.
- **on every** Sunday of the week **between the** hours of 12:00am and 12 pm UST **beginning** on 06/23/2006 and **with no end date**.

Procedure

1. In Enterprise Manager, click **Recording Management > Recording Rules > Schedule**.
2. Complete the following fields:
 - **Enabled on every**—Check all the days when you require recording to occur.
 - **Time to Schedule**—Choose one of the following: **All Day** (to have recording occur at all times during the days indicated), or **Between hours of** and then type a range of times, such as 12 a.m. to 12 p.m. If the end time is after the begin time, the time range is considered within a single day. If the end time is before the begin time, the end time is treated as a continuation of the previous day's begin time. For example, a configuration between 10PM and 6AM causes the rule to activate at 10PM on the enabled days and end at 6AM the following day, regardless of whether the following day is enabled.
 - **Time Zone**—Choose **Local Time Zone of Integration Service** to observe the local time zone such as EST (Eastern Standard Time) in effect for the Integration Service Server for this recording

system, or choose **UTC (Universal Time Zone)** to observe Greenwich Mean Time, where the time in Greenwich England is considered the base time, preferred when recording is being administered in different time zones.

- **Beginning**—Check **Immediately** to have recording begin right away, or choose **On this date** and then specify a date when the business rule will be effective and will be evaluated based on the Conditions specified.
- **and Ending**—Check **No End Date** to have recording continue infinitely, or choose **On this Date** and then specify a date when recording will end.

3. Click **Save**.

Related topics

[Configure server-level settings for recording rules \(page 304\)](#)

[Create a recording rule \(page 305\)](#)

[Create conditions for a recording rule \(page 311\)](#)

What to do next

Learn about [Validate regular expressions \(page 313\)](#).

Validate regular expressions

You can validate regular expressions contained in your Recording Rule conditions in Enterprise Manager.

To use this tool, you will first type a Regular Expression Pattern, then type values in the Match Values area, and finally test these values by clicking the Validate button. This gives you an idea of what values will suit your needs and the associated pattern that must be used for the condition. Face icons tell you visually if Match Values are valid or not.

Procedure

1. In Enterprise Manager, click **Recording Management > Recording Rules > Conditions**.
2. Click **Test Regular Expression**.
3. Enter a value in the **Regular Expression Pattern** field, referring to the definitions and examples that follow this procedure.
4. Under **Match Value**, type the values to which the Regular Expression is matched and then click **Validate**. If a red icon appears, the match is not valid. If a green icon appears, your proposed value is good and can be used successfully in a condition.



Click **Add** to add multiple match values, or click **Delete** to delete a selected value field.

Example: Testing the "in" regular expression against two values

Consider the following example to better understand how to complete the fields of this tool. This example assumes that you want to test the regular expression "in" against these two values:

- Mozilla/4.0 (compatible; MSIE 5.0; Windows NT; DigExt)
- Mozilla/4.75 [en](X11;U;Linux2.2.16-22 i586)

To perform this test, you would complete the fields in the tool as follows:

1. In the **Regular Expression Pattern** field, type the expression you want to test:
in
2. In the **Match Value** field, type:
Mozilla/4.0 (compatible; MSIE 5.0; Windows NT; DigExt)
3. In a second **Match Value** field, type:
Mozilla/4.75 [en] (X11;U;Linux2.2.16-22 i586)
4. Click the **Validate** button.
5. An icon appears under the **Matches** column to indicate a successful or unsuccessful match. (In this example, the green smile icon appears to indicate the test expression successfully matches both values).

Additional detailed examples are provided below that show how to test complex expressions.

Definitions

Term	Meaning
literal	Any character used in a search or matching expression. For example, to find ind in windows the ind is a literal string; each character plays a part in the expression – it is literally the string you are searching for.
metacharacter	One or more special characters that have a unique meaning and are NOT used as literals. For example, in the search expression, the character ^ (circumflex or caret) is a metacharacter.
escape sequence	A way of indicating that you want to use a metacharacter as a literal . In a regular expression an escape sequence involves placing the metacharacter \ (backslash) in front of the metacharacter to be used as a literal. For example, to find ^ind in w^indow , use the search string \^ind . To find \file in the string c:\\file , use the search string \\\\file , that is, each \ you are searching for (a literal) is preceded by an escape sequence \.
target string	Term used to describe the string being searched for by the expression. In other words, the string in which you want to find a match or search pattern.
search expression	Term used to describe the expression being used to search the target string, that is, the pattern you use to find what you want.

The following characters are not supported:

- <> (Greater than, Less than symbols)
- & (Ampersand)
- " (Quotation marks)
- ! (Exclamation symbol)

Pattern Matching Examples: Basic

The examples below refer to the following two target strings:

STRING1: Mozilla/4.0 (compatible; MSIE 5.0; Windows NT; DigExt)

STRING2: Mozilla/4.75 [en](X11;U;Linux2.2.16-22 i586)

Search for		Result	Description
m	STRING1	match	Finds the m in com patible.
m	STRING2	no match	There is no lower case m in this string. Searches are case sensitive unless you take special action.
a/4	STRING1	match	Found in Mozilla /4.0 - any combination of characters can be used for the match.
a/4	STRING2	match	Found in same place as in STRING1.
in	STRING1	match	Found in Wind ows.
in	STRING2	match	Found in Lin ux.
le	STRING1	match	Found in compatible e .
le	STRING2	no match	There is an l and an e in this string but they are not adjacent (or contiguous).

Pattern Matching Examples: Brackets, Ranges and Negation

Bracket expressions introduce metacharacters, in this case the square brackets that allow you to define a list of items to test for, rather than the single characters in the simple matching example. These lists can be grouped into what are known as Character Classes typically comprising well known groups such as all numbers, and other logically grouped characters.

Metacharacter	Meaning
[] (Square Brackets)	Match anything inside the square brackets for one character position once and only once. For example, [12] means match the target to either 1 or 2 while [0123456789] means match to any character in the range 0 to 9.
- (Dash)	When used inside square brackets acts as the 'range separator' and allows you to define a range. In the example above of [0123456789] you could rewrite it as [0-9]. You can define more than one range inside a list. For example, [0-9A-C] means check for 0 to 9 and A to C (but not a to c). Note: To test for a Dash inside brackets (as a literal), the Dash must come first or last. For example, [-0-9] will test for - (the Dash) and 0 to 9.

Metacharacter	Meaning
^ (Circumflex or caret)	When used <i>inside</i> square brackets negates the expression (there is an alternate use for the circumflex/caret <i>outside</i> square brackets later). For example, [^Ff] means anything except upper or lower case F and [^a-z] means everything except lower case a to z. [i] Spaces, or in this case the lack of them, between ranges are very important.

The examples below refer to the following two target strings:

STRING1: Mozilla/4.0 (compatible; MSIE 5.0; Windows NT; DigExt)

STRING2: Mozilla/4.75 [en](X11;U;Linux2.2.16-22 i586)

Search for	In	Result	Description
in[du]	STRING1	match	Finds ind in Windows .
in[du]	STRING2	match	Finds inu in Linux .
x[0-9A-Z]	STRING1	no match	The tests are case-sensitive. To find the xt in DigExt use [0-9a-z] or [0-9A-Zt]. You can also use this format for testing upper and lower case. For example, [Ff] will check for lower and upper case F.
x[0-9A-Z]	STRING2	match	Finds x2 in Linuxx2 .
[^A-M]in	STRING1	match	Finds Win in Windows .
[^A-M]in	STRING2	no match	The range A to M is excluded in the search, so Linux is not found, although linux (if it were present) would be found.

Pattern Matching Examples: Positioning (Anchors)

You can control where in your target strings the matches are valid. The following is a list of metacharacters that affect the position of the search:

Metacharacter	Meaning
^ (Circumflex or caret)	When used <i>outside</i> square brackets, this symbol means look only at the beginning of the target string. For example, ^Win will not find Windows in STRING1 but ^Moz will find Mozilla .
\$ (Dollar)	The dollar symbol means look for the preceding text at the <i>end</i> of any line. For example, 'fox\$' will match 'silver fox'.
. (Period)	A '.' matches any character - though it does require that there is a character to match.

The examples refer to the following two target strings:

STRING1: Mozilla/4.0 (compatible; MSIE 5.0; Windows NT; DigExt)

STRING2: Mozilla/4.75 [en](X11;U;Linux2.2.16-22 i586).

Search for	In	Result	Description
\$[a-z])	STRING1	match	Finds t) in DigiExt).
\$[a-z])	STRING2	no match	There is a numeric value at the end of this string but you would need [0-9a-z]) to find it.
.in	STRING1	match	Finds Win in Windows .
.in	STRING2	match	Finds Lin in Linux .

Pattern Matching Examples: Iteration Metacharacters

The following is a set of iteration metacharacters (also known as quantifiers) that can control the number of times a character or string is found in searches.

Metacharacter	Meaning
?	Matches the preceding character 0 or 1 times only. For example, colou?r will find both color and colour .
*	Matches the preceding character 0 or more times. For example, tr* will find tree and tread and trough .
+	Matches the previous character 1 or more times. For example, tre+ will find tree and tread but not trough .
{n}	Matches the preceding character n times exactly. For example, to find a local phone number, [0-9]{3}-[0-9]{4} would find any number of the form 123-4567.
	<p>i The - (Dash) in the above example, because it is outside the square brackets, is a literal character.</p>

The examples below refer to the following two target strings:

STRING1: Mozilla/4.0 (compatible; MSIE 5.0; Windows NT; DigExt)

STRING2: Mozilla/4.75 [en](X11;U;Linux2.2.16-22 i586)

Search for	in..	Result	Description
\(.*)l	STRING1	match	<p>Finds l in (compatible).</p> <p>i The opening \ is an escape character used to indicate that it precedes is a literal and not a metacharacter.</p>

Search for	in..	Result	Description
\(.*)l	STRING2	no match	Mozilla contains lls but not preceded by an open parenthesis (no match) and Linux has an upper case L (no match).
W*in	STRING1	match	Finds the Win in Windows .
W*in	STRING2	match	Finds in in Linux preceded by W zero times.
[xX][0-9a-z]{2}	STRING1	no match	Finds x in DigExt but only one t.
[xX][0-9a-z]{2}	STRING2	match	Finds X and 11 in X11 .

Pattern Matching Examples: Parentheses and Pipes

The following additional metacharacters can provide added power to searches:

Metacharacter	Meaning
() Parentheses	The ((open parenthesis) and) (close parenthesis) may be used to group (or bind) parts of search expressions together, as shown in the examples.
 (Vertical bar or pipe)	Technically called alternation , this character means find the left hand OR right hand values. For example, gr(a e)y will find gray or grey .

The examples below refer to the following two target strings:

STRING1: Mozilla/4.0 (compatible; MSIE 5.0; Windows NT; DigExt)

STRING2: Mozilla/4.75 [en](X11;U;Linux2.2.16-22 i586)

Search for	in	Result	Description
^([L-Z]in)	STRING1	no match	^ is an anchor indicating first position. Win does not start the string, so no match.
^([L-Z]in)	STRING2	no match	^ is an anchor indicating first position. Linux does not start the string, so no match.
((4).[0-3]) (2\[. [0-3]\])	STRING1	match	Finds the 4.0 in Mozilla/4.0 .
((4).[0-3]) (2\[. [0-3]\])	STRING2	match	Finds the 2.2 in Linux2.2.16-22 .
(W L)in	STRING1	match	Finds Win in Windows .
(W L)in	STRING2	match	Finds Lin in Linux .

Related topics

[Configure server-level settings for recording rules \(page 304\)](#)

[Create a recording rule \(page 305\)](#)

[Create conditions for a recording rule \(page 311\)](#)

[Create a schedule for recording rules \(page 312\)](#)

Delete a rule

Delete any rules that you no longer need to apply to your system.

Procedure

1. Click **Recording Management>Recording Rules >Settings**.
2. In the left pane select one or more rules.
3. Click **Delete**. The deletion process may take a few seconds to complete.

Related topics

[Configure server-level settings for recording rules \(page 304\)](#)

[Create a recording rule \(page 305\)](#)

[Create conditions for a recording rule \(page 311\)](#)

[Create a schedule for recording rules \(page 312\)](#)

Configure CTI adapters

This section describes how to create adapters for switch/CTI combinations. Supported combinations are described in Integration Guides specific to each vendor, and the online help.

Topics

About CTI adapters	321
Configure a CTI adapter	322
Configure adapter custom attributes	326
Adapter behavior and troubleshooting	330

About CTI adapters

CTI adapters are software components that allow the Recorder to communicate with the various switch types. This communication is necessary to receive call signaling and metadata from the switch. For example, an Avaya CTI adapter is required so that the Recorder can communicate with an Avaya switch to receive the call signaling and metadata. (You can customize call metadata by creating attributes—see [Set up attributes, tagging, and recording rules \(page 269\)](#) for the complete workflow for this process).

You can configure CTI adapters in Recorder Manager. This creates a link to the CTI Server, and associates it with a data source configured in Enterprise Manager. You are also configuring what custom attributes from the CTI Server the Adapter should pick up and make available to the rest of the system.

You must set up the Integration Service in Enterprise Manager before configuring CTI adapters, as described in [Set up Recorder roles and associations \(page 44\)](#).



All of the procedures in this chapter take place in Recorder Manager.

Configure a CTI adapter

The following procedures describe in general terms how to configure a CTI adapter in Recorder Manager:

- [Edit an adapter \(page 324\)](#)
- [Delete an adapter \(page 324\)](#)
- [Start, stop, or restart an adapter \(page 325\)](#)

You can have more than one adapter in your enterprise, and you can associate multiple adapters with a single data source. However, a single data source should be assigned only one "primary" CTI adapter. A primary CTI adapter is defined as the master controlling CTI adapter (not tagging only). SIP proxy adapters are not considered CTI adapters.

Example: A Cisco data source is associated with a single JTAPI CTI adapter, but an ICM adapter in tagging only mode is also associated with the data source.

For detailed information on specific supported adapter integrations, see the solution sheet for the switch-CTI combination in question.



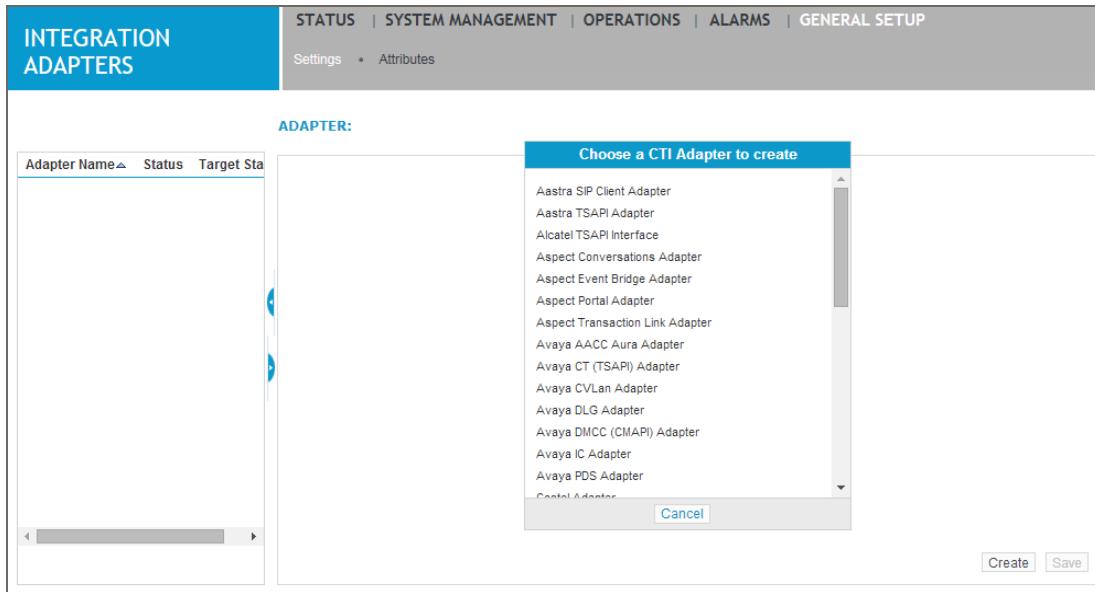
Available adapter types will only appear in Recorder Manager if you have created a data source associated with the appropriate switch in Enterprise Manager. Please also note that adapters for Trading environments are not documented here—see the associated *Integration Guide* for details.



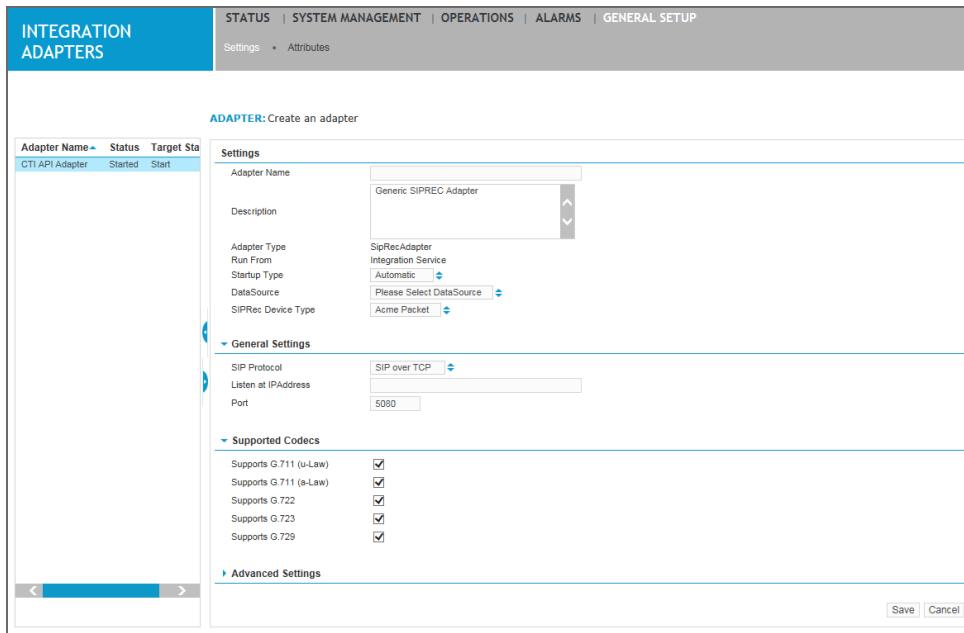
The Alcatel TSAPI, Avaya TSAPI, Avaya CVLAN, Cisco JTAPI, and Intecom adapters will require client software installed on the same server as the recorder—see the associated *Integration Guide* for details.

Create an adapter

1. Click **General Setup > Integration Adapters > Settings**.
2. Click **Create**.



3. In the right-hand pane, under **Choose a CTI Adapter to create**, select the type of adapter that you are going to use.



4. Specify settings for this adapter in the right-hand pane. The following settings apply to all adapters. For settings specific to the adapter being created, refer to the associated *Integration Guide*.

Field	Description
Adapter Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This is a required field and is not case sensitive.
Description	Type a description of the adapter.
Adapter Type	This is a read-only field that specifies the adapter selected above.
Startup Type	Select a startup type: Automatic, Manual, or Disabled. This is a required field.
DataSource	Select the data source to which you want to associate this adapter.

- Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary configuration for the Recorder Integration Service to use for this specific adapter.
- Click **Save**. The adapter appears in the left-hand pane.

Related topics

[Edit an adapter \(page 324\)](#)

[Delete an adapter \(page 324\)](#)

[Start, stop, or restart an adapter \(page 325\)](#)

Edit an adapter

Procedure

- Click **General Setup > Integration Adapters > Settings**.
- Select an adapter from the list in the left-hand pane.
- Edit the fields as necessary, and then click **Save**.

Related topics

[Create an adapter \(page 322\)](#)

[Delete an adapter \(page 324\)](#)

[Start, stop, or restart an adapter \(page 325\)](#)

Delete an adapter

- Click **General Setup > Integration Adapters > Settings**.
- Select an adapter from the list in the left-hand pane.
- Click **Delete**.

Related topics

[Create an adapter \(page 322\)](#)

[Edit an adapter \(page 324\)](#)

[Start, stop, or restart an adapter \(page 325\)](#)

Start, stop, or restart an adapter

The current status of an adapter appears beside the adapter name in the left-hand pane of the **Settings** tab, in the **Status** column. You can start, stop, or restart the adapter at any time using the following procedure.

Procedure

1. Click **General Setup > Integration Adapters > Settings**.
2. Select an adapter from the list in the left-hand pane.
3. Click **Start, Stop, or Restart**.

Related topics

[Create an adapter \(page 322\)](#)

[Edit an adapter \(page 324\)](#)

[Delete an adapter \(page 324\)](#)

Recover calls for an Amazon Connect adapter

The Amazon Connect Adapter depends on the reception of Contact Trace Records (CTRs) for call recording. If, for any reason, the CTRs are missed, the recording is also missed for those calls. You can recover these missed recordings.

Procedure

1. Under **General Setup**, click the **Settings** option under **Integration Adapters**.
2. In the left pane, click the Amazon Connect adapter for which you want to recover recordings.
3. Click the **Recover Calls** button.
4. In the **Recover Calls Settings** window, click the calendar icon  to define the time frame for which you want to recover calls.
 - a. In the **From:** section, specify the date and time that defines the start date of the time frame for which you want to recover calls.
 - b. In the **To:** section, specify the date and time that defines the end date of the time frame for which you want to recover calls.
 - c. Click **Set**.
 - d. Click **Recover**.

You can track the status of the call recovery operation from the **Recovery** section of the **Status - Interaction Capture Status** screen in Recorder Manager.

Related topics

[Create an adapter \(page 322\)](#)

[Edit an adapter \(page 324\)](#)

[Start, stop, or restart an adapter \(page 325\)](#)

Configure adapter custom attributes

On any adapter you can configure the custom attributes to refer an external name. Custom attributes are created in the Enterprise Manager and retrieved by Recorder Manager. See [Attributes \(page 271\)](#) for more details on the larger workflow of which this is a part.

Procedure

1. Click **General Setup > Integration Adapters > Attributes**.
2. Select an adapter from the left pane.

Attribute	External Name
AgentID	
AgentName	
ALI	
ANI	
CADid	
CallDirection	
CalledParty	
CalledPartyName	
CallId	
CallingParty	
CallingPartyName	
CallRef	
CallType	
ChannelName	
ChannelNumber	
ContactDuration	
DataSourceName	
DeviceName	
DNIS	
DTMFDigits	
EmergencyCall	
EmployeeGroup	
EventType	

3. Type an external name for the attributes available for this adapter. The external name can include these special characters: [] < > " & ! ?

Attribute	Description
ANI	The Automatic Number Identification or Caller ID.
AgentID	The logon ID of the employee.
AgentName	The employee involved in the call.
CallDirection	Choice for the call direction.

Attribute	Description
CallId	The identification of the call in the switch queue.
CallRef	The reference number of the call.
CallType	Type of call.
CalledParty	The identification of the called person in the case of a Cisco switch.
CalledPartyName	The name or Employee ID of the called person in the case of a Cisco switch.
CallingParty	The identification of the party that initiated the call.
CallingPartyName	The name of the party that initiated the call.
ChannelName	The name assigned to the channel (maximum 24 for T1, 30 for E1).
ChannelNumber	The channel number on which the call appears.
ContactDuration	The contact duration in seconds.
DNIS	The Dialed Number Identification Service.
DTMFDigits	The ANI-related tones generated by a touch tone telephone to denote the 10 numbers, star, and pound keys on a telephone.
DataSourceName	The name of the switch.
DeviceName	Either the Primary extension or workstation name.
EmployeeGroup	The group to which the employee belongs.
EventType	Event in a call, such as Employee Level, System Level, CTI Level, Contact Level.
ExceptionReason	You can create a recording rule that will mark a call meeting the rule's criteria as an exception. The Exception Reason field identifies the reason it's considered an exception.
ExtendedCallHistory	Provides a history of the call states through which the contact has gone.
Extension	The employee's phone extension.
ExtractionJobName	The name of the extraction job that extracted the call.
Fired Business Rules	Lists recording rules that have been triggered.
FirstMessage	The first message sent by the Recorder.

Attribute	Description
GlobalCallID	Globally unique call identifier. This will be populated in most environments if the switch or CTI infrastructure supports it.
LastMessage	The last message sent by the Recorder.
LoggedOnDuration	The length of time the employee was logged on the switch.
NetworkID	The user's network logon ID.
NumberDialed	The number dialed.
NumberOfHolds	The total number of holds in the contact.
NumberOfConference	The total number of conference events in the contact.
NumberOfTimes Transferred	The total number of transfers in the contact.
Organization	The organization of the employee involved in the call.
Parties	All parties involved in the current call.
PauseDuration	The pause duration in seconds.
PrimaryExtension	The primary extension of the phone associated with the recording.
Queue	The switch queue.
SerialNumber	The serial number of the Recorder for the primary recording of an interaction.
Skill	The skill of the employee on the switch, such as Genesys skills.
SourceCallIdentifier	The unique identifier provided to the call by the source recording system. This identifier is mapped to ensure that the source identifier of each call is maintained when the call is extracted.
Source QM Database Server	Not supported.
SupervisorName	The supervisor of the employee involved in the call.
ThirdParty	Identification of a third party in the call.
TimeOnHold	The total amount of time in seconds the contact was on hold.
Trunk	The Trunk on which the contact is being recorded.
TrunkGroup	The Trunk Group on which the contact is being recorded.
Workstation	The name of the employee's workstation.

Attribute	Description
WrapupTime	Indicates how much time the employee spent doing work related to the call after the call ends.

All of the above are available in the Attributes area in the Enterprise Manager.

4. Click **Save**. The attributes are saved for the selected adapter.

Related topics

[Adapter behavior and troubleshooting \(page 330\)](#)

Adapter behavior and troubleshooting

Adapter not receiving CTI events

If the adapter does not appear to be receiving CTI events, consider whether any of the following apply:

- Some integrations require a client to be installed (JTAPI, Avaya TSAPI, Alcatel TSAPI).
- Most integrations “Register” for events based on Data Source Groups or Extensions configured.

Attributes are not being tagged

This may be due to a missing or incorrectly configured custom attribute in an adapter. See [Attributes \(page 271\)](#).

What happens when the connection with a workstation is lost?

The system keeps track of workstations that are logged in and connected to the Recorder Integration Service using the employee server.

When a connection between the Recorder Integration Service and workstation is lost, the workstation is logged out. If the connection to the employee server is lost, all workstations are logged out. If a specific adapter (as opposed to the Recorder Integration Service as a whole) is disconnected or shut down, only employees associated with that adapter will be disconnected.

Related topics

[Configure adapter custom attributes \(page 326\)](#)

Configure Secure Communication

When SSL communication is enabled, the Recorder Control Gateway secures communication between remote recorders and the Recorder Integration Service (RIS).

Topics

[Enable secure communication between the RIS and remote recorders333](#)

Enable secure communication between the RIS and remote recorders

When SSL communication is enabled (**Enable HTTPS** is selected on the Security page in System Management), you can turn on secure communication between remote recorders and the Recorder Integration Service (RIS) by enabling the Recorder Control Gateway role.

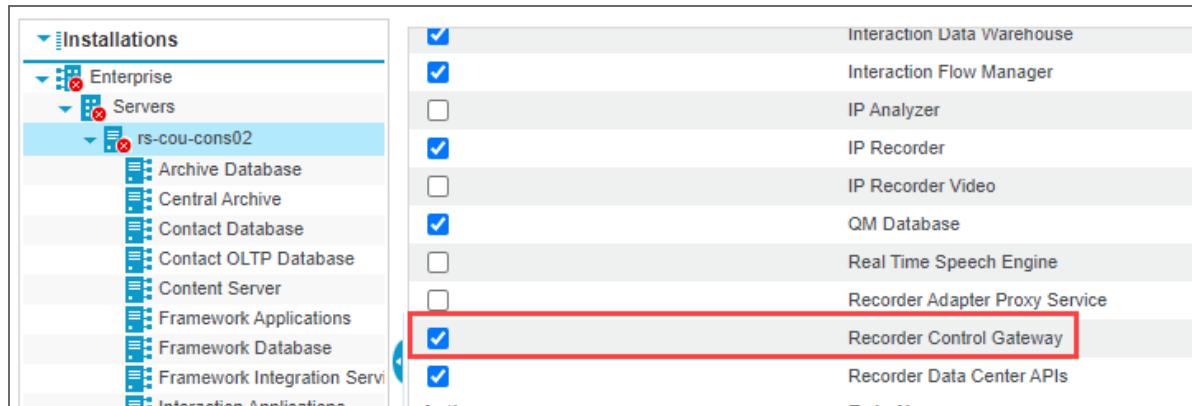
The Recorder Control Gateway

The Recorder Control Gateway is a software component that supports secure communication between remote recorder components over an NGA interface. The Recorder Integration Service uses the NGA interface to initiate and start communication with the capture engines (IP, TDM, and Screen recorder) using a proprietary NGA protocol. The Recorder Control Gateway serves as a central connection hub and gatekeeper to proxy all external communications with the local recorder roles. It provides client authentication through the system API key and provides encryption.

Starting with V15.2 2020R1, the Recorder Control Gateway is installed on each Recorder platform installation. When enabled, it runs as a Windows NT service and operates in a default Fallback mode. In Fallback mode, if a client, such as RIS, fails to connect to the Recorder Control Gateway, it will directly connect to the recorder over TCP using the plain-text NGA protocol.

Procedure

1. Go to **System Management**. Under **Enterprise**, select **Settings**.
2. In the tree structure, select a server, then select the **Server Roles** tab.
3. Select the **Recorder Control Gateway** role.



4. Select **Save**.

Related information

Configure Server Roles (*Enterprise Manager Configuration and Administration Guide*)

Recorder Control Gateway Port (*Firewall Ports Configuration Guide*)

Configure high availability

This section describes how to configure High Availability (also referred to as Redundancy) for the Recorder.

Topics

High availability	335
Recorder redundancy	338
Integration Service redundancy	361
Recorder Integration Service failover from main to back up	364
N+1 redundancy with SIP trunk recording	365
Troubleshooting	366

High availability

The Recording solution provides high availability through redundancy of the Recorders, Integration Service, or both.

The following sections describe the types of redundancy available, and subsequent sections provide configuration instructions for the basic scenarios for each. You will find additional direction for specific integrations in the applicable *Integration Guide*.

Recorder Redundancy

There are three types of Recorder Redundancy:

- N+N, in which all calls are recorded by two paired Recorders. (N+N requires Integration Service Redundancy as well.)
- N-Dedicated M-Shared, in which calls are recorded by a Main N Recorder, with a Backup M Recorder available to take over should N experience any errors.
- N+M All Shared, in which all calls are load-balanced across a pool of Recorders.

Integration Service Redundancy

All varieties of N+M may be combined with either a single Integration Service (no redundancy) or a pair (referred to as 1+1 Integration Service redundancy).

N+N requires 1+1 — that is, each pair of Recorders will have a corresponding pair of Integration Services.

Choosing a Location for your Main Integration Service in N+M

You may find it optimal to designate that the main Recorder Integration Service be that of the M Recorder, and the backup Recorder Integration Service as that of the N Recorder. In this configuration, the loss of the N Recorder means that the M system will pick up immediately as it is already designated as main. A loss of the M recorder will cause tagging loss for a time, but recording will continue on the N Recorder. Primary control of the Recorder Integration Service will then change to the N Recorder and tagging will commence.

In N-Dedicated M-Shared environments, you should never designate the Recorder Integration Service on the N-Dedicated Recorder as main, thereby co-locating these resources and creating a single point of failure. Failure of the CTI adapter on the N Recorder will cause the loss of all softphones (both dedicated and shared) and it will take time to transition over to the backup Recorder Integration Service.



Again, if shared resources are used, the Recorder Integration Service must not be collocated with a Recorder hosting dedicated resources (for the signaling service). This is because the "shared" DMCC resources will ultimately be managed over the same link as the dedicated ones, which means that failover won't be possible.

If, on the other hand, you only use dedicated resources (as in N+N), you may collocate the Recorder Integration Service on the Recorders.

! You may not associate more than one Integration Service to a single data source (except in a 1+1 redundant configuration, in which the servers are "paired", replicating the configuration of the main to the backup). So, if you associate more than one Recorder with a single CTI switch, those recorders must all be associated with the same main Integration Service.

Screen recorder failure

A screen recording failure will cause the loss of screen recordings in progress. The next call that triggers screen recording will prompt the system to look for a viable Recorder.

Backup servers

Integration Service and Recorder N+N redundancy involves the pairing of servers, wherein you can specify that a backup server automatically assume the functions of the main by creating a "secondary role" and pairing it to a server. This duplicates the server settings and associations by copying a role from one server (the main server) to another (the backup server).

All associations to the role (such as an association to a Recorder) are copied from the primary to the secondary role. Existing associations for the secondary role are then disabled, including phone extensions in Member Groups.

i To set up a secondary role, you must have Edit Installation Hierarchy privileges and privileges for the role.

Please note the following restrictions for secondary roles:

- Only active roles can be paired (that is, have primary/secondary role relationship).
- There can be only one secondary role instance for each primary instance, and only one primary per secondary instance.
- Deactivating a role removes the pairing.
- A role cannot be paired with a role that is already paired.
- When you unpair a primary role, the secondary role is also unpaired.
- When you remove a primary role's association to a data source or to rules, the same associations are also removed on the secondary role. When you add/associate a primary Integration Service to a data source, the secondary role is also associated.
- You cannot copy settings to a secondary role by using the "Copy Role Settings" feature.
- You cannot use the "Create Role from Existing" feature if a role is paired.
- If you update a primary server role on the Settings tab, the system applies all applicable updates to the secondary role automatically.

- Some fields, specific to the secondary role, such as an IP address, will not be updated. (Select the Settings screen for the secondary role in order to edit the fields that are specific to the secondary.)



After making any Server role configuration changes, manually check for any services or applications that require a restart; this will be indicated by an alarm. For more information, refer to [Start and stop components \(page 265\)](#).

Recorder redundancy

This section describes:

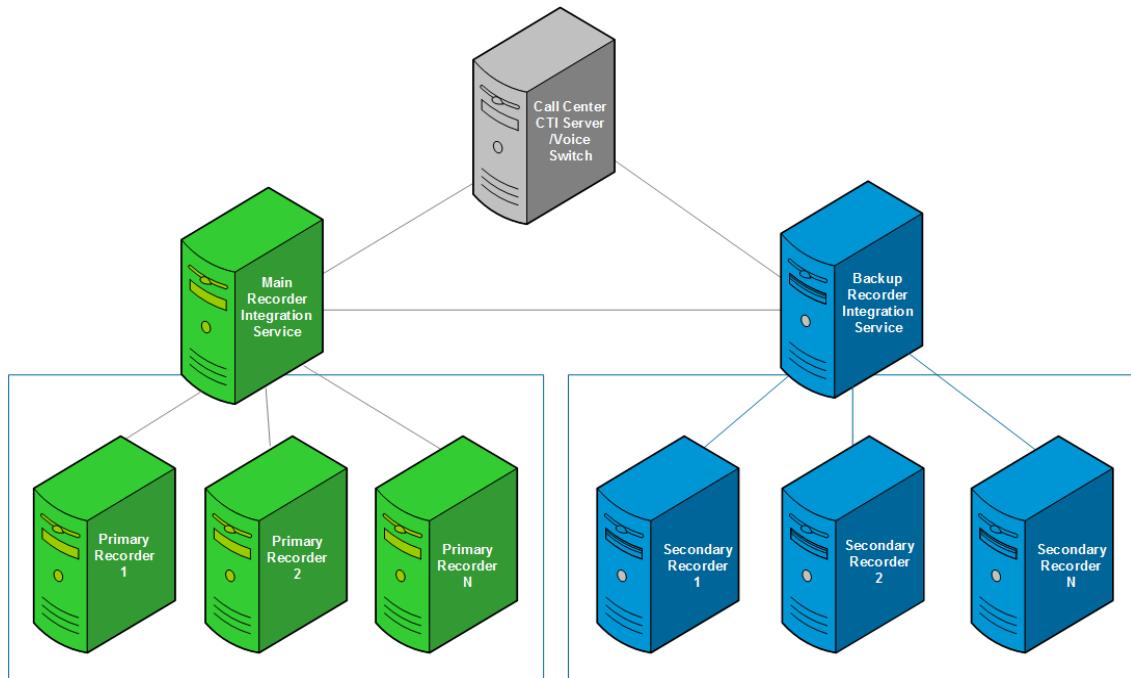
- N+N (page 338)
- N+M (page 347)
- N+N and N+M redundancy with IP Analyzer (page 358)

N+N

In N+N Redundancy, a deployment of Recorders and Integration Service servers is replicated one-for-one, creating a main system paired with a backup system. Each set of paired servers connects to the same telephony and data network infrastructure, and records the same CTI and audio data.

Each set of paired Recorders has a primary/secondary relationship. Although the main and backup servers are synchronized for recording, only one Recorder in each pair is the primary at any given time, making the other Recorder in the pair the secondary. A failure on the primary results in a reversal of roles -- the failed primary becomes the secondary and the secondary becomes the new primary.

By default, only the primary in each pair updates the databases for the recorded calls. If you need both copies marked to the database, you can enable Full Duplicate Recording, in which case both the primary and the secondary update the database for recorded calls.



Note the following general considerations related to N + N:

- Failover is initiated based on the state of the Recorder; that is, the state of each extension is compared to its paired extension. If there is a failure at the extension level, the extension marking switches to the paired Recorder and Integration Service.
- The main Integration Service does not communicate with the backup Recorders. Conversely, the backup Integration Service does not communicate with the main Recorders.
- The secondary always retains the same recordings as the primary. By default, the secondary omits the step of submitting recordings to workflow for consolidation and archiving. When Full Duplicate Recording is enabled, the secondary also submits recordings to workflow.
- If the primary control changes, N+N rollback occurs. N+N rollback means the secondary-turned-primary submits the previous 15 minutes (default setting) of calls to the system, and all new calls from that point in time. If Full Duplicate Recording is enabled, N+N rollback does not apply.
- Situations can arise where a call is recorded on the secondary, but not on the primary. This state is not associated with a Recorder failure, so the primary control remains with the main Recorder. Recorder-based failover marking ensures that the secondary Recorder consolidates the call when the primary has not recorded the call, despite the main retaining primary control. When the secondary records the call longer than the primary recorder both Recorders consolidate the same call.
- The redundancy controller prevents more than three switchovers on the same pair of channels/extension within a one-minute time period.
- When a channel moves from primary to secondary, an alarm appears in the Enterprise Manager. You can view the state of each channel/extension, whether primary or secondary, in Recorder Manager.
- All parts of contacts that start on the primary and fallback to the secondary (that is, even non-ended interactions or segments) are kept.
- When the IP Capture service is restarted on any Recorder from an N+N pair, all Extensions will become primary on both main and backup Recorders of that N+N pair. Until the primary control status of these Extensions is identified by the Redundancy Controller, the recordings from both recorders will be marked to the database. By default, the Redundancy Controller takes 30 seconds to decide primary control status of the Extensions on these recorders. This is configurable through the FailoverMapsCompareWaitTime configuration parameter of the RecorderGeneral.xml file.



An N+N deployment doubles the number of recorders and requires a primary and secondary RIS server. This type of deployment increases the number of servers required for an N+N configuration.

- IP video recording is not supported for N+N.

Supported environments

N+N supports the following recording environments:

- Passive TDM recording
 - Station Side
 - Trunk Side
- VoIP Interception
 - Signaling environments
 - RTP-based recording
 - With or without load balancers

Full Duplicate Recording

When Full Duplicate Recording is enabled, recordings from both the primary and the secondary Recorder are consolidated to the database. Use of this feature, especially applicable in compliance recording environments, provides even more robust redundancy and increased visibility for every interaction recorded by both the main and the backup systems.

The feature pairs recordings from the primary and the secondary. Access to the paired recordings is available for interaction replay and for Archive:

- **Interaction replay:** By default, only interactions from the primary recorder are shown. If a user requests interactions from the secondary recorder, pairs of interactions are shown and available for replay.
- **Archive:** Configure which interactions campaigns use. For example, create a campaign to archive only primary recordings to a medium reserved for the main system. Then create a second campaign to archive only secondary recordings to a medium reserved for the backup system.

How to configure Full Duplicate Recording

Configure Full Duplicate Recording on each phone data source by selecting **Keep duplicate recording**. The feature is disabled by default. See the related topics section to learn more.

Effect on database size and Archive media



After you enable Full Duplicate Recording, the sizing requirement for the database increases since each new interaction is duplicated in the database. If you archive recordings from both the primary and the secondary recorders, storage requirements are doubled for Archive media.

If you intend to enable Full Duplicate Recording, plan for the appropriate amount of database and Archive media storage. See the *Performance and Sizing Guidelines* for more information.

Related topics

[Create a phone data source \(page 49\)](#)

Load balancing in N+N

Load balancing is accomplished by distributing calls across multiple data centers/gateways, over the public network but managed by a single distributed PBX. In this configuration, it is possible to set up N + N with an N- main and a backup Recorder in each data center. When using a load balancer in N+N, you *must* ensure that the same signaling and media are presented to each Recorder in any N pair identically. The media must also be unique to that pair, and not presented to any other pair of Recorders. The collective channel count at each data center must be less than the channel count of a single Recorder. (Also note the particular member group settings required in the configuration section that follows.)

There are challenges inherent in configuring an external load balancing device to *guarantee* that each N pair of recorders receive identical signaling and media. Do not proceed with such an implementation if meeting this requirement is not possible.

If you can meet this requirement, and the required channel count is more than a single Recorder can accommodate, then you can use shared interception. Shared interception does, however, introduce a dependency on CTI. The Integration Service must be available for recording to occur.

Related topics

[Configure N+N Recorder redundancy \(page 341\)](#)

[Promote backup calls \(page 344\)](#)

[Disable recording-based failover marking \(page 346\)](#)

[Create a phone data source \(page 49\)](#)

Related information

Performance and Sizing Guidelines

Configure N+N Recorder redundancy

Before you begin

Install two Recorders in your Site, and assign to each the Recorder Integration Service role and at least one Recorder role (see [Set up Recorder roles and associations \(page 44\)](#)). You may have the Integration Service on separate servers, but they can co-exist on the same server as the Recorder.

If you require screen recording, enable Screen Recorder roles as well.



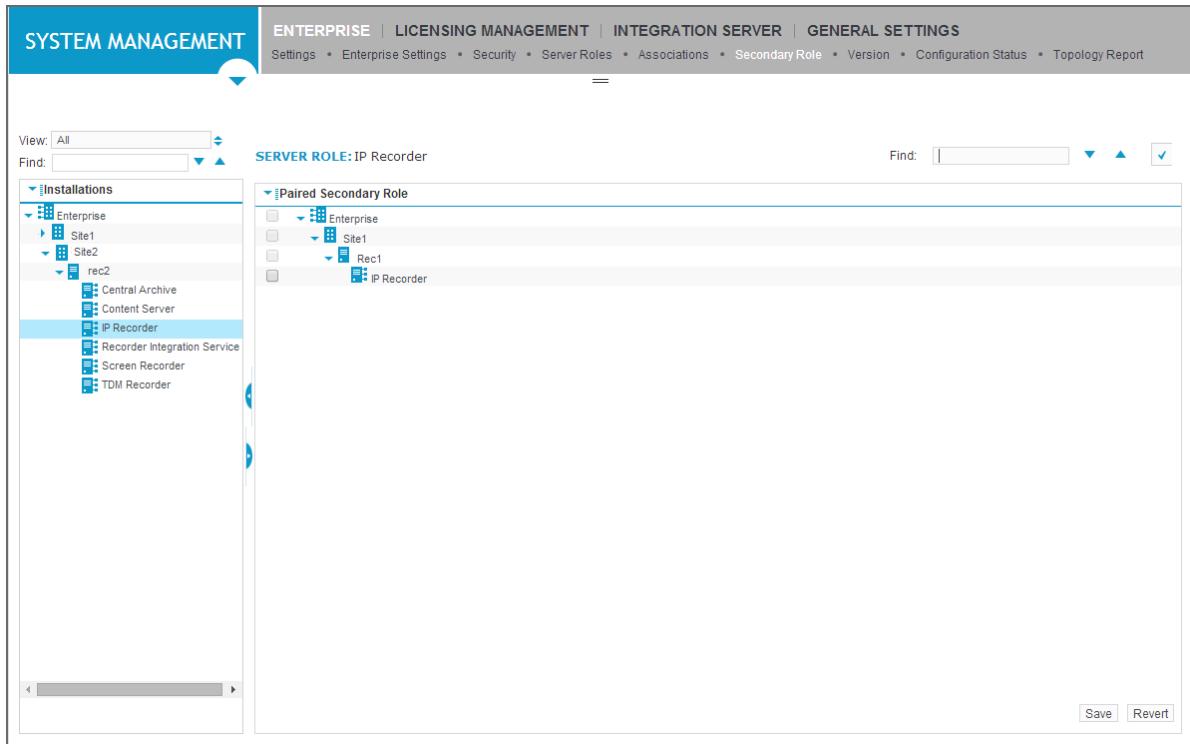
Ensure that the Recorder Integration Service role of the server to be used as the main Integration Service Server includes the fully qualified domain name (FQDN).



The Primary Recorder Integration Service role should not be co-located with a Backup Recorder. Likewise, the Secondary Recorder Integration Service role should not be co-located with a Main Recorder.

Procedure

1. In Enterprise Manager, click **System Management**.
2. Under **Installations**, locate the Recorder that will act as the Main, and click the triangle beside that node.
3. Select the **IP Recorder** or **TDM Recorder** role.
4. Click the **Secondary Role** screen. Locate the Recorder you want to act as the Backup, then select the check box beside its Recorder role (IP Recorder or TDM Recorder).



5. Click **Save**.
6. Select the **Recorder Integration Service** role under the Main Recorder.
7. Click the **Secondary Role** screen. Locate the Backup Recorder, then select the check box beside its **Recorder Integration Service** role.
8. Click **Save**.
9. You will now be able to see the associations for the Recorder Integration Service on the **Associations** and **Secondary Role** screens. You can see the associations for the Recorder on the **Secondary Role** screen.

The associations of the Main will be replicated on the Backup.



Hereafter, you can only alter these associations from the perspective of the Main node; the associations on the Backup node will be read-only.

10. Configure the phone data source and assign to the main Integration Service ([Create a phone data source \(page 49\)](#)).



Both screen and phone data sources must be associated with an Integration Service, because when the Integration Service is in control, it will control both screen and phone recording.

11. Configure a member group and assign to the Main Recorder. These settings will be replicated on the Backup Recorder.



In each case, if using a load balancer, set a load balancing type of Media Only or Media with Signaling, and refer to the specific guidelines set out in the previous section.

If you require a higher channel count than that of a single Recorder, use Shared Interception as the load balancing type.

Refer to the following table for details about the type of member group you should create:

VoIP Interception

	Primary Recorder Configuration	
Supported Switch Environment	Member Group	Recorder Control Type
Avaya	IP Extension Pool	Recorder Control
Avaya NES	IP Extension Pool	CTI Control
Alcatel	IP Extension Pool	Recorder Control
Cisco	IP Extension Pool	Recorder or CTI Control
Genesys	IP Extension Pool	Recorder Control

VoIP Delivery

	Primary Recorder Configuration	
Supported Switch Environment	Member Group	Recorder Control Type
SIP	IP Extension Pool	Recorder or CTI Control
Avaya DMCC	Multiple Registration Extension Pool	NA

TDM Trunk

Primary Recorder Configuration	
Member Group	Recorder Control Type
Compliance Trunk Span	Recorder or CTI Control

Station Tap

Primary Recorder Configuration	
Member Group	Recorder Control Type
Compliance Station Extension Group	Recorder or CTI Control

12. Create phones and assign to the member group created above ([Create and edit phones/extensions \(page 125\)](#)).
13. Complete the rest of the configuration process as described in:
 - [Configure recording \(page 42\)](#)
 - [Set up recording rules \(page 303\)](#) (assign any rules to the primary Integration Service)
 - [Configure a CTI adapter \(page 322\)](#)
14. Restart the Integration Service. It is only necessary to restart the Recorder if you have changed its **Enable Return Primary Control to Main After Recovery** setting.



You must restart the Recorder IP Recorder pairing (assigning backup to main) and IS pairing (assigning backup to main) configuration changes.

Related topics

[N+N \(page 338\)](#)

Promote backup calls

In N+N, if the Main Recorder server goes down, the last 15 minutes worth of calls (rollback window) on the Backup Recorder are automatically promoted into the database and archive systems by the Recorder Redundancy Controller.

To promote backup calls on the Backup Recorder outside the rollback window, use the manual procedure that follows.

Procedure

1. On the Backup Recorder, open a Windows Command Prompt as an Administrator, and change the directory to `IMPACT360SOFTWAREDIR%\ContactStore`.
2. Run the `WorkflowShell` utility by typing “`WorkflowShell`”. This command opens an interactive command prompt.
3. To see the available options, enter **help rebuild**.
4. To rebuild the Workflow, enter a command using the following syntax:

```
Rebuild (Full|Fix) [IncMasterCalls [IncSlaveCalls [StartTime [EndTime]]]]
```

- *Rebuild Full* usage notes:
 - Clears all calls from Workflow tables.
 - All INUMs in the call buffer which match the criteria you specify are added to Workflow.



To mark the calls into the database, reprocess call date ranges using Recorder Manager. See [Reprocess call date ranges \(page 196\)](#).

- *Rebuild Fix* usage notes:
 - INUMs in the call buffer but not already in Workflow and which match the criteria you specify are added to Workflow for consolidation.
 - INUMs already in Workflow are not added or reprocessed.
 - Added calls are automatically marked into the database, made available for replay, and considered for archive using your existing archive configuration.
 - *IncMasterCalls* and *IncSlaveCalls* format: Specify as *true* or *false*.
 - *StartTime* and *EndTime* format:

[year] [month] [day] [hour] [minute] [seconds]

Where [seconds] is specified to ten thousandths of a second (four places).

5. To rebuild Workflow, including all primary and secondary calls in the call buffer, enter the following command:

```
Rebuild Fix true true
```

Optionally, include StartTimes and EndTimes in the format shown above.

6. Allow time for the rebuild to finish.
7. After the rebuild finishes, exit the WorkflowShell command prompt by entering the **quit** command.

Related topics

[N+N \(page 338\)](#)

Disable recording-based failover marking

If a call is recorded on the backup Recorder, but not on the main Recorder, primary control remains with the main Recorder. You can prevent both Recorders from consolidating the call in these cases, resulting in duplicated recordings, by configuring a setting on the Redundancy Controller.

Procedure

1. On the Redundancy Controller, open Windows Explorer and go to:

%IMPACT360SOFTWAREDIR%\ContactStore

2. Open the following file in a text editor:

RecorderGeneral.xml

3. Locate the following parameter:

RecordingBasedFailoverMarkingEnabled

4. Set the value to false.

For example:

```
<x:RecordingBasedFailoverMarkingEnabled>false</x:RecordingBasedFailoverMark  
ingEnabled>
```

5. Save your changes to the file and close it in the editor.

6. Open a command window and use the following command to run the checksum utility on the RecorderGeneral.xml file. This will add a new checksum with the modifications. Failure to complete this step will result in a 'file tampered' alarm.

```
%IMPACT360SOFTWAREDIR%\ContactStore\Tools\Checksumutil.exe -g  
%IMPACT360SOFTWAREDIR%\ContactStore\RecorderGeneral.xml
```

7. Restart the Redundancy Controller server.

Related topics

[N+N \(page 338\)](#)

N+M

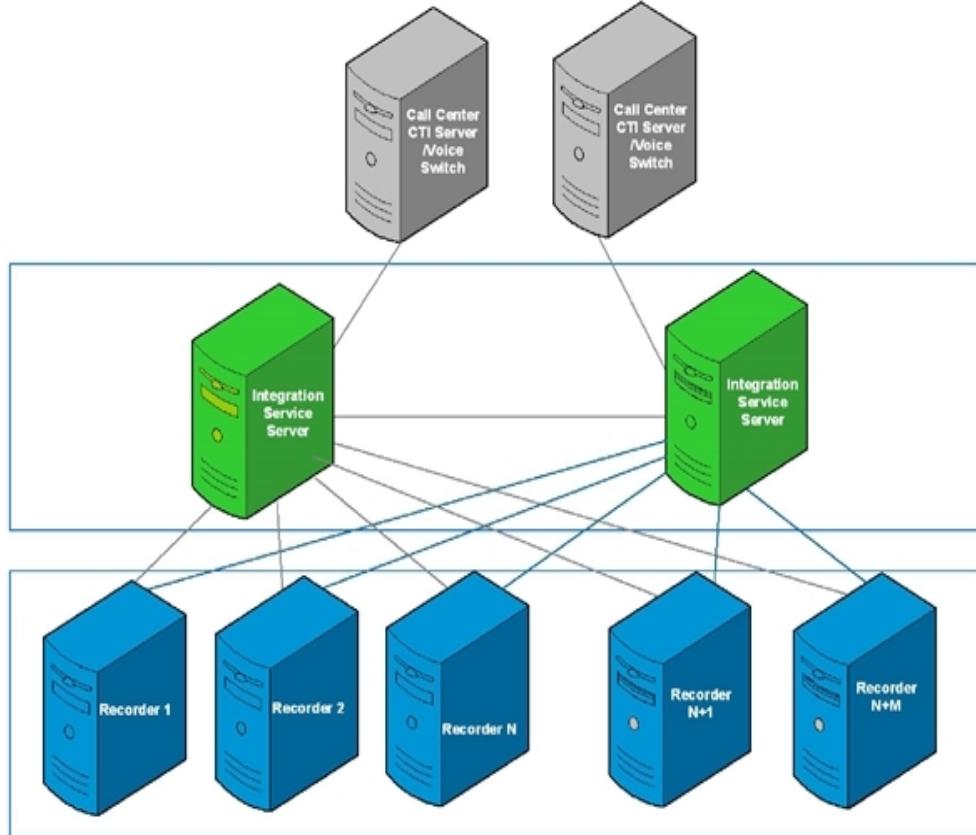
An N+M system is configured with more recording resources than necessary to prevent audio or CTI loss in any case of individual recorder failure, and any network disconnection scenario.

In CTI controlled interception, the Recorder Integration Service gives signaling to all Recorders, so the Recorder that receives audio (through load balancing) can record it. In Recorder controlled interception, the load balancer gives signaling to all Recorders, so the Recorder that receives audio (through load balancing) can record it.

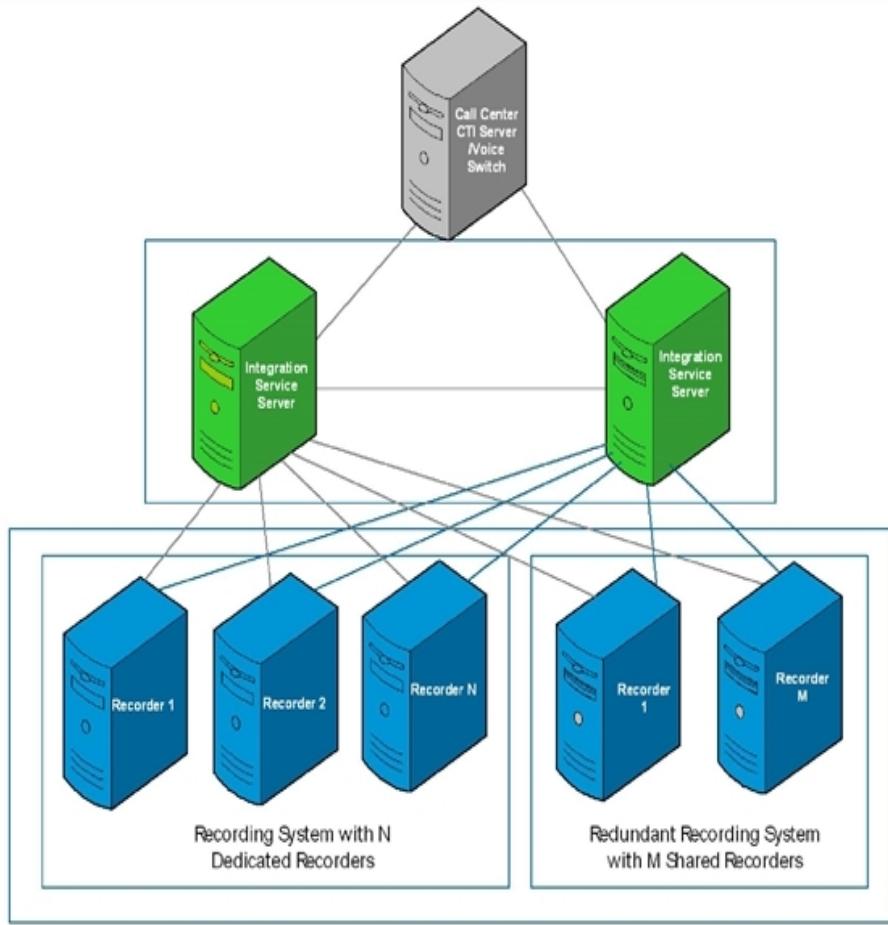
The two main N+M scenarios are *N+M All Shared* and *N Dedicated + M Shared*.

- i** While the following diagrams depict scenarios involving two Integration Services, N+M all shared or N dedicated + M shared can be accomplished using only a single Integration Service.

N+M All Shared involves a pool of M recorders all configured in the same way. Load balancing within shared recorders in a DMCC delivery environment follows the N+M All Shared algorithm. For additional information about load balancing, see [Load Balancing in N+M All Shared \(page 348\)](#).



In **N Dedicated + M Shared**, N recorders are paired with shared M recorders. These recorders remain in standby mode until an N recorder fails, at which time an Integration Service server will instruct an M recorder to take over on that channel or extension.



In environments that are N dedicated trunk side (either TDM or SIP trunk) and M shared (all types), if the dedicated trunk side recorder experiences issues (indicated by one or more alarms on the Recorder Manager status page for that recorder), the Integration service will engage the shared recorder to record a call. The dedicated recorder may still be able to record a call, even though a problem was reported. Therefore, it is possible that the system will have a duplicate recording of a call, and two interactions will appear in the portal as having the same attributes and audio. This is expected behavior.

For example, a dedicated SIP trunk recorder may discover a loss of packets for some calls that occurred in the past. An alarm is raised indicating a minor issue with the recorder. For future calls, Integration Service will engage a shared recorder to record the calls, in addition to the dedicated recorder that may or may not lose some packets. While the problem with the dedicated recorder exists, duplicate interactions may be found for each call in the portal—one recorded by the dedicated recorder (and which may have inferior audio quality) and another one recorded by the shared recorder (with good audio quality).

Load Balancing in $N+M$ All Shared

Load balancing is accomplished by the Recorder Integration Service selecting the best recorder from the pool. The definition of "best" can vary between integrations, so reference the specific integration

guide for information about any variations or differences.

The general load balancing algorithm takes into account:

- Current error priority
- Current utilization level, and
- Last recording routed to that recorder

The Recorder Integration Service first divides the overall recorder pool into sub-pools based on the recorder health. What constitutes health can vary between environments, but the recorder normalizes the overall health into a consumable value reported to the Recorder Integration Service. Within each health pool, the recording system orders the available recorders by their current server utilization. Server utilization is a relative scoring based on the hardware assigned to the system, the recording load, and any extra real time load. It is possible for two systems to have the same channel license count and same active recording load, but end up with different server utilization scores. If the server utilization scores are equivalent, the recording system will order the available recorders by their recording utilization, or remaining capacity. If there are no recorders with available capacity within the current health pool, the recording system moves on to the next health pool. Recorders with the same utilization level, or remaining capacity, are ordered by a least-recently-used (LRU) approach based on the last recording timestamp. The internal iteration order of the associated recorders within a pool is non-deterministic and not directly managed by the recording system. When all input conditions are equivalent, the recording system can choose any recorder within the pool for recording.

Real-time Monitoring

Redundancy and real-time monitoring are supported as long as the Integration Service is controlling an active recorder and a real-time audio interaction can be initiated.

Configure N+M redundancy

Before you begin

Install the Recorder on two or more servers and assign appropriate Recorder role to each. Install the Integration Service on two servers (these do not need to be on the same machine as the Recorders)—one will act as the main and one as the backup.



1+1 Integration Service deployments with N+M Delivery environments must use global resource allocation (which means that the Integration Service is falling back to a Recorder with which the extension is not associated).

In these cases, if the default behavior is to delete a recording (this will be the case in **Application Controlled** or **Start at Trigger** extension recording modes), or if the CTI adapter is down and the Recorder Fallback Type is set **Never** (meaning it will delete recordings when the adapter is down), then the recordings will be deleted. This is also true of Selective Service Observe and Selective Single Step Conferencing.

Procedure

1. If you require Screen Recording, enable the Screen Recorder role. Screen Recording servers can also be separate from the Integration Servers, and in terms of redundancy there is no limit on the number you can have in your system.
2. Associate the Recorders with the main Integration Service. See [Associate a Recorder with the Integration Service \(page 46\)](#).
3. If you are using a backup Integration Service, pair the first Integration Service with the second as described in [Configure Integration Service 1+1 redundancy \(page 363\)](#).



Note that the Recorders are not paired.

4. Create a phone data source ([Create a phone data source \(page 49\)](#)) and assign it to the main Integration Service.
5. Configure Gateway Side Correlation Pool member groups and assign them to *both* Recorders. Create additional member groups depending on your environment, as described in following tables.

N+M All Shared		
Scenario	Supported Environments	Settings
N+M All Shared Delivery Note: It is not necessary to set a load balancing type for any of these scenarios.	Avaya IP with Single Step Conferencing	<ul style="list-style-type: none"> • Extension recording resource member group settings (page 75), containing softphones. • Selective extension pool member group settings (page 77) • Set the Recorder Control Type to Single Step Conferencing.
	Avaya IP with Service Observe	<ul style="list-style-type: none"> • Extension recording resource member group settings (page 75), containing softphones. • Selective extension pool member group settings (page 77) • Set the Recorder Control Type to Service Observe. • In the Phone data source, specify settings for Service Observe.

N+M All Shared		
Scenario	Supported Environments	Settings
	Avaya TDM Service Observe	<ul style="list-style-type: none"> • Trunk span recording resource member group settings (page 75), containing softphones. • Set the Recorder Control Type to Service Observe. • In the Phone data source, specify settings for Service Observe.
	Avaya NES/Nortel CS1000 DMS	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to Selective Delivery (Duplicate Streamed).
	Cisco DMS	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to: <ul style="list-style-type: none"> ▪ Selective Delivery (Duplicate Streamed) (for application-controlled), or ▪ Full Delivery (External Controlled) (automatic).
	Genesys SIP using DMS	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to Selective Delivery (Duplicate Streamed).

N+M All Shared		
Scenario	Supported Environments	Settings
N+M All-shared with Load-Balancing	Cisco	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to Recorder Controlled or CTI Controlled. • Set the Load Balancing type to Media Only.
	Avaya	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to Recorder Controlled. • Set the Load Balancing type to Media Only.
	Avaya SIP	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to Recorder Controlled. • Set the Load Balancing type to Media Only.
	Avaya NES/Nortel	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to CTI Controlled. • Set the Load Balancing type to Media Only.
	Genesys IP Interception	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to CTI Controlled. • Set the Load Balancing type to Media Only.

N+M All Shared		
Scenario	Supported Environments	Settings
N+M All Shared with Shared Interception (no Load Balancing)	Cisco	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to Recorder Controlled or CTI Controlled. • Set the Load Balancing type to Shared Interception.
	Avaya	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to Recorder Controlled. • Set the Load Balancing type to Shared Interception.
	Avaya SIP	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to Recorder Controlled. • Set the Load Balancing type to Shared Interception.
	Avaya NES/Nortel	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to CTI Controlled. • Set the Load Balancing type to Shared Interception.
	Genesys IP Interception	<ul style="list-style-type: none"> • IP extension pool member group settings (page 71) • Set the Recorder Control Type to Recorder Controlled or CTI Controlled. • Set the Load Balancing type to Shared Interception.

N Dedicated + M Shared						
Mode	Supported Environments		Settings			
	Switch	Type	N Recorder		M Recorder	
			Member Group	Recorder Control Type	Member Group	Recorder Control Type
Delivery	Avaya	IP SO + IP SSC Please note that you must create two member groups for each Recorder as described at right.	1) Extension Recording Resource	Service Observe	1) Extension Recording Resource	Single Step Conference

N Dedicated + M Shared						
Mode	Supported Environments		Settings			
	Switch	Type	N Recorder		M Recorder	
			Member Group	Recorder Control Type	Member Group	Recorder Control Type
		The virtual extensions must be different. The target extensions (those being recorded) should be the same. In addition, for each N Recorder you must create an adapter of type CMAPI, regardless of the adapters present in the Integration Service server (see the <i>Avaya Integration Guide</i> for more information).	2) Dedicated Extension Pool Add all of the DNs you want to record to this member group, and associate it with the Extension Recording Resource above.		2) Selective Extension Pool Add the same DNs to this member group, and associate it with the Extension Recording Resource above.	
		IP Multiple Registration + IP SSC	Multiple Registration Extension Pool	Multiple Registration Control	1) Extension Recording Resource 2) Selective Extension Pool	1) Single Step Conference

N Dedicated + M Shared						
Mode	Supported Environments		Settings			
	Switch	Type	N Recorder		M Recorder	
			Member Group	Recorder Control Type	Member Group	Recorder Control Type
		TDM SO + IP SSC	Trunk Span Recording Resource	Service Observe	Extension Recording Resource	Single Step Conference
		TDM Station Side + IP SSC	Compliance Station Extension	Recorder or CTI Control	Extension Recording Resource	Single Step Conference
		TDM Station Side + IP SO	Compliance Station Extension	Recorder or CTI Control	Extension Recording Resource	Service Observe
		TDM Station Side + TDM SO	Compliance Station Extension	Recorder or CTI Control	Trunk Span Recording Resource	Service Observe
		TDM Trunk side + IP SSC	Compliance Trunk Span	Recorder or CTI Control	Extension Recording Resource	Single Step Conference
		TDM Trunk side + IP SO	Compliance Trunk Span	Recorder or CTI Control	Extension Recording Resource	Service Observe
		TDM Trunk side + E1 LS (TDM SO) Supported only on ISDN Trunks (AiLogix DT boards only)	Compliance Trunk Span	Recorder or CTI Control	Trunk Span Recording Resource	Service Observe

N TDM trunk + M IP Internal Call						
Mode	Supported Environments		Required Configuration			
	Switch	Type	N Recorder		M Recorder	
			Member Group	Recorder Control Type	Member Group	Recorder Control Type
Delivery + TDM	Avaya	TDM Trunk side + IP SSC	Compliance Trunk Span	Recorder or CTI Control	Extension Recording Resource	Single Step Conference
		TDM Trunk side + IP SO	Compliance Trunk Span	Recorder or CTI Control	Extension Recording Resource	Service Observe
		TDM Trunk side + E1 LS (TDM SO) Supported only on ISDN Trunks (AiLogix DT boards only)	Compliance Trunk Span	Recorder or CTI Control	Trunk Span Recording Resource	Service Observe

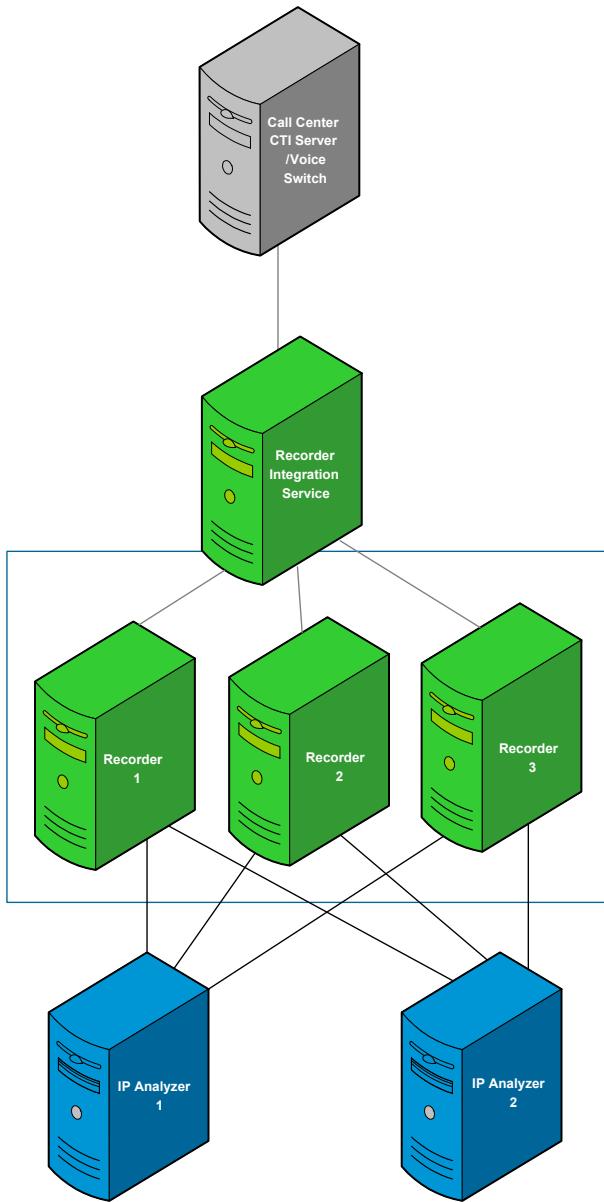
6. Complete the rest of the configuration process as described in:

- [Configure recording \(page 42\)](#)
- [Set up recording rules \(page 303\)](#) (assign any rules to the main Integration Service)
- [Configure a CTI adapter \(page 322\)](#)

N+N and N+M redundancy with IP Analyzer

In IP Analyzer Redundancy, there are two analyzers, each associated to all recorders.

Upon loss of connection with a configured Analyzer server, the system falls back to RTP detection for those member groups that are Recorder Controlled (other member groups will not be affected by IP Analyzer disconnection). Extension to IP mapping will be used in RTP detection to record calls.



You must associate at least one IP Recorder with the IP Analyzer role. It is also very important that you associate each analyzer with all Recorders in Enterprise Manager.

Use one of the following procedures to set up redundancy for IP Analyzer.

- [Configure redundancy for IP Analyzer for N+N \(page 359\)](#)
- [Configure redundancy for IP Analyzer for N+M \(page 360\)](#)



Version 11 includes enhanced alarming to generate an alert when a Recorder is not receiving messages from any of the associated analyzers (as long as at least one analyzer is sending messages there will be no alerts, however any single failed analyzer will have an alarm for this status).

Configure redundancy for IP Analyzer for N+N

To configure IP Analyzer for redundancy, complete the steps in this section.

Procedure

1. Pair the IP Analyzer roles:
 - a. In Enterprise Manager, click **System Management > Settings**.
 - b. Under **Installations**, locate the server containing the primary IP Analyzer role with which you want to pair a secondary role.
 - c. Click the triangle button beside the name of the server. Select the role, then **Secondary Role** (this will only be visible if pairing is possible given the available roles and servers). The **Paired Secondary Role** window appears, showing all eligible role instances.
 - d. Select a secondary role to be associated to the primary role.
 - e. Click **Save**.



If you make changes to the secondary role and click Save, the changes are not passed to the primary role. To unpair the role at any time, select the primary role, and then deselect the secondary role in the **Secondary Role** window.

2. Repeat step 1, this time pairing each IP Analyzer role to at least one IP Recorder role.

Configure redundancy for IP Analyzer for N+M

To configure IP Analyzer for redundancy, complete the steps in this section.

Procedure

1. Pair IP Analyzer roles:
 - a. In Enterprise Manager, click **System Management >Settings**.
 - b. Under **Installations**, locate the server containing the primary Analyzer role with which you want to pair a secondary role.
 - c. Click the triangle button beside the name of the server. Select the role, then click **Secondary Role** (this will only be visible if pairing is possible given the available roles and servers). The **Paired Secondary Role** window appears, showing all eligible role instances.
 - d. Select a secondary role to be associated with the primary role.
 - e. Click **Save**.

 If you make changes to the secondary role and click Save, the changes are not passed to the primary role. To unpair the role at any time, select the primary role, and then deselect the secondary role in the **Secondary Role** window.
2. Associate the primary IP Analyzer with *all* IP Recorders by clicking **System Management > Settings**, select a Recorder then click **Associations**, then selecting the appropriate check boxes to associate nodes list on the right with a node selected on the left. (Secondary IP Analyzers will automatically be associated with the Recorders as well.)

Integration Service redundancy

This section provides an overview of Integration Service 1+1 redundancy as well as Integration Service 1+1 configuration.

1+1

The Recorder Integration Service offers hot standby in the form of paired server roles. The pair is configured with the same kind and type of adapters, connecting with third-party systems that provide equivalent information. The pair has preference ordering of *Main* and then *Backup*. The order allows primary control to be preferred on one server over the other, when all other conditions are equal. Within the pair, primary control is negotiated at the data source level. The Integration Service with the best overall health (for example, number of healthy adapters) for a data source claims primary control over the data source. The responsibilities of the primary Integration Service differ between N+M and N+N Recorder redundancy models.

In the event of an Integration Service failure, *recording* (as opposed to tagging and other functions) becomes the highest priority of the system. In N+N solutions no audio should be lost, while in N+M, audio loss (if any) should only occur during the detection and switchover periods.

The *detection* period is the amount of time it takes the system to become aware that there is an issue. The *switchover* period is the amount of time it takes to completely switch primary control from the failing Integration Service to the other Integration Service.

The amount of time it takes to detect a failure will vary, depending on the type of failure, the network setup, and the third-party systems involved. Most issues are detected within one minute and failover happens immediately afterwards. During detection and switchover, screen recording, tagging and stitching may be incomplete for in-progress calls. Once switchover has completed, all new calls should be handled correctly.

You can find additional important details about Integration Service behavior in the event of a failure for Avaya and Cisco integrations in the corresponding Integration Guides, and in the Recorder Deployment Reference Guides for each deployment type.

N+M Recorder Redundancy

When using N+M Recorder redundancy, the primary Integration Service is responsible for all functions for the respective data source. Some of the responsibilities of the primary Integration Service includes tracking the calls on the data source, evaluating business rules, matching and tagging recordings, processing API commands, and handling Real-Time Monitoring requests. The secondary Integration Service works in a hot standby mode, tracking the same calls and gathering the same tagging data from the CTI feeds. Selective business rules may evaluate differently on the primary and secondary Integration Services, leading to minor differences for these configurations. The primary Integration Service is also responsible for any additional recordings associated with the tracked calls (for example, triggering screen recording for a phone call on a controlled data source).

In the event of a failure, primary control moves from one Integration Service role to the respective paired role. Once the fault has cleared and health restored, primary control may move back to the Primary Integration Service role if the “Return to Main” feature is enabled on the pair. This promotion process includes a synchronization period with a time delay and where all the active calls at the beginning of the synchronization period have cleared.

N+N Recorder Redundancy

When using N+N Recorder Redundancy, the paired Integration Service roles work together with paired recorder roles to create side-by-side recordings of each call. As such, both the primary and secondary Integration Service roles track, record, and tag the calls on respective paired recorders. Of the two recordings for a specified call, the better of the two is consolidated. Customers can optionally consolidate recordings from both recorders in the pair by enabling Full Duplicate Recording (select "Keep Duplicate Recording" on the data source).

Screen recording always uses N+M redundancy, which means the primary control between the Integration Service pair still affects N+N phone calls. The primary Integration Service is responsible for controlling the screen recording, but the recording matches to both sides of the Integration Service pair. This allows for screen recording to appear regardless of which side (or both) of the N+N system consolidates the call.

Configure Integration Service 1+1 redundancy

Before you begin

Install two Recorders and enable the Recorder Integration Service role on each.

Procedure

1. In Enterprise Manager, click **System Management >Settings**.
2. Under **Installations**, click the arrow to the left of the server you will consider the main Integration Service. Click the **Recorder Integration Service** role.
3. On the right-hand side, click the **Associations** screen.
4. Select the Recorder(s) you will use for the 1+1 Recorder Integration Service configuration.
5. Click **Save**.
6. Click the **Secondary Role** screen. Select the Recorder Integration Service on the server that will be the backup in your 1+1 configuration.
7. Click **Save**.
8. In the Installations tree, click the arrow to the left of the backup Recorder Integration Service server.
9. Click the **Recorder Integration Service** role.
10. Click the **Associations** screen. You should see the same associated Recorders as in the main Recorder Integration Service server, and the selections should be greyed-out and unselectable.
11. Click the **Secondary Role** screen. Ensure that the associated Recorder Integration Service server is selected and the selection is greyed-out and unselectable.
12. Complete the rest of the configuration process as described in:
 - [Configure recording \(page 42\)](#)
 - [Set up recording rules \(page 303\)](#) (assign any rules to the main Integration Service)
 - [Configure a CTI adapter \(page 322\)](#)

All data sources and rules associated with the primary Integration Service role will be associated with the secondary role. See [Backup servers \(page 336\)](#) for more information about the implications and limitations surrounding the pairing of servers.

Recorder Integration Service failover from main to back up

For the Recorder Integration Service, health is measured primarily by the CTI adapters configured and running against an assigned data source. The backup Recorder Integration Service can be determined to be healthier than the main Recorder Integration Service for a given data source. In this case, control over that specific data source is transferred to the backup. Likewise, if the main Recorder Integration Service is determined to be healthier than the backup, controls shift from the backup to the main.

After a failure, once the main Recorder Integration Service regains equal to the backup, the two services negotiate a warm handover back to the main by default. Users can control this behavior at the Recorder Integration Service server role level. Some environments and configurations recommend disabling this setting so refer to the integration guide for details.

Failover from the main Integration Service to the backup results in different behavior depending on the environment.

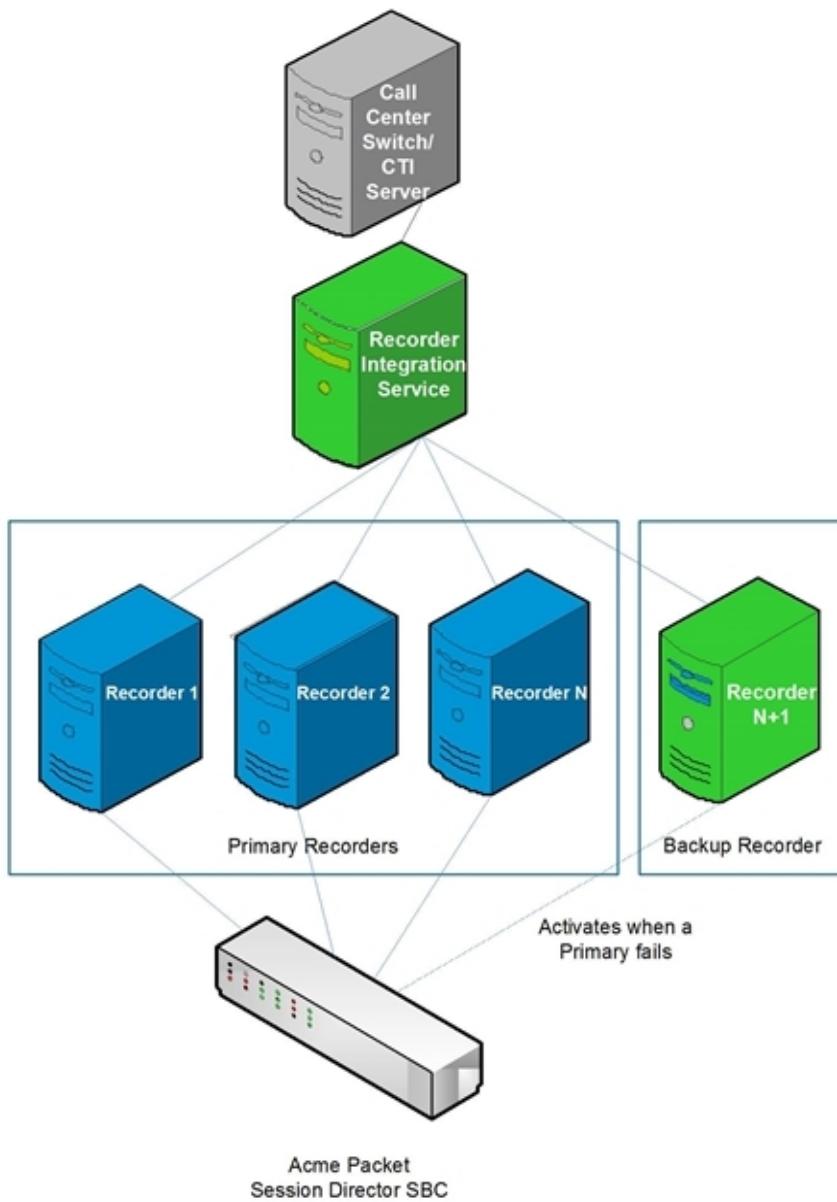
In TDM, in Performance/Liability fallback modes, channels are not stopped upon failover. If there is no redundant Recorder Integration Service and CTI is lost, the Recorder will go into fallback, and continue to record based on that. The Integration Service does not stop any recordings in progress. When CTI is restored, current recordings continue to completion in D-Channel/Vox mode, then the Integration Service picks up control again on the next call.

In Application mode, the Recorder stops recording if the Recorder Integration Service disconnects.

N+1 redundancy with SIP trunk recording

N+1 refers to an IP Recording environment that is capable of surviving one Recorder failure. If a Recorder fails, the edge device automatically forwards the audio away from the failed Recorder to the backup Recorder.

SIP Trunk Recording supports an N+1 redundancy configuration, as illustrated in the following diagram.



Troubleshooting

Use the following topics to troubleshoot issue that may occur when configuring high availability for the Recorder.

- [Gateway recording \(page 366\)](#)
- [Recording and RTM loss in Recorder Integration Service failover \(page 366\)](#)

Related topics

[Configure high availability \(page 334\)](#)

Gateway recording

For implementations involving Collection data sources, please note that when any child data source loses its CTI link, its parent gateway pool goes into fallback, which affects all child data sources in the same pool.

Related topics

[Troubleshooting \(page 366\)](#)

Recording and RTM loss in Recorder Integration Service failover

In N+M All Shared and N+N environments, if the main Integration Service is restarted, causing failover to the backup, Real-time Monitoring (RTM) will not continue to monitor the call being recorded. This situation will also occur whether or not control is subsequently returned to the main Integration Service.

If a Recorder fails there may be a loss of recording for calls in progress, and the active RTM session will lose audio. Recording will resume on the next new call for the device.

Resolution

In general, when any type of fault happens and failover occurs, exit RTM and re-enter it to restart monitoring.

Related topics

[Troubleshooting \(page 366\)](#)

Scaling for SIP and SIPREC traffic with RAPS

How to use RAPS nodes to improve scalability in SIP Proxy and SIPREC environments is explained.

Topics

Scaling solution for SIP and SIPREC environments	368
Site architecture	369
Security	370
Message flows with RAPS	371
RAPS configuration	373
Resilience and Redundancy	376

Scaling solution for SIP and SIPREC environments

In previous releases, SIP Proxy and SIPREC adapters on Recorder Integration Service (RIS) nodes handled SIP/SIPREC traffic. The co-location of these adapters on the RIS nodes presented scaling challenges, since each node could only handle a certain amount of traffic, and the number of nodes was bound into the 1+1 RIS redundancy.

To improve scalability, this release introduces a new role: the Recorder Adapter Proxy Service (RAPS). By deploying multiple RAPS nodes on servers that are separate from the RIS, customers can achieve horizontal scaling of the SIP/SIPREC interfaces.

RAPS nodes work in concert with the RIS and IP Recorders within a recording site to offload the SIP/SIPREC handling from the RIS roles. You can deploy multiple RAPS nodes to handle the necessary traffic loading from the recording environment. RAPS nodes support:

- Both full-time and selective recording on the SIP/SIPREC interfaces.
- Both N+M recorder resiliency and N+N dual recording redundancy models.

When should I deploy RAPS nodes?

Deploy RAPS nodes to remove constraints on the number of concurrent calls to a single node. By deploying multiple nodes as-needed, you can provide scale with your system.

Small sites with only a Recorder or two may not be of a sufficient size to enjoy the scaling benefits that a deployment with RAPS nodes provides. However, any deployment that may see traffic approaching capacity limits for concurrent calls on a single node should consider an architecture that includes RAPS.

Known limitations

Inside a single data source, there cannot be both a member group configured to use RAPS for SIP recording and another member group that is configured to not use RAPS. If you need this configuration to support your environment, use the legacy solution.

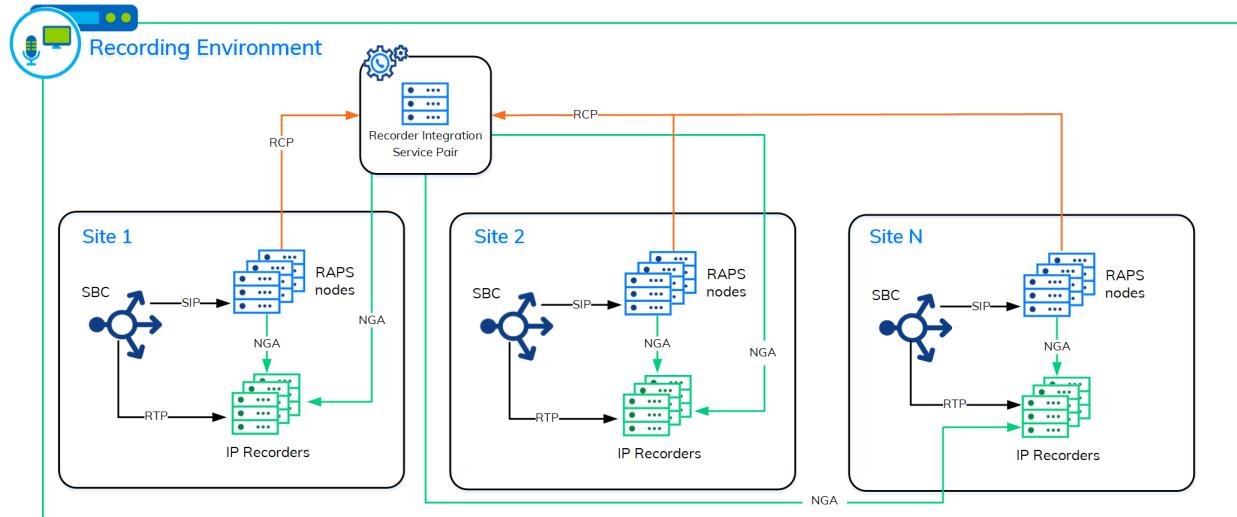
Related information

Performance and Sizing Guidelines

Site architecture

Within a SIP/SIPREC environment, enable RAPS nodes on separate servers from the RIS nodes. RAPS nodes can either be stand-alone servers or co-located with other capture services.

The following diagram shows a recording environment with multiple sites. A single RIS pair controls the environment. Each site has a separate third-party SIP device delivering the SIP/SIPREC to the RAPS nodes. The RAPS nodes direct the RTP traffic into the local pool of IP Recorders.



NGA and RCP are internal command and control protocols.

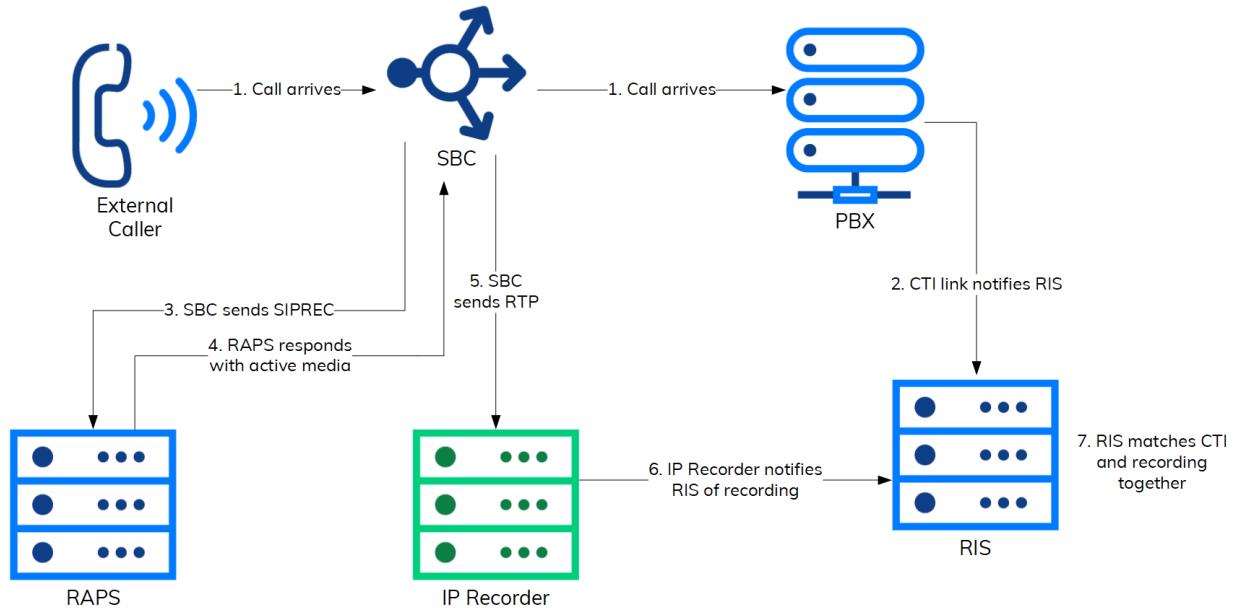
Security

RAPS nodes support standard TLS encryption over the SIP and SIPREC interfaces. IP Recorders support encrypted media using secure RTP (sRTP).

Message flows with RAPS

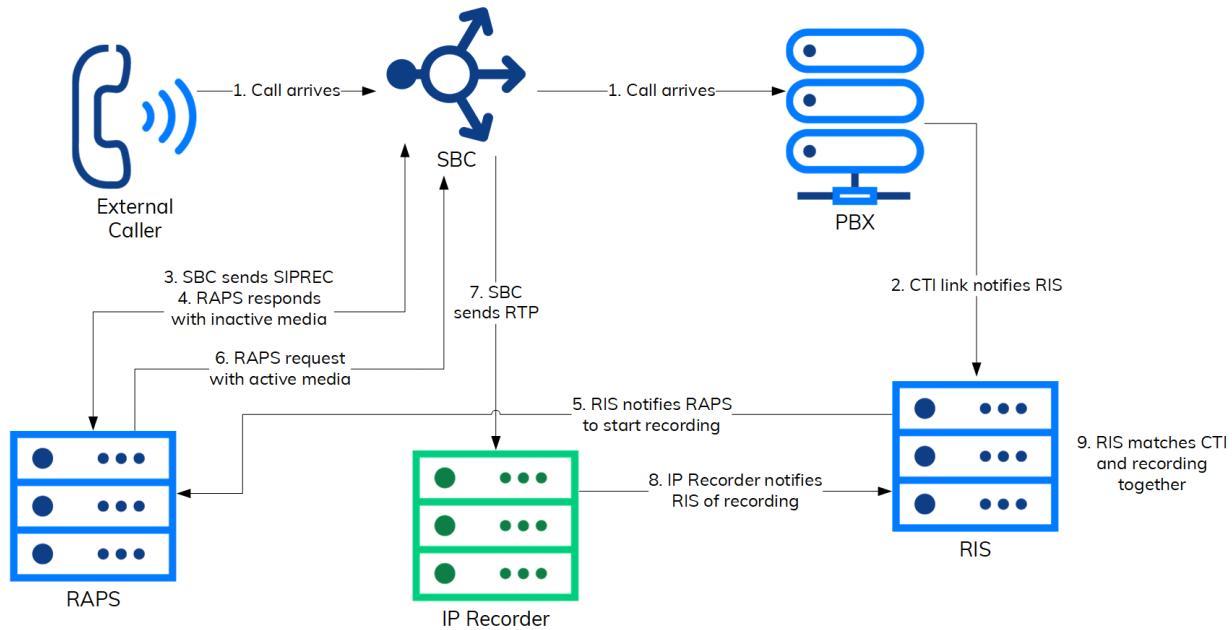
The RAPS nodes offload the SIP/SIPREC handling from the RIS. RAPS nodes are responsible for the SIP communication and negotiation, IP Recorder selection, and target media handling for call recording.

Full-Time recording flow



1. Call arrives to the switch.
2. CTI feed notifies RIS of the call.
3. Session Border Controller (SBC) sends SIPREC call to RAPS node.
4. RAPS selects a target IP Recorder and responds SBC with media target information.
5. SBC delivers RTP to the target IP Recorder.
6. IP Recorder notifies RIS about the recording.
7. RIS matches the recording with CTI context.

Selective recording flow



1. Call arrives to switch.
2. CTI feed notifies RIS of call.
3. SBC sends SIPREC call to RAPS node.
4. RAPS responds with inactive media and no RTP flows.
5. RIS notifies RAPS to start recording.
6. RAPS selects a target IP Recorder and re-INVITEs back into the call to activate the media.
7. SBC accepts the media activation and delivers RTP to the target IP Recorder.
8. IP Recorder notifies RIS about the recording.
9. RIS matches the recording with CTI context.

RAPS configuration

To configure a deployment using Recorder Adapter Proxy Service (RAPS) nodes to handle SIP/SIPREC traffic, configure full-time or selective recording as described earlier in this guide, whether without redundancy or using an N+N or N+M model. Use the following sections as guidelines throughout the configuration.

Enable RAPS roles

In Enterprise Manager, enable RAPS roles on a Recorder server. A given RAPS role can either be stand-alone or paired.

- For N+M recorder redundancy, use a stand-alone role.
- For N+N recorder redundancy, use a paired role.



Do not assign the RAPS role to the same server as the RIS role, as this negates the purpose of using RAPS to offload traffic from the SIP adapter that would traditionally be handled on the RIS server.



When RAPS and Recorders are "shared", it means that they are shared across the Recorder Integration Service. The only exception to this is N+N scenarios. In N+N the main RIS only speaks to the main RAPS and main Recorder. Likewise, the backup RIS only speaks to the backup RAPS and backup Recorder.

Procedure

1. Enable the RAPS on a target server.
 - a. Under **System Management**, locate the node you want to use as the RAPS server.
 - b. Click **Server Roles**.
 - c. Enable the **Recorder Adapter Proxy Service** role.
 - d. Click **Save**.
2. For N+N scenarios *only*, enable RAPS on another node and pair the roles.
 - a. Repeat step one, a through d, for a second node.
 - b. Select the first **Recorder Adapter Proxy Service** node that you enabled in step one.
 - c. Click **Secondary Role**.
 - d. Locate and select the secondary **Recorder Adapter Proxy Service** node/role.
 - e. Click **Save**.

Related topics

[Set up Recorder roles and associations \(page 44\)](#)

[Recorder redundancy \(page 338\)](#)

Configure Data Sources and Member Groups

You can assign a RAPS role to multiple Data Sources. However, all of the Data Sources must be assigned to one RIS or to the same RIS pair. A RAPS node cannot be shared across multiple RIS pairs.

Assign RAPS nodes to a Data Source through a Member Group. For SIP/SIPREC recording, this is either a Gateway Correlation Member Group or an IP Extension Pool.

A RAPS node can only be assigned to one Member Group per Data Source, but a Member Group may have multiple RAPS nodes:

- You can only assign a given RAPS node to one Member Group per Data Source. With paired RAPS nodes, only the node with the Primary RAPS Role can be assigned to the Member Group. The system automatically assigns the Secondary node.
- You can assign multiple RAPS nodes to a single Member Group. Each RAPS node is automatically associated with all of the IP Recorder roles assigned to the same Member Group. The number of nodes needed within a Member Group depend on the system load and resiliency needs.

Capacity

Customers should create Member Groups to represent the recording capacity at specific Points-of-Presence (PoP). Recording capacity (RAPS nodes + IP Recorders) are deployed within the PoP to capture the localized traffic. A single Member Group configuration represents each PoP.

Co-location

Do not assign the RAPS role to the same server as the RIS role, as this negates the purpose of using RAPS to offload traffic from the SIP adapter that would traditionally be handled on the RIS server.

You may, however, have an IP Recorder on the same server as RAPS role. Limit the IP Recorders to one Member Group per Data Source. Assigning the same IP Recorder to multiple Member Groups within the same Data Source complicates the system.

Procedure

1. Under **Recording Management**, go to **Data Sources** and click **Settings**.
2. Select the Phone data source you're using for the Recorder, then click **Member Groups**.
3. Select the Gateway Side Correlation Member Group or IP Extension Pool, then click **Edit**.
 - a. Under **Shared Recorder Adapter Proxy Services**, select the RAPS role.
 - b. Click **Save**

Related topics

[Create a phone data source \(page 49\)](#)

[Create a member group \(page 66\)](#)

Configure adapters

Launch Recorder Manager from a RAPS node in Enterprise Manager, then create a SIP Proxy or Generic SIPREC adapter the same way you would for a RIS adapter.

Related information

Recorder Manager Online Help

Resilience and Redundancy

You can achieve recording resiliency by deploying multiple RAPS nodes and multiple IP Recorders. In the recording site, each Recorder Adapter Proxy Service (RAPS) node connects to all of the associated IP Recorders. RAPS acts as a load balancer by distributing Incoming calls among the connected IP Recorders to provide high availability, high performance, and efficient use of servers. Similarly, SIP traffic can be load-balanced across the RAPS nodes.

Verint SIP/SIPREC implementations support SIP OPTIONS requests to “ping” the trunk to determine health state and capabilities. When multiple RAPS nodes are available, it is recommended that the third-party SIP device use SIP OPTIONS messages to maintain connectivity states of the potential nodes.

For example, the customer SBC element generating the SIPREC load into the recording site could be configured to load balance the SIPREC traffic in a round-robin manner across three RAPS targets.



SIP traffic load balancing depends on the capabilities of the third-party SIP device. The manner and number of RAPS nodes should be coordinated to work with the resiliency options offered by the third-party device. To ensure resiliency, plan the size of your RAPS pool to handle the worst-case scenario. To do this, understand the size limits of each RAPS node and each third-party SIP device. Then over-provision the RAPS pool.

For example, a customer has a three-node, clustered SBC. Each node is capable of handling 4,000 SIPREC forks. The theoretical peak of the SBC is 12,000 SIPREC forks ((3 nodes x 4,000 forks)). In this case, the customer needs two RAPS nodes to handle the theoretical maximum traffic. To ensure resiliency, deploy at least one additional node, which results in a minimum pool size of three RAPS nodes.

Ideally, each SBC load balances across all of the RAPS nodes, but suppose each node could only be configured to connect to two (2) nodes. The customer should configure the SBC nodes such that they properly overlap across the RAPS pool. This could be as simple as configuring: SBC_Node_1 to connect to RAPS_1 and RAPS_2; SBC_Node_2 to connect to RAPS_2 and RAPS_3; SBC_Node_3 to connect to RAPS_3 and RAPS_1.



RAPS nodes support busy-out responses if the node is unable to record a new incoming SIP/SIPREC call. By default, the node responds with a 486-Busy Here response code. The third-party SIP device should retry the SIP/SIPREC call on a different RAPS node.

N+N Dual Forking

The RAPS roles support dual forking of the SIP/SIPREC feeds to enable N+N recording but require specific capabilities on the third-party SIP device. The RAPS nodes must be paired in a primary-secondary relationship for N+N recording. The third-party SIP device must send one fork of the SIP/SIPREC feed to a primary RAPS node of the pair. The third-party SIP device must also send one fork of the SIP/SIPREC feed to the accompanying secondary RAPS node of the pair.

If there is only one RAPS pair assigned to the third-party SIP device, the configuration is straightforward, as the third-party SIP device simply forks all traffic to both nodes continuously.

If there are multiple RAPS pairs assigned to the third-party SIP device, the configuration becomes complex, as the third-party SIP device becomes responsible for delivering both SIP/SIPREC calls to the

primary and secondary layers, respectively. The calls do not have to be delivered to the same sides of a RAPS pair. The SIP/SIPREC signaling will be load balanced within the RAPS layer, and the RTP traffic will be load balanced within the IP Recorder layer.

To accommodate the load balance and scaling associated with the solution, SIP/SIPREC dual forking requires the use of a post-call process to identify recording anomalies and promote recordings. This configuration supports both standard N+N recording and full duplicate recording. For example, 2N.

Procedure: To enable the feature flag

1. Go to http://<servername>/wfo/control/license_edit.
2. Sign in with administrator credentials.
3. Expand the Features item and select **2021R1 - 2N Redundancy by Database**.
4. Add an advanced setting on the Data Source of "2NRedundancyByDB" = "true".

Failure Modes

You can expect the following behavior when RAPS is part of your deployment and certain nodes go down.

IP Recorder maintenance

When the IP Recorder is placed into maintenance, one or more associated RAPS nodes will begin redirecting any ongoing SIP/SIPREC calls that are targeting that IP Recorder to other IP Recorder within the site. No media loss will occur.

New calls are directed toward the running IP Recorders and not toward the IP Recorder placed in maintenance.

IP Recorder failure

The RAPS node maintains a persistent connection with each IP Recorder within the site. When this connection drops, the RAPS will redirect any on-going SIP/SIPREC call that was targeting that IP Recorder to other IP Recorders within the site. Media loss is minimized.

New calls are directed toward the remaining IP Recorders.

If there is insufficient recording capacity within the site to handle the call volume, call loss will occur.

RAPS node failure

If a RAPS node fails or the SIP/SIPREC adapter is restarted, all ongoing SIP call states and dialogs are lost. This means that any future SIP transactions on the calls are rejected by the RAPS node.



The third-party SIP device could re-establish the ongoing SIP calls upon detection that the trunk is down. See the resiliency capabilities of the third-party device for more information.

The IP Recorders continue to record the on-going calls until the third-party SIP endpoint stops sending RTP. Full-time recording environments activate the media on each call, so media loss is minimized in this failure mode. Selective recording environments activate and deactivate the media based on the CTI flow, so media loss can occur if the call was not activated prior to the failure.

N+N environments involve dual forking of every call, so media loss does not occur.

RIS failure

If a RAPS node disconnects from an RIS node, there is no immediate impact to any of the ongoing SIP/SIPREC recordings.

Full-time recording environments will continue to record ongoing and future SIP/SIPREC calls. Selective recording environments will perform a cleanup of the selective ongoing SIP/SIPREC calls started by the RIS, once RIS disconnection is detected. Future calls will not be recorded until the link back to the RIS is established. Once the RAPS has established communication with the RIS, the RIS can command the RAPS node to record the targeted SIP/SIPREC calls.

Advanced configuration

This section covers the following aspects of configuration, which may not apply to all deployments.

Topics

Configure pause recording on hold	380
Configure RTP detection	381
Record terminal sessions	382
System Tools	385
Configure the Interaction Capture Control API (eQuality Connect V6) Adapter	386
Device aliasing	391
Registration and device failures	392
Configure Recorder generated comfort noise	393

Configure pause recording on hold

You can stop the caller's side of a call from being recorded during a hold by enabling the Pause Recording On Hold feature. When a hold event is received from an employee, recording is masked until the employee returns to the call.

Procedure

1. In Enterprise Manager, click **Recording Management > Data Sources**.
2. Select a phone data source.
3. Click Advanced Settings, then click **Add**.
4. Enter **PauseRecordingOnHold** in the **Key** field and **True** in the Value field.
5. Click **Save**.

See the *Call Flow Guide* for details about the recordings that will result from different scenarios when this feature is enabled.

Related topics

[Configure RTP detection \(page 381\)](#)

[Record terminal sessions \(page 382\)](#)

[Configure the Interaction Capture Control API \(eQuality Connect V6\) Adapter \(page 386\)](#)

[Device aliasing \(page 391\)](#)

[Registration and device failures \(page 392\)](#)

Configure RTP detection

Use the following procedure to configure RTP detection (in addition to completing [Configure recording \(page 42\)](#)). See [RTP detection \(page 454\)](#) for more information about RTP.



RTP Detection is always enabled in Performance and Liability fallback modes.

Before you begin: Limitation on RTP detection

RTP detection is not supported when the RTP payload type is in the dynamic payload range of 96–127 (such as video) and for any encrypted media streams (such as Lync). Therefore, RTP detection is not supported for video recording and Lync recording.

Procedure

1. In Recorder Manager, click **General Setup > Capture Settings > IP Recording**.
2. Under **RTP Detection**, set **Detect RTP** to **Always**, **System Default**, or **Never**.



RTP detection works together with recorder call control protocols and CTI. The Recorder Fallback Type set in the member groups associated with the IP Recorder in Enterprise Manager will influence the implementation of RTP.

If the Recorder Fallback Type is Performance or Liability, the system automatically sets its internal value for RTP Detection to “Always”, regardless of the setting selected in Recorder Manager. Only when the Recorder Fallback Type is Application will the Recorder Manager RTP setting take precedence. See [Configure IP recording settings \(page 249\)](#) and [RTP detection \(page 454\)](#) for more information.

3. Click **Save**.

Related topics

- [Configure pause recording on hold \(page 380\)](#)
- [Record terminal sessions \(page 382\)](#)
- [Configure the Interaction Capture Control API \(eQuality Connect V6\) Adapter \(page 386\)](#)
- [Device aliasing \(page 391\)](#)
- [Registration and device failures \(page 392\)](#)

Record terminal sessions

Recording sessions from Terminal Servers, including Citrix Servers, allows you to capture screen activity on a remote terminal accessed using the remote desktop protocol (RDP) or Citrix ICA session. The difference between recording Workstations and Terminal Servers is that Terminal Servers must be associated with a unique Workstation Group. Thereafter, you assign phones and employee login IDs, as normal, according to seating arrangement.



Only Anonymous Terminal Session Screen Capture is supported. In other words, you must use Employees' Terminal Server Windows Logon IDs to configure the Terminal Services Screen Capture.

Related topics

[Configure pause recording on hold \(page 380\)](#)

[Configure RTP detection \(page 381\)](#)

[Configure the Interaction Capture Control API \(eQuality Connect V6\) Adapter \(page 386\)](#)

[Device aliasing \(page 391\)](#)

[Registration and device failures \(page 392\)](#)

To record terminal sessions

1. In Enterprise Manager, click **Recording Management > Data Sources**, and then create a LAN (Screen) data source and assign the data source to an Integration Service server.
2. Create a Workstation Group and associate it with a recorder, as described in [Create workstation groups \(page 110\)](#).
3. Create a Workstation, using Windows OS/2 or Windows Terminal Server as the platform, as described in [Define workstations \(page 112\)](#). Repeat this step for each Terminal Server to be configured. The Terminal Server name may be either a subnet or a workstation name. Assign it to the Workstation Group created in the previous step.



Do not assign this Workstation to an Employee (on the People page) or to an Extension.

4. Click **Employee**, and then assign the Terminal Server Employee Windows logon ID to the Employee. Repeat this for each Employee.
5. Configure Phone data source(s) and member group(s) as required.
6. Do one of the following:
 - Assign an **Extension** to the employee, if the phone seating arrangement is **Fixed**.
 - Assign a **Phone Logon ID** to a person, if the phone seating arrangement is **Free**.
 - Assign an **Extension** or **Phone Logon ID** to the employee, if the phone seating arrangement is **Hybrid**.For more information on seating arrangements, refer to [Create an employee \(page 143\)](#).
7. Create a recording rule to record screens. For more information on creating recording rules, refer to [Set up recording rules \(page 303\)](#).

Screens on the Terminal Server are now recorded according to the screen capture settings defined in the Workstation Group.

The above steps describe one way of configuring Terminal Server Screen Capture. There are other variations. For example, multiple Workstation Groups can be created and each Terminal Server can be assigned to a different Workstation Group.

Related topics

[Record terminal sessions \(page 382\)](#)

[Limitations \(screen capture of multiple sessions and Published Applications\) \(page 383\)](#)

Limitations (screen capture of multiple sessions and Published Applications)

There are some limitations surrounding screen capture of multiple sessions and Published Applications in Windows Terminal Services and Citrix environments.

Citrix Published Applications Screen Capture Limitations

In capturing screens for Published Applications, the Recorder records only one Citrix Session at a time per Employee.

The capture depends on the type of Citrix session. If the Citrix Session is:

- A Published Server Desktop session, then it will record all the activities in that Desktop Session.
- An individual Published Application session, then it will record only that particular Published Application. Configure explorer.exe as the Published Application to open a Windows folder containing Application shortcuts. Applications launched using shortcuts will run in the explorer.exe session.
- A session that is shared between Published Applications, then it will record all the Published Applications in that session. Published Applications with common properties (color depth, resolution, encryption, and so on) can be configured to share the same session within Citrix.

Refer to Citrix support for session sharing details.

The limitations for the capture are as follows:

- If the Employee opens Multiple Published Applications from different Citrix Servers in a Farm then Recording of only one session will occur.
- If the Employee opens Multiple Published Applications (not by session sharing) from a single Citrix Server, then Recording of only one session will occur.
- The session that will be recorded is the session most recently created. For example, if the Employee first opens Email as a published application on one server and then CRM as an application on a different server, the CRM application session will be recorded and associated with his next call. If he opens CRM first and Email second, then email will be recorded.

To record all Published Applications in circumstances where it may not be possible to determine which screen should be recorded:

- Restrict each Employee to work on a single Citrix Server in a Citrix Server Farm at a particular time.
- Record all Applications an Employee uses:
 - Configure Published Applications to share the Same Session.
 - Publish the Server Desktop and allow Employees to access all the Applications through the Desktop session.
 - Configure explorer.exe as the Published Application giving one of the folder names as the argument. Create file shortcuts to applications in that folder using the Windows Explorer. When the explorer.exe is launched on the client PC, it opens the file explorer with shortcuts. These shortcuts can be used to launch applications. Only one session will be created on Citrix Server when explorer.exe program is launched. All applications launched using shortcuts will run in the same explorer.exe session.

Windows Terminal Services (without Citrix) Screen Capture Limitations

In capturing screens under Windows Terminal Services, the Recorder records only one Windows Terminal Session at a time per Employee. It records all the activities in that Terminal Session.

The limitations of the capture are as follows:

- If the Employee opens Multiple Terminal Sessions from different Windows Terminal Servers then Recording of only one session will occur.
- If the Employee opens Multiple Terminal Sessions from single Windows Terminal Server then Recording of only one session will occur.
- The session that will be recorded is the session most recently created. For example, if the employee first opens Terminal Services session (session ID 1), then this session will be recorded when a call comes in. If the same employee opens another Terminal Services session (session ID 2), Session ID 2 will be recorded and associated with its next call.

To record all Published Applications in circumstances where it may not be possible to determine which screen should be recorded, restrict each Employee to working on a single Windows Terminal Server and to the single Terminal Session. Allow the Employee to access all the Applications through the Terminal Session.

Related topics

[Record terminal sessions \(page 382\)](#)

System Tools

System Tools houses stand-alone utilities.

For the Recorder, these include:

- Archiver Utility
- Archive DVD Validator

When you install the Recorder, System Tools is installed automatically to the following location on each server. The tools available on a given server are determined by that server's role. (For example, when the Centralized Archive role is enabled, the System Tools application will include the Archiver Utility and the DVD Validator.)

Launch System Tools

Use the following procedure to launch tools from System Tools.

Procedure

1. Double-click the System Tools shortcut on your desktop (or right-click the System Tools icon in your Windows tool tray).
2. Select the **Configuration** or **General** tabs to see available applications. Click the **Run** tab to access system tools-related activities that can be run with command line parameters. Double-click any application name to start that application.

Configure the Interaction Capture Control API (eQuality Connect V6) Adapter

Use the Interaction Capture Control API (eQuality Connect) Adapter to integrate Verint's Customer Feedback, Agent Initiated Monitoring (AIM), and Desktop Process Analytics (DPA) modules, and for integrating with third-party systems to ingest their email, web chat, and post-call audio and video customer engagements. This adapter was formerly named Recorder Integrations API Adapter.



Before you start configuring the Interaction Capture Control Adapter, refresh the configuration fields.

Procedure

1. In Recorder Manager, go to **General Setup**. Under **Integration Adapters**, click **Settings**.
2. Click **Create**, then click **Interaction Capture Control API (eQuality Connect V6) Adapter**.

3. Under **Settings**, configure the following:

Adapter Name	Adapter Name: Required. A unique name for this adapter. Do not use the following characters, which are reserved for XML tagging: < > \$ & ' ".
Description	Description: Optional. Enter a description for this adapter.
Adapter Type	Adapter Type: A read-only field that describes the selected adapter.
Startup Type	Startup Type: How the adapter behaves after the host server restarts. The options are: <ul style="list-style-type: none"> • Automatic: Default. The adapter starts automatically when the host server starts. • Manual. The adapter starts only when a user clicks the Start button. • Disabled. The adapter does not run when the host server starts.
DataSource	Select the data source for the custom external system or for the switch used for Quality Monitoring.
Listen Port	Specify the port number on which the eQCAdapter listens for connections. The default is 3020.
Disable Session Management Interface	<ul style="list-style-type: none"> • Select this option for the adapter to tag data while the switch controls recording. <ul style="list-style-type: none"> ■ What works: Data tagging, agent logon and logout, and recording control (pause/resume, start/stop). ■ What doesn't work: Call control, such as connected, disconnected, hold, and retrieved. • Clear this option when: <ul style="list-style-type: none"> ■ The data source needs call control. ■ Using Desktop and Process Analytics (DPA) to perform screen-only recording. ■ The data source is LAN, which captures <i>agent screen activity</i> (screen recording).
Enforce Authorization Token	Configures how the adapter responds to incoming requests that exclude an SWT authorization header. <ul style="list-style-type: none"> • Clear this option to disable it. When disabled (default), the adapter accepts requests without the authorization header, which makes the system backward compatible with older clients that do not support the authorization token. • Select this option to enable it. When enabled, the adapter rejects requests that do not include SWT authorization, and logs a 401-Unauthorized response.

Response timeout (milliseconds)	The amount of time the adapter waits for the internal service to process an API request before timing out and providing the external client with an error. Increasing the timeout can help a system that is experiencing latency or lagging to still provide meaningful response codes to API requests. By default, the timeout is 1000 milliseconds.
---------------------------------	--

4. Under **Cross Origin Responses**, configure the following:

Cross Origin Response URL	Controls how the adapter inserts the Cross Origin Resource Sharing (CORS) Access-Control-Allow-Origin header into the responses for incoming API requests. The adapter does not have any cross site capabilities, but these headers are still useful for verifying the security of the HTTP interface. Select one of the following response types as the Cross Origin Response URL setting: <ul style="list-style-type: none"> • Generic (*) - The adapter inserts an asterisk (*) for the header, indicating that any origin is acceptable. This is the default behavior. • Mirror Origin Header - The adapter echoes back the "Origin" header information from the incoming request. • Specific URL - Allows the customer to define the response string to suit their needs. If you select this option, enter the URL in the Cross Origin Response Specific URL field.
---------------------------	--

5. Under **Private Network Access**, configure the following:

Private Network Access URL	Select how the adapter responds to the Private-Network-Access header, if present. Customers may disable this option, or set a specific URL to suit their needs. System default: Allows connections to the Verint network from any location regardless of the origin. Private network access disabled: Only allows connections from within the private network. Users or devices outside the network cannot access internal resources. Private network access enabled for specific URL: Allows connections from the URL specified. This setting enhances security by ensuring that only trusted URLs can connect to the private network.
Private Network Access Specific URL	Only available when Private network access enabled for specific URL is selected. Enter the URL of the trusted site.

6. Under **Security Settings**, configure the following:

Security Settings	<p>To secure data in transit to and from the adapter, choose an HTTPS option, so only URLs starting with https:// can access the Connect Server.</p> <p>Both HTTPS with built-in keys and HTTPS with below keys cause the eQuality Connect server to run using HTTPS, so all URLs must use https:// to access the server.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • No Security (HTTP)—Use HTTP to access the server. Traffic is unencrypted. This is the default setting. • HTTPS with built-in keys—Only use for testing, do not use in a production environment. This setting uses the built-in certificates on the server. It provides encryption, but not authentication. • HTTPS with System Certificates—Supports encryption. The adapter reuses the TLS server certificates in %IMPACT360SOFTWAREDIR%\conf\security. The adapter automatically gets any updates to these certificates. • HTTPS with below keys—Provides encryption and authentication, and is required for Customer Feedback integrations. After selecting this option, complete the Keystore Filename, Keystore Password, and Keystore Format fields below using the information for your own certificates (whether from a third-party or your own certificate server). <p>⚠️ For Customer Feedback integrations, choose HTTPS with below keys. This option supports encryption and authentication.</p> <p>Do <i>not</i> choose HTTPS with built-in keys because it does not support authentication. If Customer Feedback cannot authenticate the connection, it uses the default agent for all surveys.</p>
Keystore Filename	If you selected HTTPS with below keys as the Security Setting, enter the file name of the Keystore.
Keystore Password	If you selected HTTPS with below keys as the Security Setting, enter the password for the selected keystore.
Keystore Format	<p>If you selected HTTPS with below keys as the Security Setting, select the format of the selected keystore file. Available options are JKS (default) and PKCS.</p> <p>The adapter supports a public or private keystore in the Java Key Store (JKS) or Public-Key Cryptography Standard (PKCS) 12 formats.</p>

Security Profile	If you selected HTTPS with below keys as the Security Setting, choose one of the following: <ul style="list-style-type: none">• Server Site: Uses the same setting as the local server, which is configured in the "HTTPS Protocol and Cipher Configuration" field on the Security page.• Intermediate: Uses the older security protocols and ciphers. Best for backward compatibility.• Modern: Uses the latest security protocols and ciphers. Best for security.
------------------	---

7. Under **Advanced Settings**, enter the **Key** and **Value** fields any proprietary pairs that are required by your system—this should be done only in consultation with Field Engineers.
8. Click **Save**.

You may also need to configure attributes—see [Configure adapter custom attributes \(page 326\)](#) for instructions.

Related topics

[Configure pause recording on hold \(page 380\)](#)

[Configure RTP detection \(page 381\)](#)

[Record terminal sessions \(page 382\)](#)

[Device aliasing \(page 391\)](#)

[Registration and device failures \(page 392\)](#)

Device aliasing

You can make a phone's primary extension (either the extension configured in the Enterprise Manager or, in the case of Cisco or Nortel integrations, that reported in the device registration) be the extension of a session, by enabling the **Always Report Extension as Primary Extension** check box in the phone data source (see [Create a phone data source \(page 49\)](#)).

If not enabled, by default the extension of the session will be recorded in the database as the extension on which the session started.

If this feature is enabled, the extension value will be the primary extension of the phone. The primary extension is either what is configured in Enterprise Manager or what Cisco/Avaya NES report on the device registrations.



This setting only affects multi-line phones.

Related topics

[Configure pause recording on hold \(page 380\)](#)

[Configure RTP detection \(page 381\)](#)

[Record terminal sessions \(page 382\)](#)

[Configure the Interaction Capture Control API \(eQuality Connect V6\) Adapter \(page 386\)](#)

[Registration and device failures \(page 392\)](#)

Registration and device failures



The following applies only to Nortel Symposium, Alcatel TSAPI, Avaya TSAPI, Genesys, Aspect, and CTConnect integrations.

If you configure invalid extensions (or an extension that the T-Server is not yet aware of) the integrations will periodically attempt to re-register the DNs.

If a device fails to register, an alarm will appear in the Recorder Manager in the Integration Service section. You can also query failed devices in Recorder Manager.

Related topics

[Configure pause recording on hold \(page 380\)](#)

[Configure RTP detection \(page 381\)](#)

[Record terminal sessions \(page 382\)](#)

[Configure the Interaction Capture Control API \(eQuality Connect V6\) Adapter \(page 386\)](#)

[Device aliasing \(page 391\)](#)

Configure Recorder generated comfort noise

The comfort noise feature only applies to SIP Delivery environments and is intended for use with SIP endpoints that use RTP stream(s) as a heartbeat for the SIP call. We recommend customers use send-only media streams with the recording system and SIP session timers per RFC 4028 to maintain the recorded SIP calls. For environments that do not support the SIP timers, the generated comfort noise packets may serve as an alternative keep alive method by establishing a send-receive stream with the recording system.

Standards

The comfort noise generated is per RFC 3389.

Notes

- Fixed payload ID: 13
- Fixed clock rate: 8KHz
- Fixed payload size: 1 byte (Only Energy level is sent. Spectrum envelope is not sent.)
- Comfort noise packets are delivered back to the SIP endpoint using symmetric RTP (sending and receiving of RTP from the same port) according to RFC 4961.
- Encrypting comfort noise packets is not supported.

Procedure

1. In Recorder Manager, click **General Setup**.
2. Under **Integration Service**, click **Settings**.
3. Click **Create**, then select the appropriate adapter.
4. Under **Recorder Generated Comfort Noise**, complete the following fields:

Field	Description
Generate Packets	When selected, the Recorder generates comfort noise packets that are sent to the SIP end point. The default is disabled.
Packet Interval (seconds)	The rate, in seconds, in which RTP packets are sent by the IP Recorder. The default is 20 seconds. The Packet Interval is configurable from 1 to 60 seconds.

Related information

<https://tools.ietf.org/html/rfc3389>

<https://tools.ietf.org/html/rfc4028>

<https://tools.ietf.org/html/rfc4961>

Configure SIP Interception

This chapter describes how to configure SIP Interception recording.

Topics

Overview	395
Configure the Recorder	396
Custom SIP tagging	398
Change the default SIP signaling port number	399
Add additional SIP signaling port numbers	401

Overview

The following sections focus exclusively on the configuration aspect of SIP Interception recording. For general information about VoIP Interception, including requirements and site preparation, see the *Recorder VoIP Interception Deployment Reference Guide*.

Configure the Recorder

To configure the Recorder for SIP Interception you must do the following.

- [Configure Recorder Manager \(page 396\)](#)
- [Configure Enterprise Manager \(page 396\)](#)
- [Configure SIP Proxy Addresses \(page 396\)](#)

Configure Recorder Manager

1. In Recorder Manager, click **General Setup > Capture Settings > Cards and Filters**.
2. Set the Network Interface Card (NIC) **Recording Type** to **Interception**.
3. Click the **Protocols** tab, and then select **SIP**.
4. Click **Save**.
5. Restart the Recorder IP CaptureEngine service (under **Operations > Start/Stop**).

Configure Enterprise Manager

1. Set the **Default Recording Mode** of the IP Recorder to **Do Not Record** as described in [Set a default recording mode \(page 129\)](#).
2. Create a Phone data source as described in [Create a phone data source \(page 49\)](#).

Configure SIP Proxy Addresses

1. Navigate to the <install software dir>\ContactStore folder within the installation directory.
2. Open the **IPCaptureConfig.xml** file in a text editor such as Notepad.
3. Locate the following section:
`<x:SIP>`
4. Within the `<x:SIP>` tags, locate `<x:ProxyIPAddresses>` and add the **ProxyIPAddress** between `<x:ProxyIPAddress>` tags, one address per set of tags.

Example:

```
<x:ProxyIPAddresses>
    <x:ProxyIPAddress>100.10.10.10</x:ProxyIPAddress>
    <x:ProxyIPAddress>100.10.10.11</x:ProxyIPAddress>
</x:ProxyIPAddresses>
</x:ProxyIPAddresses>
```

5. Save and close the file.
6. Use the following command to run the checksum utility on the **IPCaptureConfig.xml** file. This will add a new checksum with the modifications. (Failure to do this will result in a 'file tampered' alarm.)
`%IMPACT360SOFTWAREDIR%\ContactStore\Tools\ChecksumUtil.exe -g %IMPACT360SOFTWAREDIR%\ContactStore\IPCaptureConfig.xml`
7. Restart the Recorder IP CaptureEngine service (under **Operations > Start/Stop**).



For IP Analyzer, complete the steps above, but within the **IPAnalyzerConfig.xml** file. Run
%IMPACT360SOFTWAREDIR%\ContactStore\Tools\ChecksumUtil.exe -g
%IMPACT360SOFTWAREDIR%\ContactStore\IPAnalyzerConfig.xml, then
restart the Recorder Analyzer Service.

Extract Extension from INVITE URI or CONTACT Header

In environments where incoming calls contain an extension in the **INVITE URI** rather than in the **To** header, and outgoing calls contain an extension in the **Contact** header rather than in the **From** header, you must complete the following procedure in order to extract the extension from the InviteURI/Contact header.

1. Navigate to the <install software dir>\ContactStore folder within the installation directory.
2. Open the **IPCaptureConfig.xml** file in a text editor such as Notepad.
3. Set the **UseInviteURI** to **true**. For example:
`<x:UseInviteURI>true</x:UseInviteURI>`
4. Save and close the file.
5. Use the following command to run the checksum utility on the IPCaptureConfig.xml file. This will add a new checksum with the modifications. (Failure to do this will result in a 'file tampered' alarm.)
%IMPACT360SOFTWAREDIR%\ContactStore\Tools\ChecksumUtil.exe -g
%IMPACT360SOFTWAREDIR%\ContactStore\IPCaptureConfig.xml
6. Restart the Recorder IP CaptureEngine service (under **Operations > Start/Stop**).



For IP Analyzer, complete the steps above, but within the **IPAnalyzerConfig.xml** file. Run
%IMPACT360SOFTWAREDIR%\ContactStore\Tools\ChecksumUtil.exe -g
%IMPACT360SOFTWAREDIR%\ContactStore\IPAnalyzerConfig.xml, then
restart the Recorder Analyzer Service.

Custom SIP tagging

To tag custom data in a SIP Interception recording environment, do the following:

- Configure the IP Recorder to include custom SIP Header, SDP Media and SIP Header Parameter tags.
- Create custom data fields and attributes for these tags.

Configure the IP Recorder

1. Navigate to the <install software dir>\ContactStore folder within the installation directory.
2. Open the **IPCaptureConfig.xml** file in a text editor such as Notepad.
3. Locate the section **<CustomSIPTag>** and add any required values between the **<x:CustomSIPTag>** and **</x:CustomSIPTag>** tags.

Example: To tag the SIP header, you would specify the following.

```
<x:CustomSIPTags>
  <x:CustomSIPTag Section="SIP Header Parameter"
    Overwrite="true"/>/x:CustomSIPTag>
</x:CustomSIPTags>
```

The Section attribute is case-sensitive, and if it is not present the default value "SIP Header" will be used.

4. Save and close the file.
5. Use the following command to run the checksum utility on the IPCaptureConfig.xml file. This will add a new checksum with the modifications. (Failure to do this will result in a 'file tampered' alarm.)
%IMPACT360SOFTWAREDIR%\ContactStore\Tools\ChecksumUtil.exe -g
%IMPACT360SOFTWAREDIR%\ContactStore\IPCaptureConfig.xml
6. Restart the Recorder IP CaptureEngine service (under **Operations > Start/Stop**).



For IP Analyzer, complete the steps above, but within the **IPAnalyzerConfig.xml** file. Run %IMPACT360SOFTWAREDIR%\ContactStore\Tools\ChecksumUtil.exe -g %IMPACT360SOFTWAREDIR%\ContactStore\IPAnalyzerConfig.xml, then restart the Recorder Analyzer Service.

Create custom data fields and attributes

Once you have specified custom tags in the xml file as described above, add them to Enterprise Manager as attributes, then map them to custom data, using the procedures [Create, edit or delete an attribute \(page 278\)](#), [Create Custom Data fields \(page 291\)](#), and [Map Custom Data to an attribute \(page 292\)](#). This will allow you to use them to tag call recordings.

Change the default SIP signaling port number

By default, the system uses port 5060 for SIP signaling in a SIP interception recording environment. If signaling occurs on a different port, update the system configuration to listen for SIP signaling on that port number. To make the update, change the **IPCaptureProtocolConfig.xml** configuration file.

Procedure

1. Navigate to the following folder in the installation directory:
%IMPACT360SOFTWAREDIR%\ContactStore
2. Use a text editor, such as Notepad, to open the following configuration file:
IPCaptureProtocolConfig.xml
3. Locate the following section:
<x:name>SIP</x:name>
4. Add the following inside the SIP tags, where *<SIP Port>* is replaced with the port number to use for SIP signaling.

```
<x:defaultstreamconfig>
    <x:priority>354</x:priority>
    <x:defaultstream>UDP 0.0.0.0:0 0.0.0.0:<SIP Port>
        UDP/SIP</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority>355</x:priority>
    <x:defaultstream>UDP 0.0.0.0:<SIP Port> 0.0.0.0:0
        UDP/SIP</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority>356</x:priority>
    <x:defaultstream>TCP 0.0.0.0:0 0.0.0.0:<SIP Port>
        SIPDetector</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority>357</x:priority>
    <x:defaultstream>TCP 0.0.0.0:<SIP Port> 0.0.0.0:0
        SIPDetector</x:defaultstream>
</x:defaultstreamconfig>
```

Example: To use port 5061 instead of the default port, add the following:

```
<x:defaultstreamconfig>
    <x:priority>354</x:priority>
    <x:defaultstream>UDP 0.0.0.0:0 0.0.0.0:5061 UDP/SIP</x:defaultstream>
```

```
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority>355</x:priority>
    <x:defaultstream>UDP 0.0.0.0:5061 0.0.0.0:0 UDP/SIP</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority>356</x:priority>
    <x:defaultstream>TCP 0.0.0.0:0 0.0.0.0:5061
        SIPDetector</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority>357</x:priority>
    <x:defaultstream>TCP 0.0.0.0:5061 0.0.0.0:0
        SIPDetector</x:defaultstream>
</x:defaultstreamconfig>
```

5. Save and close the file.
6. Open a command window, and do the following:
 - a. Go to the following location:
%IMPACT360SOFTWAREDIR%\ContactStore\Tools
 - b. Run the following command:
ChecksumUtil.exe -g %IMPACT360SOFTWAREDIR%\ContactStore\IPCaptureProtocolConfig.xml
The checksum utility updates the checksum with the modifications you have made. Failure to complete this step results in a 'file tampered' alarm.
7. In Recorder Manager, go to **General Setup > Protocols**, and then click **Save**.
8. Go to **Operations > Start/Stop**, and then restart the following service:
Recorder IP CaptureEngine

Add additional SIP signaling port numbers

By default, the system uses port 5060 for SIP signaling in a SIP interception recording environment. To use additional port numbers, update the system configuration to listen for SIP signaling on those additional ports. To make the update, change the **IPCaptureProtocolConfig.xml** configuration file.

Procedure

1. Navigate to the following folder in the folder in the installation directory:
%IMPACT360SOFTWAREDIR%\ContactStore
2. Use a text editor, such as Notepad, to open the following configuration file:
IPCaptureProtocolConfig.xml
3. Locate the following section:
<x:name>SIP</x:name>
4. Add the following inside the SIP tags, where:
 - <n> is based on the next highest value available in the configuration file.
 - <SIP Port> is replaced with the port number to use for SIP signaling.Repeat the block of XML for each additional port number you want to use.

```
<x:defaultstreamconfig>
    <x:priority><n></x:priority>
    <x:defaultstream>UDP 0.0.0.0:0 0.0.0.0:<SIP Port>
        UDP/SIP</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority><n+1></x:priority>
    <x:defaultstream>UDP 0.0.0.0:<SIP Port> 0.0.0.0:0
        UDP/SIP</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority><n+2></x:priority>
    <x:defaultstream>TCP 0.0.0.0:0 0.0.0.0:<SIP Port>
        SIPDetector</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority><n+3></x:priority>
    <x:defaultstream>TCP 0.0.0.0:<SIP Port> 0.0.0.0:0
        SIPDetector</x:defaultstream>
</x:defaultstreamconfig>
```

Example: Use ports 5061 and 5062 in addition to the default port. The SIP section would look as follows (additional port configuration shown in blue):

```
<!-- SIP Call Control Protocol -->
<x:callcontrolprotocol>
<x:name>SIP</x:name>
<x:description>Session Initiation Protocol</x:description>
<x:packethandler>SIPHandler.dll</x:packethandler>
<x:requireddlls>
    <x:requireddll>TCPHandler.dll</x:requireddll>
    <x:requireddll>SIPHandler.dll</x:requireddll>
</x:requireddlls>
<x:defaultstreamlist>
    <x:defaultstreamconfig>
        <x:priority>350</x:priority>
        <x:defaultstream>UDP 0.0.0.0:0 0.0.0.0:5060
          UDP/SIP</x:defaultstream>
    </x:defaultstreamconfig>
    <x:defaultstreamconfig>
        <x:priority>351</x:priority>
        <x:defaultstream>UDP 0.0.0.0:5060 0.0.0.0:0
          UDP/SIP</x:defaultstream>
    </x:defaultstreamconfig>
    <x:defaultstreamconfig>
        <x:priority>352</x:priority>
        <x:defaultstream>TCP 0.0.0.0:0 0.0.0.0:5060
          SIPDetector</x:defaultstream>
    </x:defaultstreamconfig>
    <x:defaultstreamconfig>
        <x:priority>353</x:priority>
        <x:defaultstream>TCP 0.0.0.0:5060 0.0.0.0:0
          SIPDetector</x:defaultstream>
    </x:defaultstreamconfig>
    <x:defaultstreamconfig>
        <x:priority>354</x:priority>
        <x:defaultstream>UDP 0.0.0.0:0 0.0.0.0:5061
          UDP/SIP</x:defaultstream>
    </x:defaultstreamconfig>
    <x:defaultstreamconfig>
        <x:priority>355</x:priority>
        <x:defaultstream>UDP 0.0.0.0:5061 0.0.0.0:0
          UDP/SIP</x:defaultstream>
    </x:defaultstreamconfig>
```

```
<x:defaultstreamconfig>
    <x:priority>356</x:priority>
    <x:defaultstream>TCP 0.0.0.0:0 0.0.0.0:5061
        SIPDetector</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority>357</x:priority>
    <x:defaultstream>TCP 0.0.0.0:5061 0.0.0.0:0
        SIPDetector</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority>358</x:priority>
    <x:defaultstream>UDP 0.0.0.0:0 0.0.0.0:5062
        UDP/SIP</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority>359</x:priority>
    <x:defaultstream>UDP 0.0.0.0:5062 0.0.0.0:0
        UDP/SIP</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority>360</x:priority>
    <x:defaultstream>TCP 0.0.0.0:0 0.0.0.0:5062
        SIPDetector</x:defaultstream>
</x:defaultstreamconfig>
<x:defaultstreamconfig>
    <x:priority>361</x:priority>
    <x:defaultstream>TCP 0.0.0.0:5062 0.0.0.0:0
        SIPDetector</x:defaultstream>
</x:defaultstreamconfig>
</x:defaultstreamlist>
</x:callcontrolprotocol>
```

5. Save and close the file.
6. Open a command window, and do the following:

- a. Go to the following location:

%IMPACT360SOFTWAREDIR%\ContactStore\Tools

- b. Run the following command:

ChecksumUtil.exe -g

%IMPACT360SOFTWAREDIR%\ContactStore\IPCaptureProtocolConfig.xml

The checksum utility updates the checksum with the modifications you have made. Failure to complete this step results in a 'file tampered' alarm.

7. In Recorder Manager, go to **General Setup > Protocols**, and then click **Save**.

8. Go to **Operations > Start/Stop**, and then restart the following service:

Recorder IP CaptureEngine

Use the Configuration Checker

The Configuration Checker utility allows you to detect configuration problems related to recording systems (managed servers that operate together to support phone or screen activity recording).

Topics

Configuration Checker	406
Select your recording environment	407
Check configurations	408
View Configuration Checker details	409

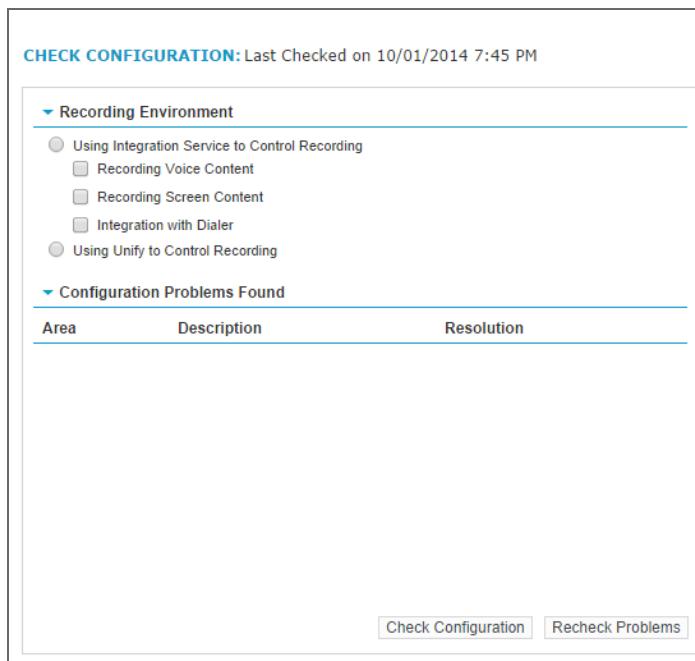
Configuration Checker

If you are using Enterprise Manager to manage servers that record telephone calls or record screen activity, you should understand how to use the Configuration Checker utility.

The Configuration Checker utility allows you to detect configuration problems related to recording systems (managed servers that operate together to support telephone call or screen activity recording).

You can launch Configuration Checker from any node of the Installations tree, and also from the Data Sources, Attributes, or Rules windows by clicking the 'check configuration' icon ✓ at the top right of applicable windows.

The Configuration Checker shows a list of any current configuration issues, and makes recommendations for resolving the problems.



You must have the necessary security privileges to run the checker tool, including the Run Configuration Checker privilege (configured in the Roles Setup window).

Related topics

[Select your recording environment \(page 407\)](#)

[Check configurations \(page 408\)](#)

[View Configuration Checker details \(page 409\)](#)

Select your recording environment

Before you can run the Configuration Checker, you must select your recording environment.

Procedure

1. From any node of the Installations tree, or from the Data Sources, Attributes, or Rules screens, click the **Configuration Checker** button (a checkmark in the upper-right corner of the screen).

 Details of the previous configuration check, if one has been done, appear in the lower portion of the window.
2. Under **Using Integration Service to Control Recording**, select one of the following:
 - **Record Voice Content** – Check this option if audio (voice) is being recorded.
 - **Record Screen Content** – Check this option if screens are being recorded.
 - **Integration with Dialer** – Check this option if a Dialer switch is integrated with the recording environment.
3. Do one of the following:
 - Click **Check Configuration** and follow procedures described in [Check configurations \(page 408\)](#).
 - Click **Recheck Problems** to run the checker on the results of a Check Configuration. In some situations, rechecking problems provides additional details about the configuration problems found during the initial configuration check.
4. Click **Close** when finished.

Check configurations

Check configurations to identify and resolve configuration issues detected in the recording environment that prevent optimum performance. You can also experiment by checking configurations with different sets of options. For example, you can view configuration problems related to recording voice content, recording screen content, or both.

Here, you select either of these options, described in [Select your recording environment \(page 407\)](#), and then click **Check Configuration** again to display new results.

Procedure

1. Click the **Configuration Checker** button (a checkmark in the upper-right corner of the screen).
2. Select the appropriate Recording Environment options, as described in [Select your recording environment \(page 407\)](#).
3. Click **Check Configuration** or **Recheck Problems**. New information displays, based on the currently selected options.
4. Review the **Configuration Problems Found** area, which contains the following information:

Item	Description
Area	Shows the area, either Installations, Data Sources, Attributes, or Rules, in which a problem has been found. Click on the link to open the area of Enterprise Manager where you can resolve the problem.
Description	Describes the problem found in the displayed area. For a complete list of all possible problems that can be found, refer to View Configuration Checker details (page 409) .
Resolution	Tells you how to resolve the configuration problems found.

5. Do one of the following:
 - Click **View Details** and follow procedures described in [View Configuration Checker details \(page 409\)](#).
 - Click any other hyperlinked item, such as **Installations** or **Data Sources**, to go to that other area.
6. Click **Close** when finished.

View Configuration Checker details

View details of a configuration check to obtain in-depth information on a selected configuration problem that has been detected. The View Details option allows you to experiment with various settings to continuously improve your configuration.

To view configuration checker details

1. Run the Configuration Checker tool as described in [Check configurations \(page 408\)](#).
2. In the **Description** column, click the (View Details) hot text that appears at the end of the description of a particular problem.
3. Review the following information:
 - **Description:** The current configuration problem.
 - **Resolution:** What you must do to resolve the current configuration problem.
 - **Server Name:** A list of managed server names in the recording environment.
 - **Site:** The name of the Site containing the specified server name.
4. Click **Back** when finished to return to the summary configuration checker window, or click **Close** to close the window.

To view all configuration checks

The following table summarizes all configurations checked, and shows the conditions under which the check will appear:

Configuration Check	Description	Conditions When Check Displays
No Servers (Recorders) in Enterprise	Checks to see if any managed recorder servers exist in Enterprise Manager.	Number of Installations equals zero.
Integration Service Not Associated to any Servers	Checks to see if Integration Service is controlling any managed recorder server.	Server with IS role exists and has no Recorders/servers associated to it.
Server Not Associated to Any Member Groups	Checks to see if there are any managed recorder servers that do not have any Member Groups associated to them. (Applies only to servers that have either the TDM Recorder or IP Recorder server roles activated.)	(Using Integration Service is true OR server has IP Recorder role), AND no Member Groups are associated to it.
Server Needs to be Migrated	Checks to see if server needs to be migrated to a newer version of the server.	Server's migration needed flag set to true.
Server Has Active Alarms	Checks to see if server has any active alarms that have not been acknowledged.	Server's active alarm count is greater than zero OR server's communication error is set.

Configuration Check	Description	Conditions When Check Displays
People Not Associated to Phone Data Source	Checks to see if employees have not been assigned to a switch by means of their employee IDs or extension.	Person is not associated to any Data Source by means of employee ID or extension.
People Not Associated to LAN Data Source	Checks to see if employees' network logon has been set in Enterprise Manager.	Person is not associated to any LAN Data Source by means of network ID or Workstation.
Data Source Has No People Associated	Checks to see if a Data Source has no people associated to it.	Data Source type is Phone, LAN, Dialer, or Application, AND Data Source has no people associated by means of employee/network ID or extension/Workstation.
Data Source Not Associated to Integration Service	Checks to see if a Data Source has been associated to an Integration Service.	Data Source's type is Phone or LAN, AND no Integration Service is associated.
No Phone Data Source Created	Checks to see if any phone Data Source has been created in system.	Check displays if Recording Voice Content is true and No Phone Data Sources exist.
No LAN Data Source Created	Checks to see if any LAN Data Source has been created in system.	No LAN Data Sources exist.
No Dialer Data Source Created	Checks to see if any Dialer Data Sources exist.	No Dialer Data Sources exist.
Dialer Data Source Not Associated to Phone Data Source	Checks to see if any Dialer Data Sources have not been associated to a Phone Data Source.	Dialer Data Source exists and is not associated to any Phone Data Source.
Extensions Not Associated to Workstations	Checks to see if any extensions exist which are not associated to a Workstation. This is needed in cases where dynamic workspaces cannot be used.	Data Source's CTI Logon Provided field is false and extension does not have a Workstation associated to it.
Workstations Not Associated to Extensions	Checks to see if any Workstations exist which are not associated to an extension. This is needed in cases where dynamic workspaces cannot be used.	Data Source's Unique Logon Per Employee is set to false and Workstation does not have an extension associated to it.
Workstation Not Associated to Workstation Group	Checks to see if any Workstations exist that are not a part of any group.	Workstation not associated to any Workstation Group.

Configuration Check	Description	Conditions When Check Displays
LAN Subnet Not Associated to Workstation Group	Checks to see if any subnets are not associated to any Workstation group.	Subnet not associated to any Workstation Group (for Dynamic Workspaces).
Workstation Group Not Associated to Server	Checks to see if any Workstation groups are not associated to a server/Recorder.	Workstation Group Not Associated to any server.
Member Group Not Associated to Server	Checks to see if any Member Groups have been created but not associated to a managed recorder server.	Member Group has not been associated to any servers.
There are no servers in the enterprise with the Interaction Capture server role activated.	Checks to see if any server in the Enterprise has the Interaction Capture server role activated.	No server in the enterprise has the Interaction Capture server role activated.
There are Lync data source(s) with no Recording Profiles created.	Checks to see if Recording Profiles are created for Lync data sources.	No Recording Profiles are created for Lync data sources.
There are no data sources created for text recording.	Checks to see if a data source is created for text recording. Either a Cisco Jabber, Lync, or Generic Text data source must be created in a text recording environment.	No data sources are created for text recording.
There are text data sources with no associated Recorder Integration Service Installations.	Checks to see if a Recorder Integration Service Installation is associated with a text data source. A Cisco Jabber data source does not require an association to a Recorder Integration Service server role.	A text data source exists that has no Recorder Integration Service Installation associated with it.
There are text data sources with no associated Interaction Capture Installations.	Checks to see if a Interaction Capture Installation is associated with each text data source. For Cisco Jabber or Lync text recording deployments, an Interaction Capture Installation must be associated to the data source. For a Lync audio-only deployment, it is not necessary to associate an Interaction Capture Installation to the data source.	A text data source exists that has no Interaction Capture Installation associated with it.
There are text data sources with no associated Lync Installations.	Checks to see if a Lync Installation is associated with each Lync text data source.	A Lync text data source exists that has no Lync Installation associated with it.

Reference

This section is an A - Z reference covering the concepts and terminology related to Recording.

Topics

Archive	414
Audio quality statistics events (AQS)	415
Conditional Custom Data	420
Conditions	421
CTI-based Recorder selection	423
Custom Data	424
Data sources	425
Delivery	426
Dialers	427
Extension recording modes	429
Extensions	430
Fallback modes	431
Hunt group	432
Integration Service	433
Interception	435
IP recording	438
Member groups	441
Multiple Recorders and high availability	444
NIC teaming	445

Phones	447
Queues	448
Real-Time Monitor	449
Recorder control types	450
Recording resources	452
Roles	453
RTP detection	454
Screen Recording	455
Seating arrangements	458
Selective extension pools	459
Shared screen Recorders	460
Shared lines	461
SIP trunk recording	462
Subnets and subnet masks	464
TDM recording	465
Trunk span groups	467
Video stitching of separate recordings	468
Workstations and workstation groups	469

Archive

Archive transfers selected recordings to a specific archive device for long-term storage or for disaster recovery. Archive may be *local* or *central*.

Local Archive

- pulls and archives recordings from a single, local Recorder only.
- archives 100% of recordings.
- uses the state of the local Recorder to identify calls (thereby reducing interaction with the database).
- is only available for Recorders that are assigned the TDM, IP, or Screen role.

Central Archive

- archives recordings from Recorders across the enterprise.
- archives selectively based on customized campaigns.
- queries the database for calls to record.

Related topics

[Reference \(page 412\)](#)

Related information

Archive Administration Guide

Audio quality statistics events (AQS)

Verint customers can validate the audio quality of recorded interactions. Audio quality can potentially be used to isolate issues in the recording system, network, or associated communications system.

Audio quality statistics events are available for real-time or recorded interactions. These scores show interactions with low audio quality, which can help identify issues with hardware or software resources, the network, or VPN connections. In Automated Verification, you can view the audio quality statistics results of your calls associated with the data sources of your organizations and set target levels of service to use as performance benchmarks.

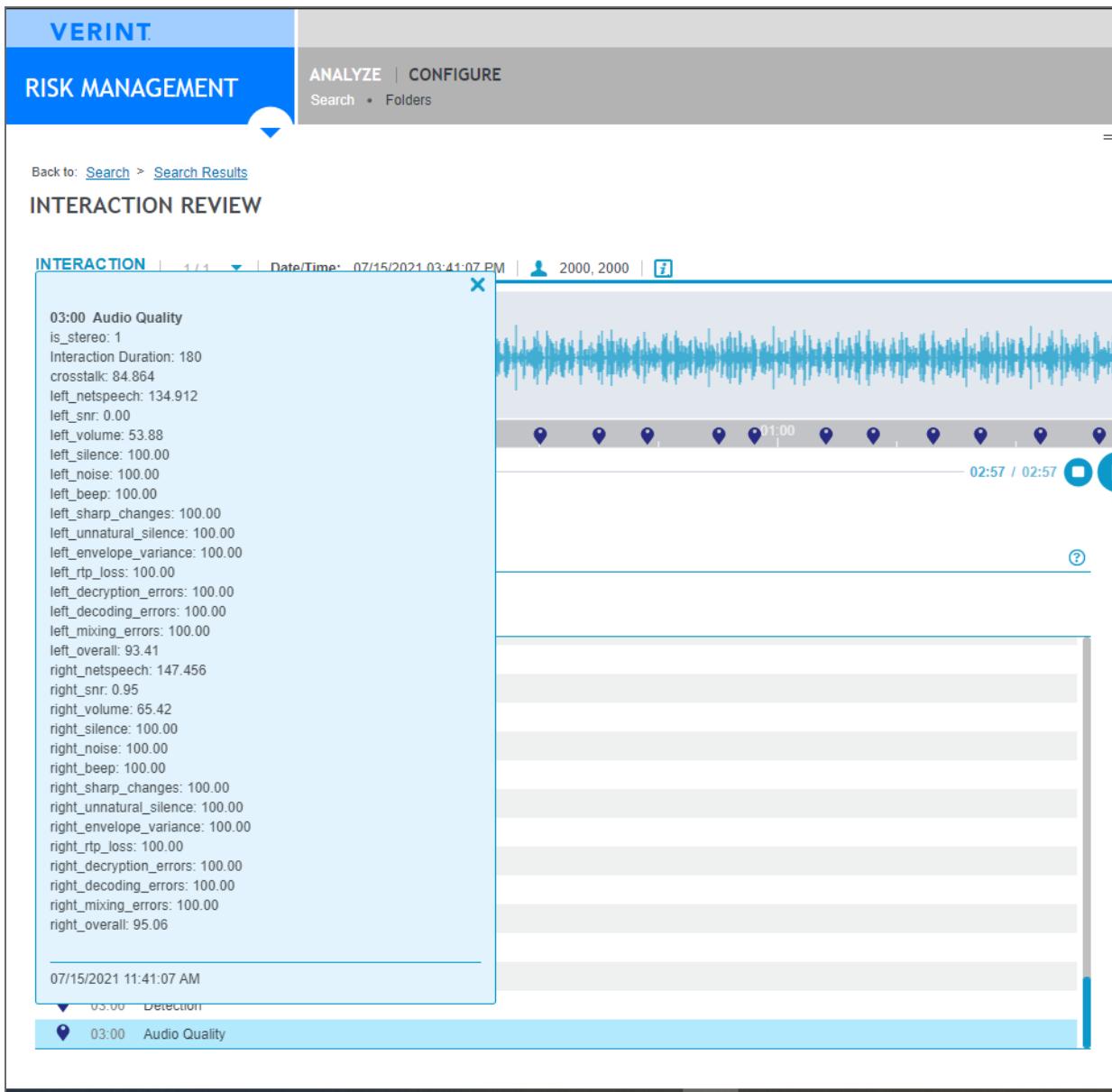
The events are stored in the database, so can affect database storage usage.

Viewing the audio quality statistics of an interaction

When viewing an interaction in Player, you can use the Tags panel to display voice quality statistics of an audio recording. Audio quality is measured as a score on a scale of 0% to 100%. The higher the percentage, the better the quality of the recording. Scoring takes place for both agent and customer sides, and at the segment level.



Audio quality scores calculated before V15.2 2021R1 are listed as Data Events and are stored and displayed per inum.



Event scoring

Scoring takes place for both agent and customer sides, and at the interaction level. The scores for an interaction are based on the weighted average scores for each segment in the interaction and its duration. By default, segments less than 15 seconds are not included in the score; however, you can change the duration on the Data Source settings page. The Minimum Recording Duration for AQS setting is available in Advanced mode.

Score	Quality
80 – 100%	Good

Score	Quality
50 – 79%	Fair
< 50%	Poor

Audio Quality event descriptions

Event	Description
RTP loss	Losing RTP packets can cause missing audio segments, which degrade voice quality.
SRTP decryption errors	Decryption errors cause silence in recording instead of the decoded voice or audio.
Decoding errors	Decoding errors cause silence in recording instead of the decoded voice or audio.
Media mixing errors	Discarded late frames due to stream synchronization. Some errors are normal; however, too many errors can cause dropping the voice of one or all participants.
Volume	Detects whether the average volume is below a specific threshold. When the average volume is below a specific threshold, the voice cannot be heard.
Silence	Too much silence is a recording issue. Silence can be caused by network errors and media processing issues. The amount of silence can be different for certain use cases where long silence is typical, such as trader voice open lines.
Noise	Too much noise can severely degrade voice quality. Noises that affect the original call are caused by: <ul style="list-style-type: none"> • Endpoints with a poor acoustic environment. • Endpoints with bad quality devices. • Media decoding or decryption errors during recording.
Beeps and clicks	Beeps or clicks are considered decoding issues. Too many beeps or clicks can affect the ability to understand the recording.
Amplitude sharp changes	Speech characteristically has words or phonemes that fade softly. A quick or sharp change in speech signals processing issues, such as dropped voice frames or fragments.
Unnatural silence	Unnatural silence is: <ul style="list-style-type: none"> • Silence followed by sharp amplitude changes. • A sign of dropped voice frames or fragments caused by media processing and network issues.

Event	Description
Waveform envelope variance	A histogram is built based on amplitude delta ranges, whose variance shows a statistical correlation to speech. Too much deviation from this model is scored as an unnatural voice, which indicates media processing or network issues.
Net speech	Quantity of net speech, in milliseconds
Signal-to-Noise ratio	A comparison of the level of a desired signal to the level of background noise. For a reliable connection, the signal level has to be significantly greater than the noise level.
Crosstalk	Interference from other channels that results in random signals or sounds in the audio.
Overall	The overall score for the interaction, calculated from the values of the individual statistics.

Related topics

[Enable AQS \(page 418\)](#)

Related information

Tags tab (*Player User Guide*)

Enable AQS

The capture of audio quality statistics (AQS) is a licensed feature introduced in 15.2 2021R1. You must enable the capture of these events through the IP Recorder server role.

AQS with SQL Server 2016 SP1 and newer

When licensed and enabled in an environment with SQL Server 2016 SP1 or newer, the audio quality scores are listed as Audio Quality Events and are stored and displayed per interaction.

With previous versions of SQL Server

When licensed and enabled in an environment with previous versions of SQL Server, the audio quality scores are listed as Data Events and are stored and displayed per inum.

Before you begin

Ensure that the system is licensed for Audio Quality Statistics.

Procedure

- Enable the Audio Quality Statistics feature license:
 - a. In a browser, go to `http://<wfo_app_server_address>/wfo/control/license_edit`.
 - b. On the **License Data** page, under **Features**, enable **2021R1 - Audio Quality Statistics**.
 - c. Click **Save**.

- Turn on Advanced Mode:
 1. In **System Management**, go to **Settings**.
 2. Select the Enterprise node, and then select **More Actions**.
 3. Select **Turn Advanced Mode On**.
- Enable Audio Quality Statistics on the IP Recorder server role:
 1. Under **System Management**, go to **Enterprise** and select **Server Roles**.
 2. In the **Installations** tree, expand the server nodes and select the IP Recorder server role.
 3. Under **Advanced**, select **Audio Quality Statistics**.
 4. Click **Save**.

Related information

License and product activation for a system license (*System Administration Guide*)

Related topics

[Audio quality statistics events \(AQS\) \(page 415\)](#)

Conditional Custom Data

Conditional Custom Data fields are used to tag data that cannot be directly obtained from an external source, but rather calculated from the value in another field or the employee's profile. (For example, Skill Set based on Employee Name.)

Rules define the logic of the value to tag, and the rules are executed when the segment ends. For example, an enterprise may want to tag a contact with an indication of the line of business to which it belongs, when this data is not available from CTI. It may be possible to determine the line of business based on the dialed number (DNIS). In this case, a Conditional Custom Data field can be dedicated to the "Line of Business" information. You can configure rules that determine how this field is populated.

Example: Line of Business

An enterprise has three lines of business. They want to tag the line of business to the call and use this to drive analytics and reports. In this hypothetical case, data is not available from CTI, but it is possible to determine the line of business based on the dialed number (DNIS).

Define a Conditional Custom Data field called "Line of Business" and set up the following rules in the System Toolbox Conditional Custom Data application:

If DNIS = 1800-111-222, Line of Business = Car Insurance

If DNIS = 1800-111-333, Line of Business = Health Insurance

If DNIS = 1800-111-444, Line of Business = Home Insurance

Related topics

[Reference \(page 412\)](#)

Conditions

Your recording system includes standard Contact, Employee, and CTI attributes. You can use these attributes for tagging and to build recording rules, where the attributes become criteria upon which the decision to record or not is based.

Recording rules extend the functionality of your recording system by allowing you to implement recording and tagging on the basis of a business logic that reflects the goals of your enterprise. Each rule consists of a set of conditions (such as "extension starts with") and actions (record, block, and so on). These rules are like if-then propositions that you can use to extract, from the contacts, a set of meaningful data that you can then analyze for a business purpose. The rules trigger recording when contacts that take place between customer interaction center employees and customers meet the specified criteria.

Examples:

- You could create a rule that specifies "if Contact Duration is **Greater Than20 minutes** (1200 seconds), then Record Audio, at a level of 25% of all contacts (with Randomize on Individual member enabled)." This will provide a sample of contacts lasting longer than 20 minutes, and handled by a range of employees. You could use the results to examine whether certain factors may be contributing to lengthy resolution times in a support center.
- Imagine that you have an employee within your organization who is particularly successful at resolving contacts without placing the caller on hold to seek additional help or resources. You could create a rule that specifies "if **Employee Name** is Equal to AgentABC and Time on Hold is Equal to 0 (zero), then Record Audio and Screen at a level of 100%." You could use the captured data to analyze whether the employee uses strategies that are repeatable, and then, with the use of eLearning tools available in Advanced packages, turn the data into a Web-based learning clip that you could then distribute internally as an educational tool.
- Imagine that you are running a specific campaign, and you want to analyze whether specific supervisors were successful in communicating to employees the key goals of the campaign. Assume all calls for this campaign are to a special promotional number; you could set up the following rule: "if Number Dialed Equals **1-800-555-5555**, then Record Audio, at a level of 10% of all contacts, where the Supervisor Name is Equal to Supervisor A Or Supervisor B (with Randomize on Individual member enabled)." This will record a random sampling of campaign-related calls to employees working for Supervisors A and B.

Monitoring a block of time

Occasionally, you may want to monitor a block of time for an employee. You can make any rule run on specific schedule, triggering contact recording on certain days or during defined time periods.

Example: Monitoring a block of time

To identify opportunities for professional development for a specific employee, you might create a schedule-based rule to record the employee's interactions with customers during certain hours each day.



You can enter multiple values for some conditions, and these must be separated by a semi-colon (;).



For Full-time Recording, the schedule defines a time period during which a rule is actively evaluating its recording criteria or entirely inactive.

Tagging a recording

You can specify that each recording triggered by a given rule is tagged, so that you can later identify it as such.

Configuring rules

You can configure recording rules in the Enterprise Manager, and propagate these rules across the Enterprise to associated sites.

Related topics

[Reference \(page 412\)](#)

CTI-based Recorder selection

In Shared Interception or Avaya DMCC environments, you may specify that individual calls be directed to a Recorder based on specific call data (for example, the call's trunk group).

Settings

- Custom Attributes, which you may use to create a non-standard attribute upon which to base recording—see [Create, edit or delete an attribute \(page 278\)](#).
- Recording Resource Allocation Behavior—see [Create a phone data source \(page 49\)](#).
- Member Group settings, where you will identify an attribute and value which, if present in the call data, will signal to the system that the associated Recorder should record that specific call:
 - For Shared Interception, see [IP extension pool member group settings \(page 71\)](#)
 - For Avaya DMCC, see [Extension recording resource member group settings \(page 75\)](#)

Related topics

[Reference \(page 412\)](#)

Custom Data

Custom Data (also known as private data) is the term for fields customized to store data used for purposes such as reports and analytics. The value of these data fields is populated by CTI or by other applications. Each segment has its own custom data, and the contact entity inherits the custom data of the last segment.

You do not need to map Custom Data fields to particular user-defined fields. However, you can store additional attributes in the database as custom data. You can define up to 300 custom data fields and map them to a standard attribute in the Enterprise Manager.

Related topics

[Reference \(page 412\)](#)

Data sources

Data sources are third-party systems, such as private branch exchanges (PBXs) and CTI middleware servers, that generate employee state, device state, and data change events. The Recorder makes business decisions on the interactions to record based on the events supplied by the Integration Service. They also provide business views of interactions based on different logic.

Each type of recording you can configure involves a different type of data source:

- Phone or PBX data sources are for *voice recording*
- Dialer data sources are for *voice recording for a dialer*
- LAN data sources are for *screen capture* (also called screen recording)

Related topics

[Reference \(page 412\)](#)

Delivery

TDM Delivery

Trunk Delivery (line-side recording using E1 trunks) is a type of trunk termination that can be implemented in Avaya switches and is supported on ISDN trunks (DT6409 and DT3209 cards only).

E1 line-side (E1 LS) is a recording method in which the Recorder uses service observe in to control extensions (supported in Avaya switches). It maps each of its recording channels to one of the E1 trunk time slots and to specific employee extensions. When an employee logs in to the switch, the Recorder establishes silent observation for the extension on a recording channel, and from that moment on, the trunk delivers the extension's audio to the Recorder.

VoIP Delivery

VoIP Delivery is supported in SIP-based DMS for Cisco Call Manager, and Device and Media Call Control (DMCC)-driven DMS for Avaya, and certain Trading environments. (See the associated *Integration Guide* for solution-specific information.)

VoIP Delivery in DMCC Environments

DMCC is a software connector that provides a programming interface for device and media control on the Avaya Communication Manager switch. Using the DMCC, you can develop applications that can do the following:

- Gain exclusive or shared control of extensions defined in the switch.
- Perform telephone operations, such as silent observation.
- Process or redirect media using RTP (VoIP), such as sending an extension's audio to a specific IP address.

Applications developed for DMCC communicate with the Avaya Communication Manager switch through the DMCC Connector interface. These applications send the DMCC Connector requests to take control of an extension defined in the switch, in order to perform telephone operations on these extensions. These operations can include making calls, receiving calls, sending announcements, applying tones, detecting digits and redirecting the extensions calls to a specific IP address.

The DMCC Connector sends the request to the switch and in effect creates a "soft phone" for the relevant extension (that is, a virtual phone that is controlled using an application rather than a physical telephone device). The DMCC Connector can instruct the switch where to direct the audio (in the format of RTP streams) for calls made to and from the extension. This feature enables the Recorder to record calls on these extensions.

For complete information about DMCC integrations, including details on Single Step Conferencing, Service Observe, and Multiple Registration, see the *Avaya Integration Guide*.

Related topics

[Reference \(page 412\)](#)

Dialers



For configuration instructions and network diagrams, please see [Set up a dialer integration \(page 116\)](#), and the *Avaya Integration Guide* and *Aspect Integration Guide*, and tapping diagrams for dialers in IP, station side and trunk side environments.

A dialer is a device that generates outbound calls to customers based on targeted lists of names and phone numbers. It sequentially and automatically calls these numbers, detects when a customer answers and then routes the call to an employee in the call center. Dialers dial multiple customer numbers simultaneously to ensure there are a sufficient connected calls to keep the employee population busy.

Dialers use sophisticated algorithms to predict the appropriate number of simultaneous calls to make so that when a live customer is reached, an employee will be available to take the call. For this reason, dialers are often referred to as "Predictive Dialers."

Soft Dialers

Soft dialers are software-only dialers that instruct the PBX to initiate calls using Active CTI. This dialer type has no external trunks to the PSTN. When working in environments with soft dialers, the only CTI connection is with the PBX.

Hardware Dialers

Hardware Dialers connect to the PSTN (directly or indirectly through the PBX) and can be configured in the following working modes:

- **Nailed agent**—The Predictive Dialer establishes a long call with each outbound employee, for the whole duration of the employee's shift, and connects employees with the outbound calls it generates internally. Employees are dedicated to answering calls initiated by the Predictive Dialer throughout their shift; from the moment that login has been performed. In the common "Nailed Agent Mode", the PBX's CTI link reports just one long call between the employee and the dialer.
- **Blended agent**—the Predictive Dialer "manages" the employee's extension by transferring outbound calls to the employee but also allowing the connection of incoming ACD calls when necessary.
- **Stand alone**—Stand-alone dialers act as a PBX and the extensions are connected directly to the dialer. This mode is rare.

If trunk-side tapping is required, trunks are intercepted in two places: between the PSTN (Public Switch Telephony Network) and the contact center switch (PBX), and between the dialer and the PBX. Trunk-side tapping is supported for all of the hardware dialers we integrate to, assuming a trunk supporting PBX integration.

Note that the Recorder taps the trunks between the Dialer to the PBX and not between the dialer to PSTN. In some cases there may be a TDM network between the dialer and the PBX, for example if the dialer and PBX reside in two different countries.



In some dialers the first call is not marked as "nailup" until the first campaign call is made. In this case, since the Recorder Integration Service cannot distinguish this call from any other non-nailup switch call, the call is monitored ("Call in Progress" is displayed and the customer will hear silence). This is expected behavior.

Phone Data Sources for Dialer Integrations

When Dialer employees login to dialers, typically a call is placed from the dialer to the employee through the PBX and a connection is established and maintained for their entire dialer login session. This call is typically called a "nailup call". When doing trunk side recording deployments it is necessary to tap the trunks that are between the dialer and the PBXs that are used to establish these nailup calls in order to record the voice for dialer calls.

You configure this by creating a Phone Data Source with a Trunk Side Member Group for the dialer trunks. Usually these trunks are set up by the PBX administrator with either Trunk IDs or with Extension IDs, so the member group "Type" field should be set accordingly. In the Member Group you should configure either the Extensions or Trunk IDs for the trunks between a dialer and the PBX that are being used for nailup calls. In addition, you must select the Dialer Data Source that defines the dialer to which the trunks are connected.

Related topics

[Reference \(page 412\)](#)

Extension recording modes

Each phone associated with a Phone data source has a primary extension, and optional secondary extensions. Each extension has a default recording mode that determines the recording behavior for that extension.



Block Recording Rules and Block commands using AIM, Connect and other third party APIs will cause the interaction or contact to not be recorded, regardless of the extension recording mode, recording rules or other third party API commands.

Available recording modes

- **Record**—Record all calls on this extension.
- **Do Not Record**—Do not actively record this extension. Other extensions on the same call will follow their respective Recording Mode, and may record audio for this extension. External API commands or recording rules do not override this setting.
- **Application Controlled**—Record every call, and then delete it. At any time during a call, an Recording Rule or external API command can cause the Recorder to keep the call.
- **Start on Trigger**—Do not record calls on this extension until a recording rule is triggered or an external API command starts recording. If the Recorder is set to CTI Controlled, recording will start whenever the Recorder starts, but audio prior to the recording trigger will be deleted; the interaction will start there, and continue to the end of the call. If the recorder control type is Recorder Controlled, recording start at the beginning of each call. Each segment is flagged, and this flag determines whether segment is kept or discarded when the call ends. If a recording rule is triggered, the Integration Service will segment the recording that is ongoing (if one exists) and the portion before the recording rule will be discarded. The portion after the recording rule will be kept. If no recording rule is triggered, the entire recording is discarded.
- **Recording Resource**—Only for soft phones. Use in conjunction with a Service Observe or Single Step Conferencing Recorder Control type.

Related topics

[Reference \(page 412\)](#)

Extensions

You can configure telephone extensions either as a group (in cluster mode), or individually. In clustered mode, extension configuration is the same across Recorders within the Site. In unclustered mode, you configure extensions individually. You can only cluster extensions in an IP extension pool.

The recording mode is applied to all extensions that are not included in the member groups associated with the Recorder. For example, if a Recorder is associated with a member group that uses extensions 1000 and 1001, 1000 and 1001 will be governed by the settings of the member group, but all other extensions will use behavior of the *recording mode*.

In [Set up phones and extensions \(page 124\)](#), you can add primary and secondary telephone extensions for use throughout the organization, specify whether phone extensions are recorded, and select a recording mode.

Recording Duplicate Extensions

You can record duplicate extensions on different switches using a single IP or TDM Recorder/Integration Service. This could be required in a number of scenarios, including environments in which load balancing/redundancy are performed at the switch (as opposed to the Recorder), where employees may log on using the same extension on different switches.

The Recorder uses the source or destination IP addresses of the signaling messages to identify the particular data source with which a call is associated. It does not use any data inside the signaling itself to make this determination. For this reason, the source/destination of the IP packets presented to the Recorder *must be different for each duplicate extension*. Make sure that your network is set up in such a way as to allow for this.

Example:

A proxy server in front of separate PBXes using duplicate extensions can cause IP packets to appear as though they are using the same IP address (even though the SIP signaling would indicate otherwise). This will prevent the duplicate extensions from being recorded correctly. To configure these types of deployments,

- Enter the duplicate extensions in Enterprise Manager, creating a separate data source for each switch (each with whatever extensions are in use).
- In the data source settings, under **Device IP Configuration**, enter the **IP Address or Host Name** of the server used to send/receive the control messages to/from the extensions, and set the **Server Type** to **PBX Side - Near End** (see [Create a phone data source \(page 49\)](#) for instructions).
- Associate the data source with the same Recorder and Integration Service.

The recording system will use the data source and extension in combination to uniquely identify the call for tagging and recording purposes.

Related topics

[Reference \(page 412\)](#)

Fallback modes

There are three fallback modes, supported for both IP and TDM recording.

Fallback modes

- **Never (Application)**—If CTI is disconnected, no audio or screen recording will occur. If CTI is up, CTI segments will be retained.
- **On CTI Disconnection (Performance)**—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, only CTI segments with recorded audio are retained; if we receive CTI for a call but no audio (for any reason), recording will not occur. VOX segments (not associated to CTI calls) will be discarded. You can set a Rollback Period in the phone data source to specify the length of time preceding a disconnection for which recordings will be held.
- **Always (Liability)**—If CTI is disconnected, audio recording continues (VOX-detected segments will be retained), but screen recording does not. If CTI is up, both CTI- and VOX-detected segments will be retained. (If a signalling protocol is configured, it will be used before VOX to record the call.)

If you are using the Pause and Resume feature, ensure that you are also using Application mode. Use of Application mode ensures that any non-CTI call segments are discarded (rather than recorded and kept) if the CTI link goes down. Also, consider performing a manual review of calls recorded when CTI was down and verify that no sensitive data was maintained.



The fallback mode doesn't affect [Recorder control types \(page 450\)](#); rather, it is always the Recorder control type that defines how a recording is initiated (using CTI, Protocol, or VOX).

Related topics

[Reference \(page 412\)](#)

Hunt group

A hunt group is a way of distributing phone calls from a single telephone number to a group of several phone lines.

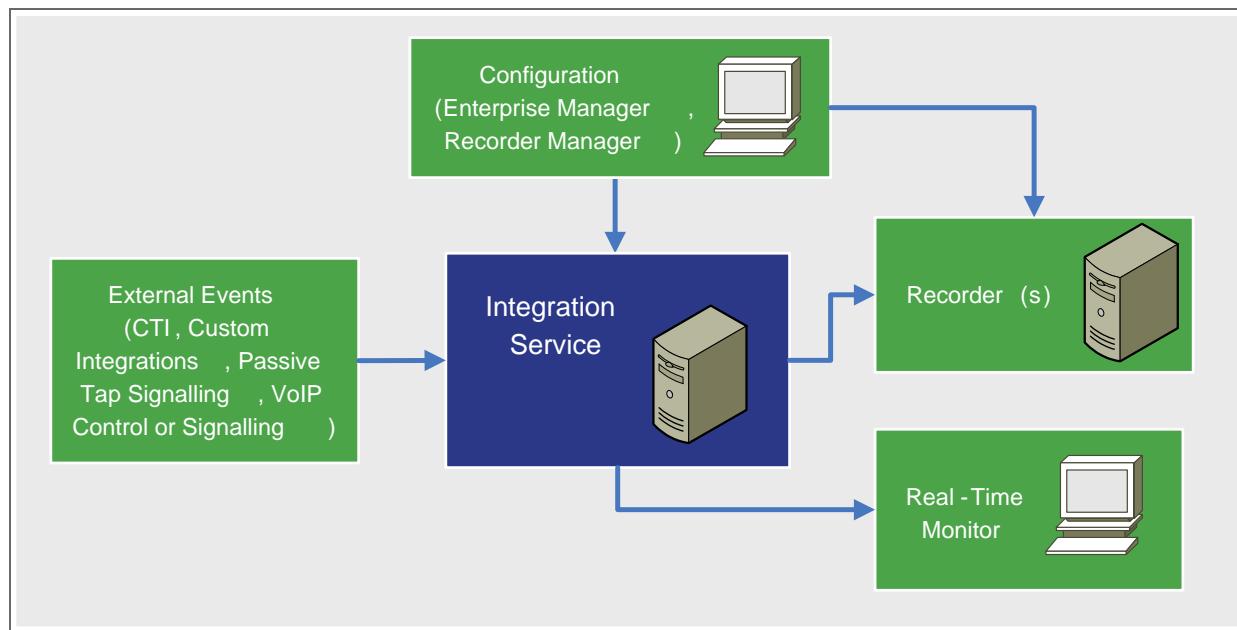
Related topics

[Reference \(page 412\)](#)

Integration Service

The Recorder Integration Service acts as an interface between the recording system and output from the switch and other data sources. The Integration Service processes events from the server interfaces, detects state or data changes, and passes them along to other subsystems. It can capture CTI event streams to file for later playback and viewing, and holds employee state, device state, call state, and data associated with all known devices and calls.

The Integration Service controls recording, and manages recording rules configured in the Enterprise Manager. It is also integral to the real time monitor process, with multiple Integration Services providing rollup state information into the Data Center application.



The Integration Service provides:

- A real-time common representation of the enterprise contact center state to other products in the suite
- Control of recording
- Auditing and event logging, with a level of detail sufficient to allow for troubleshooting
- A mechanism for capturing third-party application events, using captured events to test system behavior, and to facilitate support and testing of integrations when the third-party product is not accessible in-house

Integration and Adapters

The Integration Service performs call tracking and includes integration adapters, which enable the translation of recorded events from third-party systems (such as private branch exchanges [PBXs] and CTI Middleware Servers). Adapters connect to and receive events from the third-party systems, translating the event data into key-value pairs that are then sent to the Integration Service. Adapters notify the Integration Service of any serious errors in the third-party system, or in the communication

with that system. The Integration Service translates this information into data that is usable by the Recorder.

Configuration of adapters through the Recorder Manager enables the translation of recorded events from third-party systems into key-value pairs that are then sent to the Integration Service components. The Integration Service in turn translates this information into data that the Recorder and related applications can use.

Limitations

In non-CTI environments, the Recorder Integration Service does not support stitching (joining multiple segments into a single contact) of audio INums. In such environments, each INum will result in a separate contact/interaction.

For example:

- A call broken up by IPCapture as a result of a long time out
- Call transfers
- Call conferences

Related topics

[Reference \(page 412\)](#)

Interception

In interception, multiple Recorders may be used to record the calls.

IP Interception

IP Interception is essentially "typical" IP recording with a SPAN Port/port mirror. In IP interception there are two load-balancing types: Shared and Dedicated.

In Shared Interception:

- all recorders will see all the calls (that is, call control and media control messages plus audio).
- the Integration Service load balances call recording by enabling/disabling the resources.

In Shared Interception you may also specify (in Enterprise Manager) that individual calls be directed to a recorder based on specific call data (for example, the call's trunk group).

In Dedicated Interception (also referred to simply as "Interception"):

- all recorders will see all the calls (that is, call control and media control messages plus audio).
- Enterprise Manager load balances call recording by distributing the extension list to all the recorders with which the Member Group (on which Dedicated Interception is configured) is associated.

TDM Interception

Trunks transmit calls on randomly allocated time slots, where each trunk has either 30 timeslots (non-US E1 trunks) or 24 time slots (US T1 trunks), meaning that each trunk can simultaneously transmit 30/24 calls. In Recorder systems, the physical recording resource (or "channel") is dedicated to recording one time slot, regardless of the agent or extension transmitted on it.

In Interception, the recorder intercepts the trunks running between the Public Switch Telephony Network (PSTN) and the contact center switch (PBX). The trunks are rerouted to the PBX using a custom-built tap point. The card that interfaces with the trunks can be one of the following:

Supported Card	Tapping Method
Ai Logix DP6409 or DP3209	Trunk Side
NGX800-2400	Station Side

The trunk connected to the custom-built tap point contains both sides of the conversations (Tx and Rx), each side carried on a twisted pair wire. When routed to the recorder, a Y-cable is used to send each twisted pair into a separate connector on the acquisition board on the module. Thus, two "trunk inputs" are required for every customer trunk recorded. The recorder then concatenates both sides of the conversation.

Trunk-side tapping records the calls from the customer's perspective, meaning internal calls will not be captured, unless the customer is present on the call. For example, if two agents conduct a conference call, the recorder will not capture this conference, but rather anything the customer is saying while being on hold. However, if the DMCC VoIP feature is included in the solution, internal calls can be recorded too.

About Trunk Signaling Protocols

ISDN and Robbed Bit are types of Signaling Protocols, specific protocols on top of T1 and E1 trunks used for signaling things such as dial tone, ring, busy, or answer. The Recorder records trunks at a lower level, disregarding the signalling, since we are only interested in receiving the audio. Therefore both Robbed Bit (sometimes referred to as CAS) and ISDN T1 trunks can be tapped.

Trunk Interception with DMCC

Internal calls (including consultations, conferences and screened transfers) can be recorded in trunk-side interception environments. As DMCC is a Delivery solution, the following represents a hybrid recording approach.



As the solution requires using Device and Media Call Control (DMCC), this solution is only available for Avaya switches.

The solution involves the Integration Service initiating a conference call, known as a "single step conference", on a specific active internal call. The switch creates a conference call on the internal call that is taking place between the two (or more) agents using a virtual extension that is created in the switch by DMCC VoIP. Each virtual extension created by DMCC VoIP is mapped to a unit and channel. This allows audio to be transferred to the relevant DMCC VoIP channel that is mapped to this virtual extension.

For every agent (other than the original agent) that is added to the call, the Integration Service sends a "start session" event. In order to indicate that this is an internal call, rather than sending the module and channel that should be used to record the call, it uses a special channel mapping value (-1), that indicates that a dynamic unit-channel-virtual extension allocation will be required if the segment needs to be recorded.

Available DMCC units and channels, and the virtual extensions that DMCC VoIP uses, are stored. When an internal session starts, if it should be recorded, based on recording rules, free unit-channel and virtual extension is assigned, the Integration Service initiates the single step conference on this virtual extension for the recorded agent's extension. This will always be the extension of the agent who has been added to the existing customer call, or the agent who received the internal call from another agent. At the same time the conference is initiated, a CTI start event is sent to the relevant DMCC VoIP, telling it what channel to record.

Please note the following:

- Internal calls cannot be heard using the Real-time Monitoring feature.
- The number of internal calls that can be recorded depends on the number of virtual extensions supplied by the customer.
- As each single step conference initiated counts as a participant in the call, this solution limits the number of real participants who can participate in a conference call by one, for each single step conference that is initiated. For example, if 5 agents could normally participate in an internal call, in order to be able to record this call only 3 agents can participate (as two resources are required for the single step conference to record agents 2 and 3).
- The DMCC virtual extension numbers must be consecutive per DMCC VoIP unit.
- Under this configuration, two interactions are created.

- One interaction is for the extension.
- One interaction is for the trunk.

Screen recording can be interrupted and split into two recordings when both interactions try to record the screen. Since screen stitching is not supported, only the first screen recording is associated with the contact.

The result is a screen recording for only the first few seconds of the contact, with the remainder of the screen recording unavailable for simultaneous playback with the audio.

See [Configure network cards and filters \(page 243\)](#) for configuration instructions.

Related topics

[Reference \(page 412\)](#)

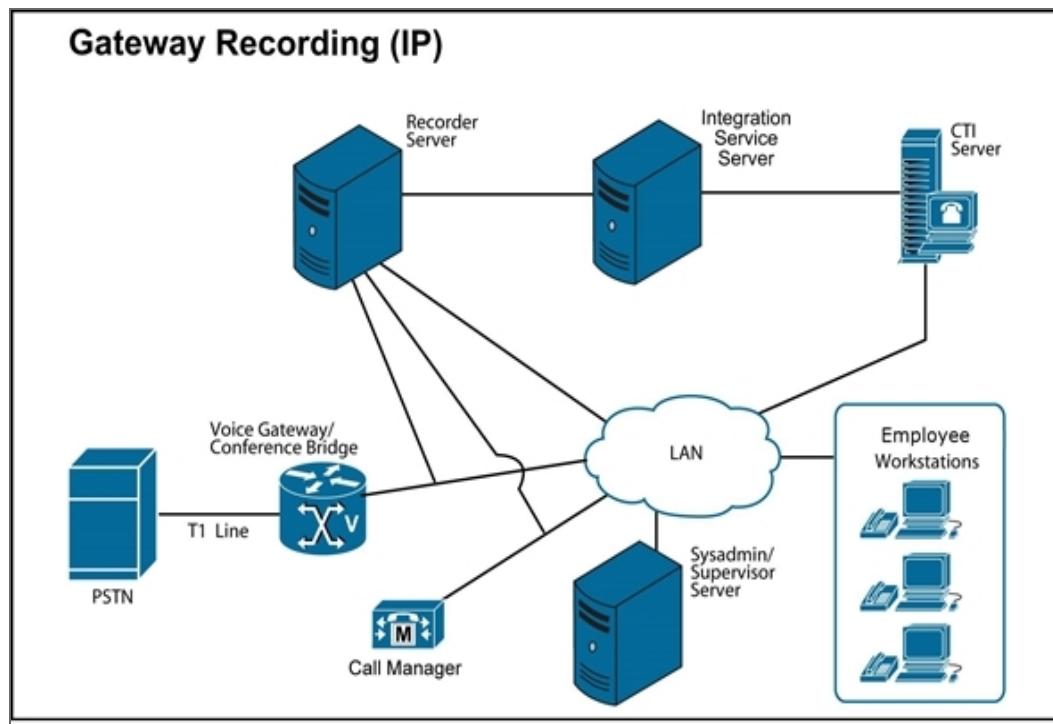
IP recording

Support for IP Recording includes Gateway and Extension-Side recording, DMS, Real-time Transport Protocol (RTP) Detection, and SIP Trunk Recording.

IP Gateway Recording

Gateway recording in IP environments can be compared to trunk-side recording in TDM environments. Configure gateway recording by SPANning the gateway and the call control server. In Cisco environments, the call control server is Call Manager. To record conference calls, any conference bridge resources/participants must be SPANned. At the same time, care must be taken to ensure that SPANning the conference bridge resources does not take the IP Recorder over the maximum number of concurrent channels for which it is configured. A possible limitation of this configuration is that it can be difficult to record employee to employee calls, since these calls do not usually go over the gateway.

The following diagram illustrates a typical gateway recording configuration.



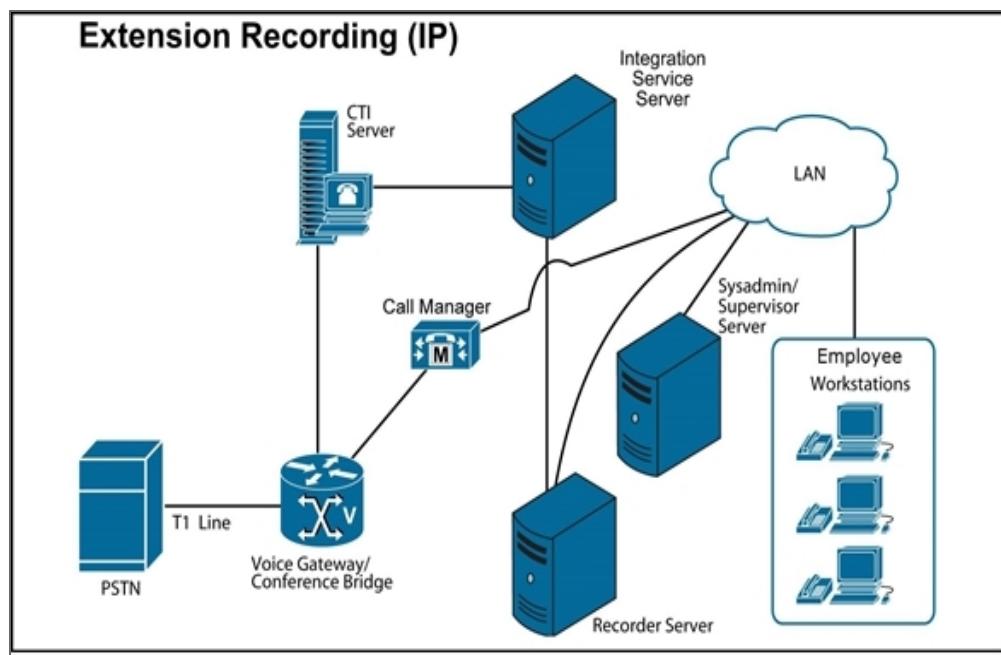
Spanning the gateway enables the Recorder to see the RTP traffic between the IP device and the gateway. When a conference is established, the RTP traffic flows between the gateway and the conference bridge, meaning that the IP Recorder cannot associate it with any device. The conference bridge must be SPANned, therefore, to enable the IP Recorder to access and record the RTP streams going to and from IP devices.

Extension-Side IP Recording

Extension-side recording in IP environments is comparable to station-side recording in TDM environments. Configure extension-side recording by SPANning (that is, copying) the traffic to and from an IP phone, typically using either port or VLAN SPANning.

SPANning the IP device itself means that the IP Recorder receives all RTP traffic to and from that device, and traffic between the device and the Cisco Call Manager Server/Cluster. In this configuration, it is not necessary to explicitly SPAN the Call Manager or any of the conference bridge resources.

The following diagram is an example of extension-side recording. In this configuration, the access switches to which the IP phones connect are SPANned directly.



DMS Recording

DMS Recording is supported in Avaya NES DMS, DMCC-driven DMS for Avaya, and the Cisco Call Recording implementation.

See the appropriate *Integration Guide* for more information.

Unified Trading Recording

Unified Trading Recording is supported. See the appropriate *Integration Guide* for more information.

RTP Detection

In IP Recording, you can use RTP detection to record calls in Recorder Controlled or CTI Controlled spanning environments (either all the time or in fallback mode).

RTP detection is always enabled in Performance mode (which prevents loss of audio due to CTI disconnection) and Liability modes (in which audio records either by CTI or VOX and as VOX in between CTI calls).

RTP detection is not supported when the RTP payload type is in the dynamic payload range of 96–127 (such as video) and for any encrypted media streams (such as Lync). Therefore, RTP detection is not supported for video recording and Lync recording.



In Load-Balanced Recorders, the RTP streams are only visible to one of the Recorders, and, therefore, only recorded on that Recorder.

Related topics

[Configure RTP detection \(page 381\)](#)

[Reference \(page 412\)](#)

Member groups

You set up the particular type of recording you require (trunk-side, station-side, and so on) by creating member groups. Member groups tie channels to Recorders, and define different groupings and their associations to Recorders, such as TDM extensions, TDM trunk spans and IP extension pools.



When you create a member group you will assign a Recorder Control Type and Fallback Type. The Integration Service uses these and other settings to determine what should be recorded and when—see “Recording Decisions” in the *Technical Overview* for more information about how these settings impact one another.



Each member group requires assignment to a recorder, which automatically assigns any Integration Service associated with the member group to the Recorder. View the relationships on the Associations page.

The types of member groups available to you depend on your specific recording configuration.

Type	Description	Settings
Compliance Station Extension Group	Used to set up extensions for TDM station side recording.	Compliance station extension member group settings for TDM (page 67)
Compliance Trunk Span	Used to simplify the management of multiple phone lines from T1 (up to 24) or E1 (up to 30) trunk spans. Trunk group members are the actual channels derived from the T1 or E1 trunk span.	Compliance trunk span member group settings for TDM (page 68)
IP Extension Pool	Used to group extensions in the IP switch or a hybrid switch that supports both IP and TDM. These groups of extensions are assigned to Recorders. Use this type of member group for DMS and for IP Interception.	IP extension pool member group settings (page 71)
Trunk Span Recording Resource	Used to represent T1 or E1 lines on TDM switches with selective recording capabilities like SO.	Trunk span recording resource member group settings (page 75)

Type	Description	Settings
Extension Recording Resource	Used to represent a list of extensions used on IP switches with selective recording capabilities like SO and SSC (for example, these extensions are used on Avaya as softphone extensions).	Extension recording resource member group settings (page 75)
Selective Extension Pool	A selective extension pool is a list of extensions to be recorded, and at least one recording resource (described above) should be associated with it (the recording resources define and perform the actual recording).	Selective extension pool member group settings (page 77)
Dedicated Extension Pool	Used with the Avaya switch for Dedicated SO (either with DMCC [IP] or TDM). Specific extensions to be recorded are statically assigned to channels (for TDM) or softphones (for DMCC/IP) and the channels or softphones will remain service observed onto the recorded extensions. A dedication extension pool must be associated with a recording resource.	Dedicated extension pool member group settings (page 78)
Multiple Registration Extension Pool	Used in Avaya DMCC environments to support multiple device registration (including support for N+N redundancy).	Multiple registration extension pool member group settings (page 79)
DMCC Recording	Used in Avaya DMCC environments to support Avaya on demand recording. Specific extensions to be recorded are statically assigned to softphones.	DMCC recording group member group settings (page 81)
Gateway Side Correlation Pool	Use this member group to record traffic at a Session Interface Protocol (SIP) Trunk. This includes environments in which SIP trunk sessions are replicated by an edge device such as Acme Packet SBC to the Recorder.	Gateway side correlation pool member group settings (page 83)
Amazon Connect	Used for recording with Amazon Connect data sources.	Amazon Connect member group settings (page 90)

Type	Description	Settings
Microsoft Teams Group	Used for recording with Microsoft Teams data sources.	Microsoft Teams Group member group settings (page 90)
AudioHook Recording	Used for recording with Genesys PureCloud data sources.	AudioHook Recording member group settings (page 92)
Streaming Media Capture Pool	Used to record real-time traffic from a Streaming Media Capture server in Avaya.	Streaming Media Capture Pool member group settings (page 93)
Stream Recording	Used for recording real-time interactions from a cloud contact center that has a real-time streaming API that uses WebHooks for delivering interactions to the Verint system. Used by Twilio Flex and Zoom Contact Center data sources.	Stream Recording member group settings (page 97)

Related topics

[Create a member group \(page 66\)](#)

[Reference \(page 412\)](#)

Multiple Recorders and high availability

A single instance of an Integration Service can support multiple Recorders either by segregating the extensions by assigning them to specific Recorders, or by sharing extensions across Recorders (in the case of load-balanced or redundant Recorders). Within your site you may deploy pairs of Integration Service servers for high availability.

When extensions are assigned to specific Recorders, the Integration Service only sends recording control messages to the Recorder assigned to a given extension through configuration.



For information about configuration for all high availability/redundancy scenarios, see the individual *Integration Guide* for the solutions in which it is supported.

Redundant Recorders

This release supports redundant Recorder configurations with Recorders for both CTI Controlled and Recorder Controlled configurations.

In a redundant Recorder Controlled IP Recorder configuration, the Integration Service can track extensions involved in a call and send tagging messages to associated Recorders.

For redundant CTI Controlled IP Recorder configurations, the Integration Service sends recording control commands in addition to tagging, as in the Recorder Controlled configuration. The Integration Service also sends commands to any Recorder associated with any extension involved in the call, as in the Recorder Controlled solution, but it is assumed that recording only takes place on the Recorders to which the audio is available.

For both Recorder Controlled and CTI Controlled configurations, you must assign extensions to Recorders to utilize the Integration Service with that Recorder, even with a Recorder that is configured to Record All.

See [Configure high availability \(page 334\)](#) for information about supported N+N and N+M configurations.

Redundant Integration Services

Paired Integration Services allow for scenarios in which a main Integration Service goes down, a backup Integration Service takes over, controlling recording and tagging. When the main Integration Service comes back up, it resumes control.

Load-Balanced Recorders

At the Recorder level, load balancing is achieved either by:

- using a load balancing device
- recording a subset of the calls
- Integration Service load balancing (in DMS configurations)

The Integration Service configuration for load-balanced Recorders is almost the same as that for redundant IP Recorders. However, in Load-Balanced Recorders the RTP streams are only visible to one of the Recorders, and, therefore, only recorded on that Recorder.

Related topics

[Reference \(page 412\)](#)

NIC teaming

NIC teaming is the process of grouping together several physical NICs into one single logical NIC, which can be used for network fault tolerance and transmit load balance.

Network Fault Tolerance

By teaming more than one physical NIC to a logical NIC, high availability is maximized. Even if one NIC fails, the network connection does not cease, and continues to operate on other NICs.

High Capacity Delivery

The High Capacity Delivery NIC is the NIC used to record calls in Duplicate Media Streamed environments. You must configure the logical teamed NIC for recording.

RFC 2003 Interception

The RFC 2003 Interception NIC is the NIC used to record traffic from Acme Packet SBC. Network traffic handling is similar to Delivery recording mode so you must configure the logical teamed NIC for recording.

Management NIC

The Management NIC is the NIC used to manage the Recorders (in other words, configuring the Recorders, archiving the recorded data and so on). This NIC is not used for recording so the limitation of not supporting “Transmit Load Balancing” network teaming option is not applicable here.

Related topics

[Reference \(page 412\)](#)

[Limitations of NIC teaming \(page 445\)](#)

Limitations of NIC teaming

Transmit Load Balancing

Balancing the network traffic load on a server can enhance the functionality of the server and the network. Load balancing within NIC teams enables the distribution of traffic amongst the members of a NIC team, so that traffic is routed among all available paths. In IP recording, no data is expected to be transmitted on the NICs used for recording, so the “Transmit Load Balancing” network teaming option is not required for the Recorder NICs and is not supported. “Network Fault Tolerance” only network teaming options are validated and are supported.

Interception NIC

The interception NIC is the NIC used to record calls from the SPAN port. In this mode of recording, a cable from SPAN port is connected to the Recorder NIC. If you want to team the NICs in this mode, you must have identical SPANS configured and connected to each of the teamed NICs. NIC teaming is not supported in Interception mode.

For screen recording, the Integration Service attempts to send screen recordings to the Recorder that is least utilized, when more than one Recorder can record that workstation.

Related topics

[Reference \(page 412\)](#)

Phones

All of the phones that you want to record are associated with a Phone data source during configuration in the Enterprise Manager. A phone has a primary extension and optional secondary extensions. To each extension, you must assign a recording mode that determines the kind of recording that can occur on the extension.

In voice recording, the recording mode and Recorder control type define what gets recorded and how—see [Recorder control types \(page 450\)](#) and [Extension recording modes \(page 429\)](#) for more information, including descriptions of the recording mode and Recorder control type settings necessary to produce the recording behavior you require.

Related topics

[Reference \(page 412\)](#)

[Extensions \(page 430\)](#)

Queues

An Automatic Call Distribution (ACD) queue allows contact centers to keep customers on hold until someone is available to take their call. To record a queue rather than a specific employee, complete the following tasks.

Workflow

1. Create a Phone Data Source—see [Create a phone data source \(page 49\)](#). Set the **Seating Arrangement** to **Free**.
2. Create a member group—see [Create a collection data source for gateway recording \(page 61\)](#). Assign the member group extensions under Group Members.
3. Add phones with both primary and secondary extensions—see [Create and edit phones/extensions \(page 125\)](#).
4. Create a Data Source Group—see [Create data source groups \(page 154\)](#). Enter the queue number as the **Data Source Group Name**. As the Type, select ACD Queue DN (QDN).
5. In Enterprise Manager, click **Employee > Profiles**. Locate the Data Source created in step 1, then enter the Employee ID in the corresponding field. Click **Save**.

Related topics

[Reference \(page 412\)](#)

Real-Time Monitor

The Real-Time Monitor (RTM) feature in Interactions allows you to monitor employee calls and screens in real time. The Integration Service provides information to the Agent Event Service (MAS) component about employee states and calls, which can then be viewed in the Enterprise Manager to be monitored live. It also starts and stops streaming by communicating with the Recorder.

RTM limitation for TDM calls

In a TDM recording environment, real-time monitor streaming is only supported when the voice cards are configured with G.711 format.

To avoid having G.711 recordings use excessive space on the Calls drive, set the post-recording compression option for G.723 or G.729. You can set the compression in Recorder Manager under General Setup > Compression.

Secure RTP (Real-time Transport Protocol)

This release supports secure RTP (SRTP) between the Recorder and certain applications.

For real-time monitoring, Cisco phones in secure mode send encrypted RTP to the recorder. The recorder decrypts the encrypted RTP, then (optionally) re-encrypts the audio using its own encryption mechanism before sending it to RTM. Playback decrypts this audio before playing.

For Playback, the corresponding release must be installed on the desktop. If the desktop client installation is not updated with the same software update, disable the Recorder encryption mechanism. Turn off the EncryptAudioOnRTMInterface setting in IPCaptureConfig.xml.

For Analytics, the Recorder decrypts the encrypted RTP before sending it along. (The native encryption provided by the Recorder for RTM does not apply to audio sent to the Real Time Analytics client, nor to the TPS client.)

Limitation

Real-Time Monitoring may not work if the web socket port for secure or non-secure connections is changed. The default port for secure connections is 29424. The default port for non secure connections is 29423.

Related topics

[Reference \(page 412\)](#)

Recorder control types

The recorder control type determines what method will be used to record extensions assigned to a given member group, and a given deployment can be a mix of any or all of the Control Types in this section.

There are seven recorder control types. The two main deployment types are CTI Controlled and Recorder Controlled. Recorder Control types apply to member groups, which define phone extensions associated with trunk groups (spans), station-side extension groups, and IP extension pools (IP only).

- **CTI Controlled** deployments are those in which the Integration Service tells the Recorder when to start and stop recording. If you are using Avaya DMCC, use this setting (see the *Avaya Integration Guide* for more details).
- **Recorder Controlled** deployments are those in which the Recorders themselves control recording, and the Integration Service is used for segmentation, stitching, and tagging purposes. In the context of an IP Recorder, recording is accomplished by a means of decoding of IP control packets, such as Skinny or SIP. In the context of a TDM Recorder, recording control is accomplished through either D-Channel detect, VOX, CAS, or line voltage (tap sense) recording, and the Integration Service provides tagging information from CTI events. If you are using IP Analyzer, use Recorder Controlled.

During a Pause, nothing is recorded. Similarly, use of the Exec Delete button will override recording according to the **Delete/Block Behavior** setting.

- Use **Selective Delivery (Duplicate Streamed)** in selective delivery recording. Specifically, in environments where the Recorder Integration Service issues requests to start recording to a third-party application. The Duplicate Stream recorder control type is available for Avaya DMCC, Avaya NES DMS, Cisco Call Recording, Twilio Flex, and SIPREC recording.
- Use **Full Delivery (External Controlled)** in compliance delivery recording. Recording is controlled by a 3rd party application, which redirects audio to the Recorder. The Full delivery recorder control type is available for Cisco DMS (where the Recording Option of the line has been set to Automatic Call Recording), Genesys SIP full Delivery, and Zoom Contact Center.
- The **Service Observe** recorder control type is available when using an Avaya or Generic switch type to support configurations in which the recorder analyzes call control messages and then uses the Service Observe functionality of the switch to record the call. *Service Observe* allows a specified user, such as a supervisor, to observe or monitor another user's calls. Use this control type in conjunction with a Trunk Span Recording Resource or Extension Recording Resource member group. For Avaya DMCC, use either this or Single Step Conference as the recorder control type.
- The **Single Step Conference** recorder control type is available when using Avaya, Alcatel, and Generic switch types. *Single step conferencing* is used to connect an in-progress call to a device. Use this control type in conjunction with a Trunk Span Recording Resource or Extension Recording Resource member group. For Avaya DMCC, use either this or Service Observe as the recorder control type.
- The **Multiple Registration Control** type is the default recorder control type for Multiple Registration Extension Pools, used in Avaya DMCC environments to support multiple device registration (including support for N+N redundancy).



In Avaya DMCC, the member groups are a combination of an Extension Recording Resource (for which you must select either the Service Observe or Single Step Conference recorder control type), and either a Selective or Dedicated Extension Pool (for which there is no recorder control type to select).

Related topics

[Reference \(page 412\)](#)

Recording resources

Trunk Span Recording Resources and Extension Recording Resources are member groups representing resources on a switch that are capable of selectively recording extensions. For example, this could be a TDM E1/T1 line capable of Service Observe in the case of a Trunk Span Recording Resource, and IP softphones/Virtual Extensions in the case of an Extension Recording Resource.

Related topics

[Reference \(page 412\)](#)

Roles

Each Recorder in your system must have a *role*. For recording purposes, there are five roles that you will be concerned with primarily.

Roles

- **Recorder Integration Service (RIS)**—To allow a Recorder or Screen Recorder to be controlled by a CTI or LAN adapter, associate it with an *Integration Service* role.
- **IP Recorder**—For IP-based audio recording.
- **TDM Recorder**—For TDM-based audio recording.
- **Screen Recorder**—For screen recording.
- **Recorder Adapter Proxy Service**—By deploying multiple Recorder Adapter Proxy Service (RAPS) nodes on servers that are separate from the Recorder Integration Service, customers can achieve horizontal scaling of the SIP/SIPREC interfaces.
- **Content Server**—Provides a Web Service to allow external applications to retrieve recorded files from an Recorder, including files stored on Archive.
- **IP Analyzer**—IP Analyzer spans IP traffic from an IP data source and distributes the traffic to designated gateways and Recorders. This role applies only to IP recording and must be associated with an IP Recorder Server Role.
- **Central Archive**—To allow any combination of Recorder types to participate in an archive system where all archived calls are located in one, central location, associate the Recorders with a Centralized Archiving Server role. Refer to the *Centralized Archive Management Installation and Configuration Guide* for more information.

Server role restrictions

- Recorder Integration Service can be associated only with the TDM, IP, or Screen Recorder roles.
- Centralized Archiving can be associated only with TDM, IP, Screen, or External Server roles.
- IP Analyzer cannot be associated with Recorder Integration Service.
- You cannot change the associations of secondary roles.

Changing and managing roles

To change or manage roles within your recording system after initial setup, click **System Management > Settings**, select a Recorder and then click **Associations**. Use the check boxes to associate the nodes list on the right with a node selected on the left.

Related topics

[Reference \(page 412\)](#)

RTP detection

See [IP recording \(page 438\)](#).

Related topics

[Reference \(page 412\)](#)

Screen Recording

The easiest way to trigger screen recording for all calls or a percentage of calls is by using Recording Rules. You can also use AIM, or external commands by means of the Integration Service.

To configure screen recording, you must create LAN data sources, Workstation Groups, and Workstations. LAN data sources are assigned to Integration Services and Workstation Groups are assigned to Screen Recorders. Workstation screens are recorded on one of the assigned Screen Recorders, which is associated to its Workstation Group. You can also create subnets for recording range of workstations whose IP Address matches the subnet criteria. For screen recording with audio, you must also create a phone data source (for screen-only recording, it is only necessary to create a LAN data source).

To record screens, you must build the relationship between a Workstation, Extension, and optionally an Employee. For Static Workspaces, you can assign the workstation to an extension and the opposite way directly. For Dynamic Workspaces, you must use the Employee to build the workstation and extension relationship. Use the Dynamic Workspace mechanism to record workstations belonging to subnets. When you use subnets, you do not need to create individual workstations.

Static/Dynamic Workspaces

A ‘workspace’ refers to the conceptual entity of a phone tied to a workstation. You can configure your phones and workstations such that this association is either static, or created dynamically during login.

A *static workspace* is one in which the association between a phone extension and a workstation is established during the configuration in Enterprise Manager. The association occurs through one of the following methods:

- Associating a workstation with a Phone Data Source/Extension when configuring the workstation under the LAN data source.
- Associating a LAN data source/workstation with the phone extension under the Phone Data Source.

In *dynamic workspaces*, associations between phone extensions and workstations are built dynamically. To build the phone extension and workstation relationship dynamically, assign the Phone Extension or Phone Employee ID and Workstation or Workstation Logon ID to an Employee. Assign these values to Employees depending on the environment and source of available logon events. If the phone has a logon/logoff events source, then assign a Phone Logon ID to the Employee, otherwise assign a phone Extension to the Employee. If the workstation has a logon/logoff events source, assign Workstation Logon ID to the Employee, otherwise assign a Workstation to the Employee. For workstations that are covered under a subnet IP address range, assign the Workstation Logon ID to the Employee.

See also [Seating arrangements \(page 458\)](#).

Static/Dynamic Workstations

A workstation is called a Static Workstation when its name is used to build the relationship with Phone Extension. When the static workstation is used, you can either associate it directly to a Phone Extension (in this case it is a Static Workspace) or assign the Workstation name to Employee (in this case, the relationship to the Phone extension is built dynamically). Next, assign the Phone Extension

or Phone Logon ID (whichever is required) to the Employee. Workstation Windows Logon ID is not used in the Enterprise Manager configuration.

A workstation is called a Dynamic Workstation when its Logon ID is used to build the relationship with Phone Extension. When the Dynamic Workstation is used, you must assign the Workstation Windows Logon ID to the Employee (in this case, the relationship to the Phone extension is built dynamically). Next, assign the Phone Extension or Phone Logon ID (whichever is required) to the Employee. Dynamic workstations are matched against subnet ranges through the Windows Logon ID. The Capture Service running on the computer of the Employee sends the logon/logoff messages to Integration Service automatically when the Employee logs on and off the computer. The Capture Service on the employee computer must be configured with the Integration Services server name or IP address and port number. Separate LAN data sources can have overlapping subnet ranges if, and only if, the configured Windows Logon IDs are unique among the data sources. The dynamic workstation is created on the data source with the matching Windows Logon ID.

See also [Seating arrangements \(page 458\)](#).

After Call Work

Within your recording rules, you can specify whether you want to capture employee desktop activity after a call ends. See [Create a recording rule \(page 305\)](#).

Playback

In addition to viewing captured screen activity when replaying a contact, playback also shows color-coded frames under different conditions:

- Black screen: Employee paused screen recording. The black frame continues to display during playback until the employee resumed screen recording.
- Green screen: No data to display. No data occurs when an issue with screen recording occurred and there are no data to display. The green screen continues to display until data are available.

Selective Screen Application Recording

Selective Screen Application Recording allows you to specify the applications and URLs on the agent screen that will be recorded or will not be recorded. Applications and URLs on the agent screen that are not recorded display in gray.

Screen Recording in Non-CTI Environments

Screen recording in non-CTI environments is supported for both IP and TDM Recorders. This functionality is supported by default but you must specify rules to trigger recordings using select attributes.



This release does not support screen recording in trunk-side TDM environments without CTI.

The behavior of this feature is different depending on the type of Recorder, TDM or IP:

- **Station-Side TDM Recording Environments:** In station-side TDM recording environments, there can be latency between the time recording starts and the time the recording rule is triggered to

start screen recording.

- **IP Recording Environments:** In some IP environments (for example, Avaya Passive IP), the IP Recorder sends multiple start and stop recordings for a single call. This case results in multiple segments appearing in the Interactions application, since there is no way to distinguish one start message from another. There is one screen recording segment for each STARTED message sent by the Recorder.

Recording Rules and Screen Recording in Non-CTI Environments

Create one or more recording rules to trigger screen recording in non-CTI environments. You can use a recording rule based on Event Type Begin_Call or based on Extension. In addition, you can also use a recording rule based on Recorder attributes. The attributes available for use in recording rules depend on whether it is a TDM or IP Recorder environment.

Related topics

[Reference \(page 412\)](#)

Seating arrangements

The following describes the types of employee seating arrangements. The employee seating arrangement can be Fixed, Free, or Hybrid.

Seating arrangements

- With *fixed seating*, an employee has a permanently assigned workstation and the Workstation name is used to build the relationship with the Phone Extension.
- In a *free seating* arrangement, employees do not have permanently-assigned workstations. They are assigned a unique Windows Logon and can log in from any location in the call center. Assign the Windows Logon ID and assign the Phone Extension or Phone Logon ID, whichever is available and preferable, to the Employee in order to build the workspace dynamically.
- Hybrid seating* refers to an arrangement in which some employees are using free seating and some are using fixed.

Related topics

[Reference \(page 412\)](#)

Selective extension pools

A Selective Extension Pool is the list of extensions to be recorded, and you associate them with Trunk Span Recording Resources and Extension Recording Resource member groups to perform the recording. The number of configured phones (among primary extensions only) must not exceed the number of recording resources.

Related topics

[Reference \(page 412\)](#)

Shared screen Recorders

Shared screens refer to environments in which you have a group of screen Recorders that are treated collectively as a pool of screen recording resources. The screen Recorders are all associated with the same Integration Service.

Related topics

[Reference \(page 412\)](#)

Shared lines

A shared line phone is one in which a single extension is associated with several devices (each could also have a unique extension of its own). Support for recording shared lines is included in this release.



Real Time Monitor is not supported for shared lines on phones without unique DNs.

Related topics

[Reference \(page 412\)](#)

SIP trunk recording

A Session Initiation Protocol (SIP) trunk is a logical connection between an IP PBX and a service provider's application server that allows voice over IP (VoIP) traffic to be exchanged between the two.

To deploy SIP trunks you need the following components:

- PBX with a SIP-enabled trunk side
- a SIP-compatible enterprise edge device (this can either be a firewall with complete support for SIP, or an edge device connected to the firewall handling the traversal of the SIP traffic)
- and Internet Telephony Service Provider (ITSP) or SIP trunking service provider

When a call is placed from an internal phone to an external number, the PBX sends the necessary information to the SIP trunk provider, who establishes the call to the dialed number and acts as an intermediary for the call. All signaling and voice traffic between the PBX and the provider is exchanged using SIP and RTP protocol packets over the IP network.

If the called number is a traditional PSTN telephone, the trunk provider routes the IP packets to the PSTN gateway that is closest to the number being called, to minimize possible long distance charges. The provider can also terminate PSTN numbers, and route incoming calls for those numbers back to the IP PBX over the SIP Trunk. This allows businesses to offer local phone numbers in several geographical areas, but service them all from a single location.

If the called number can be reached over a SIP Trunk, the call does not need to be routed over the PSTN, but can instead be carried on the IP network end-to-end, creating a very cost-effective solution. SIP trunking can also serve as the starting point for the entire breadth of real time communications possible with the protocol, including Instant Messaging, presence applications, white boarding and application sharing.

The SIP trunk can be provided by the Internet Service Provider (ISP), or by an independent ITSP. In fact, there can be several parties involved, each one providing a different part of the service required to deliver end-to-end communication.

Because a SIP trunk is not a physical connection, there is no explicit limit on the number of calls that can be carried over a single trunk. Each call consumes a certain amount of network bandwidth, so the number of calls is limited by the amount of bandwidth that can flow between the IP PBX and the provider's equipment.

Implementation

The Recorder records traffic at the SIP Trunk. This includes environments in which SIP trunk sessions are replicated by an edge device such as Acme Packet™ SBC to the Recorder.

The way in which traffic is provided to the Recorder depends on the spanning/replication mode. In SIP Trunk Recording, the edge device provides the Recorder with both signaling and audio; in this case, the signaling does not carry the employee's extension. SIP Trunk Recording is therefore established at the member group level (not at the extension level). A SIPREC adapter created in Recorder Manager allows the retrieval of custom tags from SIP headers or SIPREC metadata.

You may have multiple data sources in environments in which there are multiple tenants (contact centers) hosted on separate switches, and each tenant is identified by a unique switch IP address.

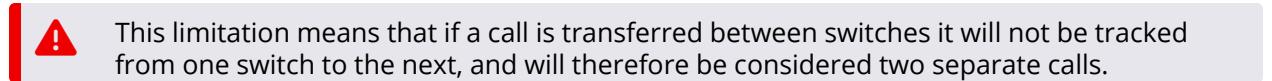
Each switch requires its own Phone data source, with the switch IP address or host name configured as the call center's SIP trunk interface. The **Server Type** under **Settings > Device Configuration**

should be set to **PSTN Side - Far End**. The Recorder uses this IP address or host name to identify the data source and tag it to the recordings. The Recorder Integration Service uses the data source tagged to the recordings to then match it to relevant CTI.

For configuration details see [Gateway side correlation pool member group settings \(page 83\)](#), and the Avaya or Genesys *Integration Guide*. (You may have multiple data sources that use this member group type, but only one member group per data source.)

Limitations

Calls are not tracked across data sources, and therefore are not tracked across different switches.



This limitation means that if a call is transferred between switches it will not be tracked from one switch to the next, and will therefore be considered two separate calls.

Support

SIP Trunk Recording works with all of the following recording features and modes, and no special configuration:

- Application, Performance and Liability Recorder Fallback Types
- Shared Interception and Dedicated Interception Load Balancing Types
- VOX Fallback
- Redundancy
- Screen Recording
- Recording in SIP and TDM mixed trunk environments
- Recording SIP trunk traffic from multiple PBX/ACDs
- Option to stop recording when the Customer is put on hold

Related topics

[Reference \(page 412\)](#)

Subnets and subnet masks

Remote client nodes typically connect over a VPN or from behind a NAT. When creating a subnet configuration to capture these client nodes, you need to know which path the client node will take.

A client connecting over a VPN typically has more than one (1) IP address defined, but can connect through the VPN IP address. To capture client nodes connecting through a VPN, create a subnet configuration representing the VPN IP address range.

Client nodes connecting through a NAT typically have only one (1) IP address defined. To capture client nodes behind a NAT, create a subnet configuration representing the internal (usually private) IP range.

Work with the site IT network administrator to obtain appropriate subnet and subnet mask settings that cover the range of IPs to be recorded.

Sample configurations

- Subnet 10.56.2.0 (Network address/Subnet ID)

Subnet Mask 255.255.255.0

In this configuration, the Starting Host is 10.56.2.1 and the Ending Host is 10.56.2.254 (a total of 254 workstations).

- Subnet 10.56.2.0 (Network address/Subnet ID)

Subnet Mask 255.255.255.224

In this configuration, the Starting Host is 10.56.2.1 and the Ending Host is 10.56.2.30 (a total of 30 workstations).

- Subnet 10.56.2.32 (Network address/Subnet ID)

Subnet Mask 255.255.255.224

In this configuration above, the Starting Host is 10.56.2.33 and the Ending Host is 10.56.2.62 (a total of 30 workstations).

Related topics

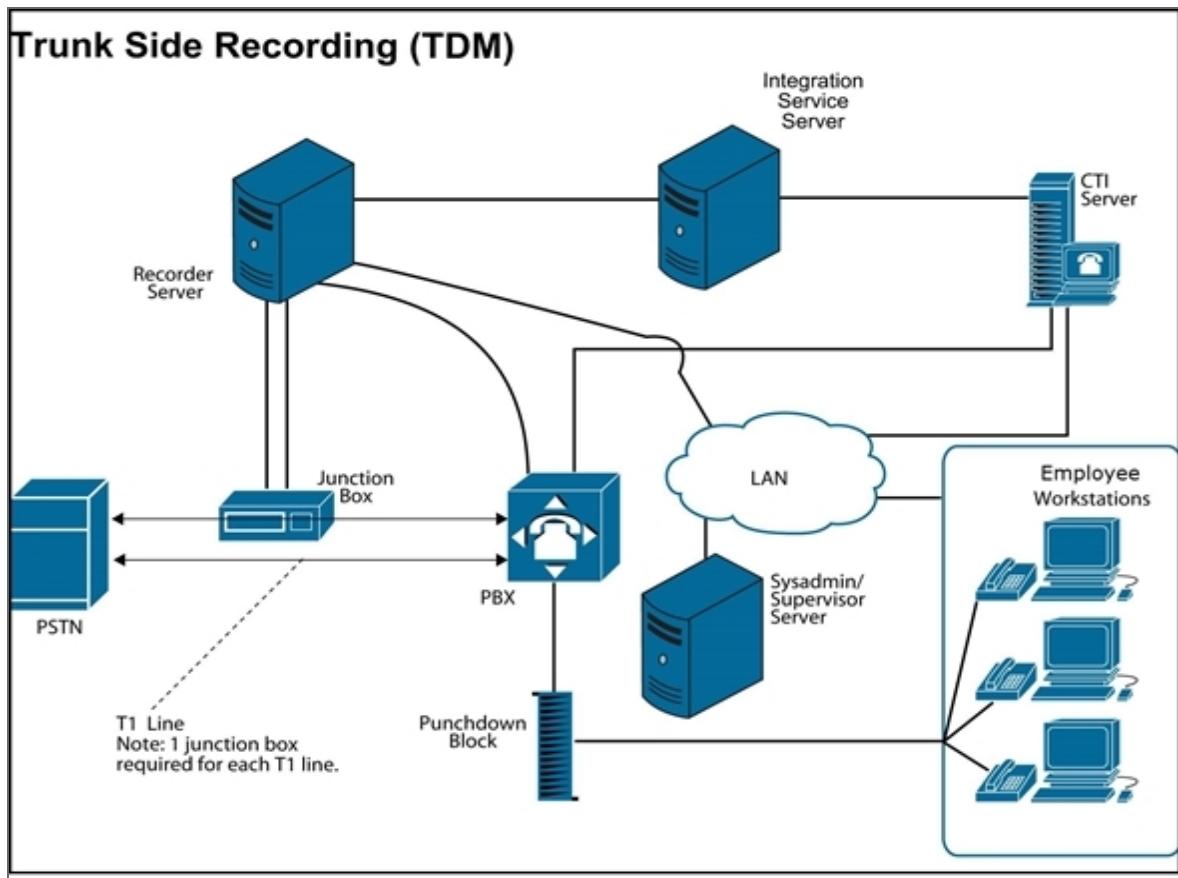
[Reference \(page 412\)](#)

TDM recording

The recorder supports four types of TDM recording: Trunk-Side, Station-Side, Service Observe, and Single Step Conference.

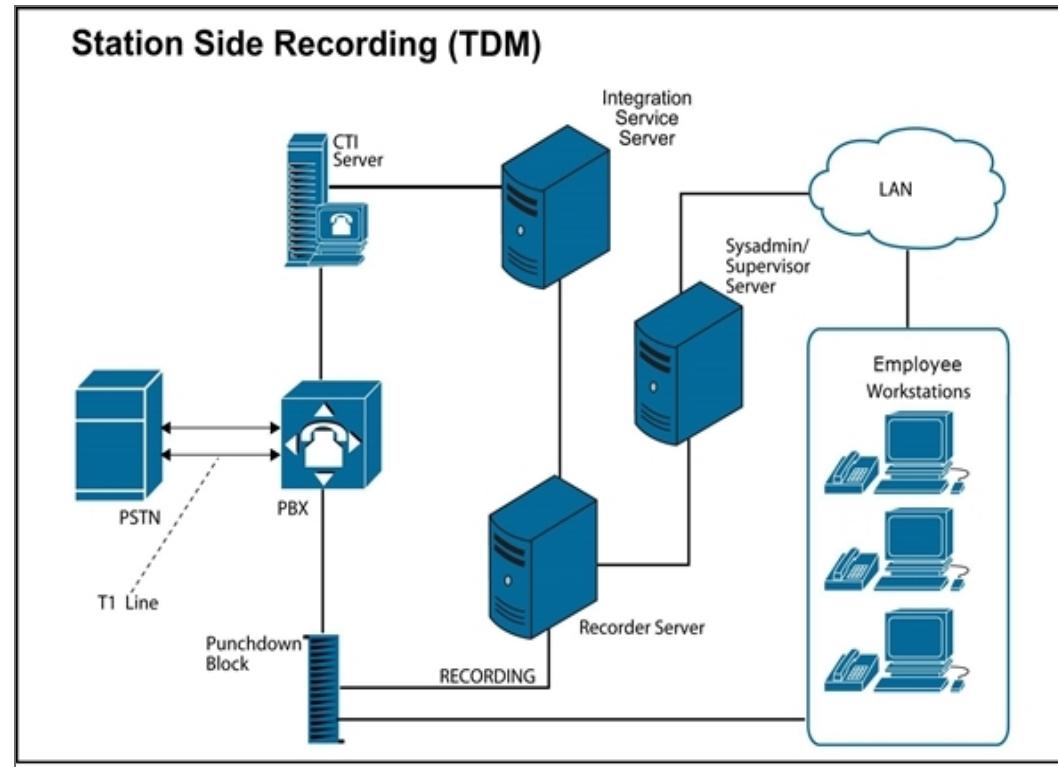
TDM Trunk-Side Recording

In TDM environments, trunk-side recording taps directly into a T1 or E1 line to record all incoming calls at the demarcation point before going to a switch. Passive tap trunk-side recording requires a physical connection directly between the demarcation point and the switch system. The following diagram illustrates a typical passive tap trunk-side configuration scenario within a Call Center environment.



TDM Station-Side Recording

In TDM environments, station-side recording is initiated between the switch/ACD and a phone. This is done by tapping into the line that connects the switch to the telephone using a punch-down block. A cable is installed so that each extension connects directly to a port on the voice card. The following diagram illustrates a typical passive tap station-side configuration within a Call Center environment.



Service Observe

The recorder can use Service Observe to monitor an agent's extension, thereby allowing a specified user, such as a supervisor, to observe or monitor another user's calls. The recorder can monitor an agent's extension using service observe. You will need to configure Trunk Span Recording Resource Member Group Settings to represent T1 or E1 lines the TDM switches, or Extension Recording Resource Member Group Settings for IP recording.

Single Step Conferencing

Single step conferencing is used to connect an in-progress call to a device. You will need to configure Trunk Span Recording Resource Member Group Settings for TDM, or Extension Recording Resource Member Group Settings for IP recording.

Related topics

[Reference \(page 412\)](#)

[Trunk span recording resource member group settings \(page 75\)](#)

[Extension recording resource member group settings \(page 75\)](#)

Trunk span groups

Create a trunk group to simplify the management of multiple phone lines from T1 (up to 24) or E1 (up to 30) trunk spans so that you can create numerous unique phone extensions. Trunk group members are the actual channels derived from the T1 or E1 trunk span.

You can create trunk groups and trunk group members from more than one switch and from more than one span per switch. For example, you could create three trunk member groups from two trunks spans, with trunk group members consisting of a combination of channels/phone lines from each trunk span.

Related topics

[Reference \(page 412\)](#)

[Compliance trunk span member group settings for TDM \(page 68\)](#)

Video stitching of separate recordings

Recorded video for a single interaction can be stored in the system as separate video recordings. Separate recordings are a result of the configuration settings of the **IP Recorder Video** server role. The settings determine the maximum size and recorded length for each segment of video.

During playback, video segments are combined or "stitched" together in the order they were recorded to create a single MP4 video interaction file for playback and review. Usually, the transition from one recorded segment to another during playback is transparent to users.

Segment overlap

Because video recording is segmented, it is possible for the end of one recording to duplicate the beginning of the next segment. In such cases, during playback duplicated video from the previous segment is discarded and replaced with the video from the next segment.

Time gaps between segments

Alternatively, segmentation can also result in a short gap in time between video segments. In such cases, during playback the system will display to users a still video frame until the gap has elapsed.

Stitching and third-party media players

Stitching is supported only when replaying video using the suite. Stitching is not supported when using third-party media players, such as Windows Media Player and VLC media player. The third-party player may replay separate segments, but not as a continuous contact and only the first segment will correctly display the video.

Related information

IP Recorder Video role settings (*Enterprise Manager Configuration and Administration Guide*)

Workstations and workstation groups

Within your network, workstations on which you want to implement screen recording are known as LAN data sources. Whereas you configure Phone switches for recording telephone calls, you set up the LAN as the Data Source for creating and tracking employee workstations for recording screens within those screens, by creating workstations and groups of workstations in both IP and TDM environments.

Multiple integration services can be associated with one LAN. You may wish to do this to support a large number of workstations, or if you need to segregate the configuration of different business units or locations.

Related topics

[Reference \(page 412\)](#)

Administration

The following sections describe tasks that are not necessarily part of initial Recorder setup, but you may need to perform as part of ongoing administration.

Topics

Administer the Recorder	471
Export and Import Data Source Settings	478

Administer the Recorder

Administering the Recorder includes making updates to workstations and creating filters to view specific data.

Related topics

[Manage Workstations \(page 471\)](#)

[Create View Filters \(page 474\)](#)

Manage Workstations

The following sections describe administrative tasks related to workstations:

- [Edit and Batch Update Workstations \(page 471\)](#)
- [Edit Multiple Workstations \(page 472\)](#)
- [Batch Update Workstations \(page 472\)](#)

Edit and Batch Update Workstations

Edit Workstations to make changes to an existing Workstation's Host Name, Platform, Domain, Workstation Group, Phone Data Source, and Extension. Only if you edit a single Workstation does the description field display. You update Workstation subnets separately.

Procedure

1. Click **Recording Management > Data Sources > Settings**, and then select a LAN (Screen) Data Source.
2. Click **Workstation**, select two or more Workstations, and then click **Edit**.
In a multi-tenant enabled environment, the tenant to which the selected data source is associated displays in parentheses in the screen heading. An organization belongs to a tenant. When a data source is associated to an organization, the screen heading displays the tenant to which the organization belongs. The data source can be associated to a particular tenant or have the **Shared** status. A data source associated to a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.
3. Do one of the following:
 - If you chose to edit a single Workstation, type in or choose new values as described in [Define workstations \(page 112\)](#) or [Create subnets \(page 114\)](#) and then click **Save**.
 - If you selected two or more Workstations, complete the fields as described in [Edit Multiple Workstations \(page 472\)](#).

Related topics

[Edit Multiple Workstations \(page 472\)](#)

[Batch Update Workstations \(page 472\)](#)

Edit Multiple Workstations

Use the following procedure to edit multiple workstations at once. When you edit more than one Workstations, Description fields do not display.

Procedure

1. Click **Recording Management > Data Sources > Settings**, and then select a LAN (Screen) Data Source.
2. Click **Workstation**, select two or more Workstations, or click **Select All**, and then click **Edit**. The List of Workstations appears.
3. Complete the fields as described in [Define workstations \(page 112\)](#) or [Create subnets \(page 114\)](#) and then click **Batch Update**.
4. Complete the Batch Update window as described in [Batch Update Workstations \(page 472\)](#), and then click **Save**.

Related topics

[Edit and Batch Update Workstations \(page 471\)](#)

[Batch Update Workstations \(page 472\)](#)

Batch Update Workstations

Use the following procedure to update multiple Workstations at the same time.

Procedure

1. Click **Recording Management > Data Sources > Settings**, and then select a LAN (Screen) Data Source.
2. Click **Workstation**, select two or more Workstations, and then click **Edit**.
3. Click **Batch Update**.
4. Complete the following fields in the **Batch Update** window:

Item	Description
Platform	Shows the platform for this Workstation. Options are Windows (the default), OS/2, Remote Terminal , and Windows Terminal Server . If you select Remote Terminal, the Workstation Group field is disabled. If you select Windows Terminal Server, the phone Data Source and Extension fields are disabled.
Workstation Group	Choose an existing Workstation Group for the selected Workstations.
Domain	Type the domain, such as an IP address or network path, to which the selected Workstations are to belong.

5. Click **Batch Update** to update the selected Workstations and close the Batch Update window.
6. Click **Save**.

Related topics

[Edit and Batch Update Workstations \(page 471\)](#)

[Edit Multiple Workstations \(page 472\)](#)

Create View Filters

The following describe how to filter the views on various pieces of information throughout Enterprise Manager:

- [Create and Edit Employee Filters \(page 474\)](#)
- [Create and Edit Phone Filters \(page 475\)](#)
- [Filter the Workstations View \(page 476\)](#)

Create and Edit Employee Filters

Use the following procedure to create filters to help you search large numbers of employees, or to search for specific subsets of employees. You can also set a filter as the default filter.

Procedure

1. In Enterprise Manager, go to **Recording Management**, under **Data Source**, click **Settings**.
2. Select a Phone, Application, LAN (Screen), Radio, or Trader Data Source.
3. Under **Employees > Add Employee Mapping**.
4. In the View area of the window, click **Create Filter** or click **Edit Filter**.
5. In the upper left pane, select the organization(s) to filter. Selecting an organization automatically selects all its sub-organizations.
6. In the lower left pane, select a time frame for the filter:

Item	Description
Now	The active Organization, Supervisor, Rank, Employees currently in adherence. For most filter fields, this setting is the same as Today.
Today	From the current time to 24 hours ago. For the filter field Adherence Status, Today means "different than now," so all employees who were out of adherence in the last 24 hours would be returned.
Viewing Context	The date range selected in the work pane is used to evaluate the filter. The filter is dynamically evaluated and the list of employee is refreshed if it changed when the date range in the work pane changed. In screens that do not have this feature enabled or where the work pane does not have a date or date range, the filter is evaluated using the option Now.
Last X days	From the current time to X 24 hour periods ago. This options is useful for scheduled reports when you want a moving time window.
Time Window	Select the applicable date range. For example, if the filter field is Organization, the filter return any employee who was a member of that organization at any time within the specified time window.

7. Complete the Name/Value area (right pane). For each item you want to filter by, type a value or make a selection from the drop-down menu. The menus contain only information applicable to the selected organization(s). If you change the organization, the data is refreshed.
8. Click **Default Filter** to display this filter automatically the next time you log in.
9. Save by doing one of the following:
 - Click **Save As**, and then type a name. This creates a filter with a new name.
 - Click **Save** to save the filter and return to the previous page.

Related topics

[Create and Edit Phone Filters \(page 475\)](#)

[Filter the Workstations View \(page 476\)](#)

Create and Edit Phone Filters

Create or edit a filter to control how phone extensions are sorted on the Phones screen.

Procedure

1. Click **Recording Management > Data Sources > Settings**, select a phone data source, and then click **Phones**.
2. Click the drop-down box beside **View**, and then click **Create Filter** to create a new filter, or click **Edit Filter** to edit a selected filter.
3. Complete the following fields:

Item	Description
Primary Extension Name	Type the primary extension number, including a case-insensitive prefix or suffix, such as 3344, or X3344, or X3344A. For example, if you have 1000 Workstations and do not wish to scroll through 50 pages of extensions, you could add a filter such as blue to the name. Wildcards are permitted, as in the following examples: 33* = any extensions that start with 33 *33 = any extensions that end with 33 *33* =any extensions containing 33 If you enter invalid characters, a message appears.
Recording Mode	Choose an extension recording mode as described in Extension recording modes (page 429) .
LAN (Screen) Data Source	Choose the LAN (Screen) Data Source to which the extension being filtered is to be associated.
Workstation Name	Type the name of the Workstation to be associated with the phone filter.
Member Group	Check all Member Groups to be associated with the phone filter.

Item	Description
Default filter	Check Default filter to apply the displayed filter to all phones. Whenever the page is opened after logging in, all phones will be displayed according to the default filter. If Default filter is not checked, then the All filter is applied at the next log in. While flipping between tabs in Enterprise Manager, the currently selected view is remembered in the Phones window, regardless of the default filter selection.

4. Do one of the following:
 - Click **Clear** to remove all information from the fields and start a new filter.
 - Click **Save** to save the displayed information under the name of the current filter.
 - Click **Save as** to save the displayed filter information under a new name.

Related topics

[Create and Edit Employee Filters \(page 474\)](#)

[Filter the Workstations View \(page 476\)](#)

Filter the Workstations View

Use the following procedure to filter the workstations view according to specific criteria. To view all Workstations, clear the filter.



You can apply only one filter. Filters are per data source per user: if you delete the data source or user, filters are also deleted.

Procedure

1. Click **Recording Management > Data Sources > Settings**, choose a LAN (Screen) Data Source, and then click **Workstations**.
2. In the Workstations window, click dropdown list next to **View**, and then click **CreateFilter** to create a new filter, or click **Edit Filter** to edit a selected filter.
3. Complete the following fields:

Item	Description
Filters	Shows All if this is the first Workstation filter being created, or shows the currently selected filter if it is being edited.
Host Name	Type the network name or IP address of the Workstations to be filtered. You can use wildcards, as in the following examples: WS* = any Workstation that start with WS *WS = any Workstation that end with WS *WS* =any Workstation containing WS If you enter invalid characters, an error message appears.
Domain	Type the network domain of the Workstation.

Item	Description
Phone Data Source	Choose the phone switch (Data Source) from the list.
Extension	Type the extension. If you have multiple extensions, separate them with a semicolon.
Workstation Group	Check all the Workstation Groups to which the Workstation belongs.
Default filter	Check Default filter to apply the displayed filter to all Workstations. Whenever the page is opened after logging in, all Workstations will be displayed according to the default filter. If Default filter is not checked, then the All filter is applied at the next log in, and all Workstations display. While using Enterprise Manager, the currently selected view is remembered in the Workstations window, regardless of the Default filter selection.

4. Do one of the following:

- Click **Clear** to remove all information from the fields in the filter window and start a new filter.
- Click **Save** to save the displayed information under the name of the current filter.
- Click **Save as** to save the displayed filter information under a new name.
- Click **Delete** to delete the selected filter(s). Filters are not shared between users, and are available only to the current logged in user.

Related topics

[Create and Edit Employee Filters \(page 474\)](#)

[Create and Edit Phone Filters \(page 475\)](#)

Export and Import Data Source Settings

You can export and import the configuration of Phone, Application, LAN (Screen), Radio, or Trader Data Sources from an external file that was exported from another source. The format of the imported files must conform to requirements for Data Source import formats.

You may wish to use this feature if you have a large number of extensions in your enterprise. You can create a data source in Enterprise Manager, export the data source settings, then copy, paste, and edit within the .csv file to create multiple member groups and associated extensions, finally importing the new file back into your system.

 If you export Data Source settings that are associated with a Recorder that has no serial number, then the settings can not be re-imported, as a Recorder with no serial number is considered unlicensed.

 Select a data source before selecting the **Import** button—otherwise the import schedule options are limited to an immediate import.

Related topics

[Export Data Source Settings \(page 478\)](#)

[Import Data Source Settings \(page 479\)](#)

[Review the Status of Data Source Imports \(page 480\)](#)

[Delete a Data Source \(page 482\)](#)

[Import formats for data sources \(page 556\)](#)

Export Data Source Settings

Use the following procedure to export data source settings.

Procedure

1. In Enterprise Manager, go to **Recording Management**, under **Data Source**, click **Settings**.
2. Select a Phone, Application, LAN (Screen), Radio, or Trader Data Source.
3. Click **Export**.
4. Click **Save as** and select a location for the CSV file.

 If data source groups are present, this information is automatically exported, and will appear at the end of the file.

5. To add or change settings, edit the file, then save it.

Example:

You want to add member groups to the data source. A member group in the exported .csv file looks like the following:

```
Multiple Registration ExtensionPool, Multiple Reg Pool1, This has  
all the agents extensions in ATL, OnCTIDisconnection,"{326001}",  
RETAIN
```

The above will create a Multiple Registration Extension Pool with the name "Multiple Reg Pool1" and a Recorder Fallback Type of "On CTI Disconnection". It associates the dedicated server with a serial number of 326001 to this pool, and discards all abandoned CTI.

You can then replicate this entry in the file (or any other settings you require, including extensions), edit as required, then import the modified file.

Related topics

[Import Data Source Settings \(page 479\)](#)

Import Data Source Settings

Use this procedure to import a file containing the data source settings. The maximum file size you can import is 40 MB.

Procedure

1. In Enterprise Manager, go to **Recording Management**, under Data Source, click **Settings**.
2. Select a Phone, Application, LAN (Screen), Radio, or Trader Data Source.



Select a data source before you click the Import button—otherwise the import schedule options will be limited, allowing only an immediate import.

3. Select **Import**.

4. In the **Import Data Source Settings** window, complete the following fields:

Item	Description
Import Name	Give this import operation a name. This name is required when scheduling an import, but optional for an immediate import.
Import File Location	Click Browse , and then navigate to the directory where the file (to be used for the import scheduling) is located.
Schedule Type	Select one of three schedule types: <ul style="list-style-type: none"> • Import Immediately causes the import to take place immediately. No other entries are required. • Import Using Date and Time Within the File causes the import to take place on a scheduled basis at a time specified within the file, according to the choice of Local Time Zone or Universal Time Zone fields. • Import Using Specified Date and Time causes the import to take place on a scheduled basis on a date and time specified in Specify In and Date/Time fields.
Specify In	Check one of two time zone options if you selected a scheduled import (that is, a Schedule Type other than Import Immediately): <ul style="list-style-type: none"> • Local Time Zone causes the scheduled import to occur at the local time, so that, for example, imports would be made at different times across the globe. • Universal Time Zone causes the import to take place at a time relative to a universal time so that, for example, imports would be made at the exact same time all across the globe.
Date/Time	Shows the date and time of the import if ImportUsing Specified Date andTime is selected as the Schedule Type .

5. Click **Import**.

Related topics

[Export and Import Data Source Settings \(page 478\)](#)

[Import formats for data sources \(page 556\)](#).

Review the Status of Data Source Imports

Use the following procedure to review the status of scheduled, pending, failed, or completed data source imports from .csv files.

Procedure

1. In Enterprise Manager, go to **Recording Management**, under **Data Source**, click **Settings**. Click **Recording Management > Data Sources > Settings**.

2. Select a Data Source and click **Import Status**.

In a multi-tenant enabled environment, the tenant to which the selected data source is associated displays in parentheses in the screen heading. An organization belongs to a tenant. When a data source is associated to an organization, the screen heading displays the tenant to which the organization belongs. The data source can be associated to a particular tenant or have the **Shared** status. A data source associated to a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

3. Click the **View** menu, and choose the imports you wish to review from the following options:

Item	Description
Scheduled Import	All Data Source import jobs that are scheduled to run at a future time.
Pending	Scheduled import jobs that are currently in progress.
Failed	Import jobs that have not succeeded, allowing you to take corrective action.
Completed	Successful import jobs that are complete.
All	All import jobs, including manual, scheduled, pending, failed and completed.

4. The Data Source import status window lists the following information:

Item	Description
Job Name	The name of the import operation, as assigned by the person who created the import operation. This is different from the filename.
Status	The status of the import operation. Options include Complete, Pending, and Failed.
Detail	Details of the import for statuses other than complete.
Scheduled Date	The date when the import was scheduled. If the import type is Immediately, as described in Export and Import Data Source Settings (page 478) , this date is the same as Start Time (below).
Source	The source file location, if applicable. This field does not show if the status of the import is completed.
Start Time	The date and time when import started.
End Time	The date and time when the import finished.
User	The user name of the user who initiated the import.

5. Do one of the following:

- Click the **Configuration Checker** icon to view any configuration problems detected.
- For imports with a status of **Failed**, take the necessary corrective action.
- Click **Refresh Rate** to show a list of refresh rate time options. Default is one minute, which

means that the Server will check for Data Source import updates every minute.

- Delete imports with a status of **Completed** as necessary.

Delete a Data Source

Delete a Data Source to remove the Data Source from the Data Source Settings window and thereby disassociate the Data Source with the Integration Service.

Procedure

1. In Enterprise Manager, go to **Recording Management**, under **Data Source**, click **Settings**.
2. Select the data source you want to delete.
3. Select **Delete Data Source**.
4. In the **Delete Data Source Confirmation** prompt, review the message regarding deleting the data source. If you still want to delete the data source, in the **Delete Data Source Confirmation** prompt, select the check box and click **Delete**.

Related topics

[Export and Import Data Source Settings \(page 478\)](#)

System status, logs, and alarms

This following sections describe the troubleshooting tools available for the Recorder.

Topics

Recorder and component status screens	484
System logs	511
Alarms	515

Recorder and component status screens

The Recorder Status area in Recorder Manager provides a visual update on how the Recorder and its components are working. You can view statistics on general Recorder settings or one of the other areas (Capture, Integration Service, and “Other”, which includes information about Archive, database consolidation, disks, NIC cards, and Compressor). The components that appear depend on which are installed (for example, if the Integration Service is not installed, status for this area will not appear).

Related topics

- [View a Recorder's status summary \(page 484\)](#)
- [Edit status summary thresholds \(page 487\)](#)
- [View System Monitor status \(page 489\)](#)
- [View capture status \(page 489\)](#)
- [View Recorder capture status \(page 490\)](#)
- [View channel status \(TDM capture\) \(page 493\)](#)
- [View extension status \(IP capture\) \(page 495\)](#)
- [View workstation status \(page 498\)](#)
- [View Integration Service status \(page 499\)](#)
- [Query Integration Service status \(page 506\)](#)
- [View the status of other components \(page 509\)](#)

View a Recorder's status summary

Use this function to monitor the overall health of the Recorder. Face icons beside the name of the Recorder indicate the status of the Recorder.

Status summary icons

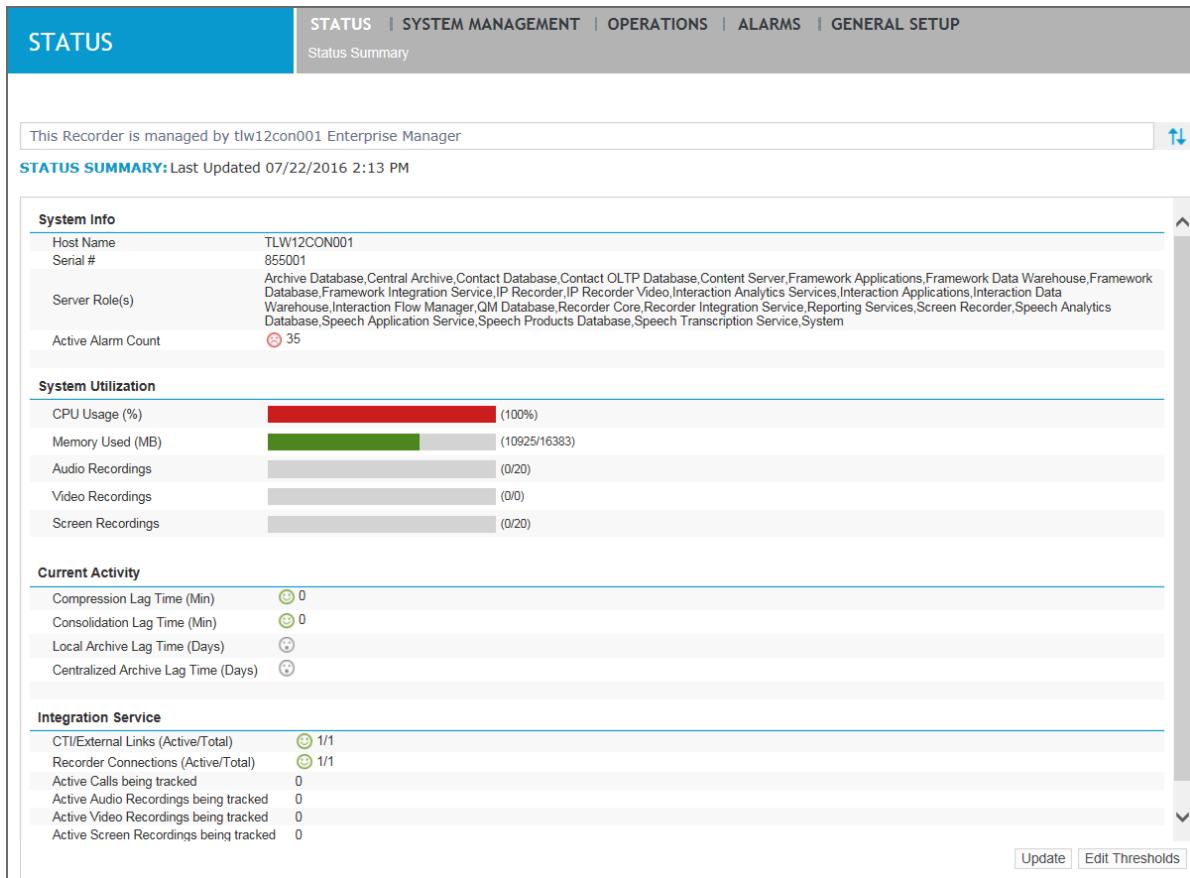
- Green: All is well
- Grey: Unknown status
- Orange: Warning
- Red: Error



For detailed capture settings, refer to [View capture status \(page 489\)](#).

Procedure

1. Click **Status > Status Summary**.



2. Review the following status summary information:

Field	Description
System Info	
Host Name	The name of the PC.
Serial #	The serial number of the Recorder. A serial number is not used with IP Analyzer.
Server Role(s)	All of the roles associated with the Recorder server, including the type of Recorder it is.
Active Alarm Count	The number of currently active alarms.

Field	Description
System Utilization	
CPU Usage (%)	Shows the percentage of the central processing unit's cycles being used, including all related activities such as archiving and disk processing. High usage indicates high usage of the processor (CPU).
Memory Used (MB)	Shows the amount of memory (RAM) in megabytes currently being used by the PC.
Audio Recordings	Shows the number of audio recordings currently in progress. For example, if (10/40) appears, the number of audio recordings currently in progress is 10, and the total number of configured voice channels is 40.
Video Recordings	Shows the number of video recordings currently in progress. For example, if (10/40) appears, the number of video recordings currently in progress is 10, and the total number of configured video channels is 40.
Screen Recordings	Shows the number of screen recordings currently in progress. For example, if (10/40) appears, the number of screen recordings currently in progress is 10, and the total number of configured screen channels is 40.
Current Activity	
Compression Lag Time (Min)	<p>Shows a graphical representation of the amount of time in minutes that the compressor component is behind. Default times are:</p> <ul style="list-style-type: none"> • Less than 5 minutes, a smiling face • More than 5 minutes but less than 1 hour, a neutral face • More than 1 hour, a red face <p>You can change these time by editing thresholds, as described in Edit status summary thresholds (page 487).</p>
Consolidation Lag Time (Min)	Shows a graphical representation of the amount of time in minutes that the consolidator component is behind. Times for smiling faces are the same as with Compression Lag Time above.
Local Archive Lag Time (Days)	Shows a graphical representation of the time in minutes since the last local archive operation. For less than 60 minutes a smiling face shows; for more than 60 minutes and less than 2 hours, a neutral face shows; for more than 2 hours, a red frown face shows. Statistics for centralized archiving display separately.
Centralized Archive Lag Time (Days)	Shows a graphical representation of the time in minutes since the last centralized archiving operation. For less than 60 minutes a smiling face appears; for more than 60 minutes and less than 2 hours, a neutral face; for more than 2 hours, a red frowning face.

Field	Description
Integration Service	
CTI/External Links	The number of current active CTI/External links and the total number of links. This value appears as a fraction that indicates how many Integration Service links are configured for that Recorder, including active and non-active links. For example, 1/2 indicates that one link is up and one is down, out of a total of two links setup.
Recorder Connections (Active/Total)	The number of active Recorder connections to the Integration Service server PC and the total number of connections. This value appears as a fraction that indicates how many Recorder connections are configured for the Integration Service on the Recorder, including active and non-active connections. For example, 1/2 indicates that one connection is up and one is down, out of a total of two connections setup.
Active Calls being tracked	Shows the current number of recordings being tracked by the Integration Service at this time.
Active Audio Recordings being tracked	Shows the number of active audio recordings being managed by the Integration Service at this time.
Active Video Recordings being tracked	Shows the number of active video recordings being managed by the Integration Service at this time.
Active Screen Recordings being tracked	Shows the number of active screen recordings being managed by the Integration Service at this time.

3. Do one of the following:

- Click **Edit Thresholds** to edit status summary threshold values, as described in [Edit status summary thresholds \(page 487\)](#).
- Click **Update** to get the latest system data and reload the page.

Edit status summary thresholds

Edit status summary threshold values to increase or decrease the point at which a warning or error appears in Recorder Manager.

For example, if you set the warning and error thresholds for CPU Usage to 80 and 90 respectively, then when CPU Usage reaches 80 percent, a warning appears. When CPU Usage reaches 90 percent, an error appears. For an explanation of each Field Name, see [View a Recorder's status summary \(page 484\)](#).

Procedure

1. Click **Status > Status Summary**, and then click **Edit Thresholds**.

RECORDER STATUS SUMMARY THRESHOLDS:

System Utilization Thresholds (%)		
Field Name	Warning Threshold	Error Threshold
CPU Usage (%)	80	90
Memory Used (%)	90	95
Audio Recordings (%)	80	90
Video Recordings (%)	80	90
Screen Recordings (%)	80	90

Current Activity Thresholds (Time Since Last activity in minutes)		
Field Name	Warning Threshold	Error Threshold
Compression Lag Time (Min)	5	60
Consolidation Lag Time (Min)	5	60
Local Archive Lag Time (Days)	3	3
Centralized Archive Lag Time (Days)	3	3

Default **Save** **Cancel** **Revert**

2. In the **Status Summary Thresholds** screen, do one of the following:
3. To set all fields to their default values (recommended), click **Default**, and then click **Save**.
4. Enter a number between one and 100 for the Warning Threshold and Error Threshold values, and then click **Save**. This value will represent a percentage or an amount in minutes or days, depending on the field. When this number is reached, a warning or error message will appear.

Field	Threshold Default Value
System Utilization	
CPU Usage (%)	Warning Threshold default 80 percent. Error Threshold default 90 percent.
Memory Used (%)	Warning Threshold default 90 percent. Error Threshold default 95 percent.
Audio Recordings (%)	Warning Threshold default 80 percent. Error Threshold default 90 percent.
Video Recordings (%)	Warning Threshold default 80 percent. Error Threshold default 90 percent.

Field	Threshold Default Value
Screen Recordings (%)	Warning Threshold default 80 percent.
	Error Threshold default 90 percent.
Current Activity Thresholds	
Compression Lag Time (Min)	Warning Threshold default 5 minutes.
	Error Threshold default 60 minutes.
Consolidation Lag Time (Min)	Warning Threshold default 5 minutes.
	Error Threshold default 60 minutes.
Local Archive Lag Time (Days)	Warning Threshold default 3 days.
	Error Threshold default 3 days.
Centralized Archive Lag Time (Days)	Warning Threshold default 3 days.
	Error Threshold default 3 days.

View System Monitor status

Click **Status > System Monitor** to view the status of different components across the system.

View capture status

You can view and filter the capture status of IP Extensions, TDM Channels, and Screen Workstations to monitor the operation of the capture engine in the recording system.



The maximum number of filter rows that the system can display at any one time is 1000.

This section describes how to do the following:

- [View Recorder capture status \(page 490\)](#)
- [View channel status \(TDM capture\) \(page 493\)](#)
- [View extension status \(IP capture\) \(page 495\)](#)



Filter settings apply to the entirety of data available on the Recorder at the time you click the Update button. That is, if you filter the results once, additional changes to the filter settings do not apply to that subset of data, but rather to the whole. To see all results again, click **Clear Filter**, then **Update**.

View Recorder capture status

View the Recorder's capture status to obtain statistics about current capture operations. Statistics such as the number of calls being recorded, and total calls recorded, are summarized according to Recorder roles that are activated.

Please note the following:

- Calls may be counted as recorded in the **Screen Capture** section under **Calls Recorded** even if the recorded content does not contain the screen activity of an active, logged in employee. If the employee is logged off or their machine is offline, a blank blue screen will be recorded and an alarm will be raised in the Recorder Manager, indicating that no active employee screen content was received from the employee's workstation. However, a call will be added to the calls Recorded Count.
- Calls will not be counted as recorded if a command to start recording screens is not sent to the employee's workstation. This will happen if employee screen capture is not configured correctly in Enterprise Manager or the Recorder Screen Capture service is not running and hence no command to start recording is sent to the employee's workstation.

Procedure

Use the following procedure to view the Recorder's capture status.

1. Click **Status > Capture Status > Recorder Status**.
2. The status page displays some or all of the following information depending on the server roles that are active on the recorder:

IP Recorder (Audio) status

Field	Description
Refresh Rate	The refresh rate for the screen. Values range from one minute (the default) to 20 minutes. Longer refresh rates lessen the impact on system performance.
Calls in progress	The current number of in-progress IP audio contacts.
Calls Recording	The number of IP audio contacts being recorded.
Total Calls Recorded	Total number of IP audio contacts recorded since the last restart of the Recorder.
Calls recorded in last hour	The total number of IP audio contacts recorded in the last hour.
Peak Unlicensed Calls	The maximum number of unlicensed audio contacts received at the same time. This can be helpful in various licensing scenarios to determine whether the number of calls in progress is greater than the number of calls recording.

IP Recorder (Video) status

Field	Description
Calls in progress	The current number of in-progress video contacts.
Calls Recording	The number of video contacts being recorded.
Total Calls Recorded	Total number of video contacts recorded since the last restart of the Recorder.
Calls recorded in last hour	The total number of video contacts recorded in the last hour.
Peak Unlicensed Calls	The maximum number of unlicensed video contacts received at the same time. This can be helpful in various licensing scenarios to determine whether the number of calls in progress is greater than the number of calls recording.

TDM Recorder status

Field	Description
Refresh Rate	The refresh rate for the screen. Values range from one minute (the default) to 20 minutes. Longer refresh rates lessen the impact on system performance.
Calls in progress	The current number of in-progress TDM audio contacts.
Calls Recording	The number of TDM audio contacts being recorded.
Total Calls Recorded	Total number of TDM audio contacts recorded since the last restart of the Recorder.
Calls recorded in last hour	The total number of TDM audio contacts recorded in the last hour.
Peak Unlicensed Calls	The maximum number of unlicensed audio contacts received at the same time. This can be helpful in various licensing scenarios to determine whether the number of calls in progress is greater than the number of calls recording.

Screen Recorder status

Field	Description
Calls in progress	The current number of in-progress audio contacts.

Field	Description
Calls Recording	The number of screen recordings occurring.
Total Calls Recorded	Total number of screen recordings since the last restart of the Recorder.
Calls recorded in last hour	The total number of screen recordings in the last hour.
Peak Unlicensed Calls	The maximum number of unlicensed audio contacts received at the same time. This can be helpful in various licensing scenarios to determine whether the number of calls in progress is greater than the number of calls recording.

3. Click **Update** for an immediate refresh.

View channel status (TDM capture)

View the status of channels in a TDM capture environment to obtain statistics related to channels supported by the Recorder. You can configure these channels in Enterprise Manager.

Procedure

1. Click **Status > Capture Status > TDM Channels Status**.

The screenshot shows the 'CAPTURE STATUS' section of the Recorder's interface. At the top, there are navigation links: STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP. Below these are sub-links: Recorder Status, IP Extensions Status, and TDM Channels Status. The main content area is titled 'TDM CHANNEL' and shows the last update time as 'Last Updated 05/11/2014 1:30:06 PM'. A 'Filter' button is available. Below the filter are several columns: Channel, Recording Status, Last Seen INUM, Last Call Seen Time, Error Severity, CTI Available, Primary, Member Group, Channel Status, and Card Type. There is a large empty table body below these headers. At the bottom right of the page are 'Update' and 'Clear Filter' buttons.

2. The status screen displays the following information:

Field	Description
Channel	The channel number.
Recording Status	Shows the status of the extension: <ul style="list-style-type: none">Recording—The extension is currently being recorded.Idle—The extension is not being recorded.Call Seen—An active call for the extension is present, but is not being recorded yet.

Field	Description
INUM	Applies only to pre- Version 11 databases. Shows the INUM of the last call recorded by this extension.
Call Seen Time	Last call start time of this extension.
Error Severity	This is the N+N Redundancy severity of the extension. Possible severities are No Error, Minor Error, Major Error, Critical Error or Not Applicable.
CTI Available	Shows the state of CTI availability. Yes indicates that the Integration Service is capable of either providing the CTI tagging or controlling the Recordings, including tagging. No indicates that CTI is not available.
Primary	Shows whether this extension has the primary state. Yes indicates that the extension is primary and the channel is consolidating calls to the database, while No indicates that it is secondary and is not consolidating calls to the database.
Member Group	Identifies the member group to which the extension belongs.
Channel Status	The status of the channel being recorded (Enabled or Disabled).
Card Type	Lists the type of voice card associated with the channel being recorded.

3. To view a subset of the status information, in the **Filter** section, select the criteria by which you want to filter the results, then click **Update**.

The screenshot shows the 'CAPTURE STATUS' page with the 'TDM CHANNEL' tab selected. At the top, there's a navigation bar with links to STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP, along with sub-links for Recorder Status, IP Extensions Status, and TDM Channels Status.

TDM CHANNEL: Last Updated 05/11/2014 1:36:36 PM

Filter Applied:

Channel	From	To			
Last Seen INUM	From	To			
Recording Status	<input type="checkbox"/> Idle	<input checked="" type="checkbox"/> Recording			
Error Severity	<input type="checkbox"/> Not Applicable	<input type="checkbox"/> No Error	<input type="checkbox"/> Minor Error	<input type="checkbox"/> Major Error	<input type="checkbox"/> Critical Error
CTI Available	<input type="checkbox"/> No	<input checked="" type="checkbox"/> Yes			
Primary	<input type="checkbox"/> No	<input checked="" type="checkbox"/> Yes			
Channel Status	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Disabled			
Member Group					
Card Type					

Table Headers: Channel, Recording Status, Last Seen INUM, Last Call Seen Time, Error Severity, CTI Available, Primary, Member Group, Channel Status, Card Type.

Buttons: Update, Clear Filter.



Your filter settings apply to the entirety of data available on the Recorder at the time you click the Update button. That is, if you filter the results once, additional changes to the filter settings do not apply to that subset of data, but rather to the whole.

View extension status (IP capture)

You can view the status of both configured and dynamic extensions in an IP capture environment.

- Configured Extensions—The status of extensions that you configure within Member Groups in Enterprise Manager will appear on the IP Extensions Status page (even those extensions with an extension Recording Mode of ‘Do Not Record’).
- Dynamic Extensions—Dynamic extensions are those that are not specifically configured in Enterprise Manager, but rather are those the Recorder is aware of either via the Integration Service or through protocol messages (such as SCCP or SIP). They include both trading extensions and non-trading extensions. In the case of the latter, IP Extensions Status page will show extensions in both CTI- and Recorder-controlled environments, whether the extension is recorded or not.

Procedure

1. Click **Status > Capture Status > IP Extensions Status.**

The screenshot shows the 'CAPTURE STATUS' interface with the 'IP EXTENSION' tab selected. The table lists the following data:

Extension	Recording Status	Audio Inum	Video Inum	Call Seen Time	Error Severity	CTI Available	Primary	Member Group	Data Source	Last Call ID
102	Idle	0	0	N/A	No Error	No	Yes	Huawei IP Extension Pool	Huawei DS1	N/A
104	Idle	0	0	N/A	No Error	No	Yes	Generic IP Extension Pool	Generic DS1EDIT	N/A
106	Idle	0	0	N/A	No Error	No	Yes	Avaya IP Extension Pool	Avaya DS1EDIT	N/A
112	Idle	0	0	N/A	No Error	No	Yes	Huawei IP Extension Pool	Huawei DS1	N/A
114	Idle	0	0	N/A	No Error	No	Yes	Generic IP Extension Pool	Generic DS1EDIT	N/A
116	Idle	0	0	N/A	No Error	No	Yes	Avaya IP Extension Pool	Avaya DS1EDIT	N/A

Page 1 of 50 | Update | Clear Filter

2. The status screen displays the following information:

Field	Description
Extension	The extension number that is configured to be recorded.
Recording Status	Shows the status of the extension: <ul style="list-style-type: none"> Recording—The extension is currently being recorded. Idle—The extension is not being recorded. Call Seen—An active call for the extension is present, but is not being recorded yet.
Inum	The INUM assigned to the last recorded audio call on this extension. If the last audio call seen on this extension was not recorded, Inum is set to 0.
Video Inum	The INUM assigned to the last recorded video call on this extension. If the last video call seen on this extension was not recorded, Video Inum is set to 0.
Call Seen Time	Time of the last call seen on this extension.
Error Severity	This is the N+N Redundancy severity of the extension. Possible severities are No Error, Minor Error, Major Error, Critical Error or Not Applicable.
CTI Available	Shows the state of CTI availability. Yes indicates that the Integration Service is capable of either providing the CTI tagging or controlling the Recordings, including tagging. No indicates that CTI is not available.

Field	Description
Primary	Shows whether this extension has the primary state. Yes indicates that the extension is primary and the channel is consolidating calls to the database, while No indicates that it is secondary and is not consolidating calls to the database.
Member Group	Identifies the member group to which the extension belongs.
Data Source	Lists the data source with which this phone is associated.
Last Call ID	Call reference of the last call seen on this extension.
Audio Recording Mode	Shows the audio recording mode of the extension. Possible values include Start on Trigger, Application Controlled, Do Not Record, and Record.
Video Recording Mode	Shows the video recording mode of the extension. Possible values include Start on Trigger, Application Controlled, Do Not Record, and Record.

3. To view a subset of the status information, in the **Filter** section, select the criteria by which you want to filter the results, then click **Update**.



Your filter settings apply to the entirety of data available on the Recorder at the time you click the Update button. That is, if you filter the results once, additional changes to the filter settings do not apply to that subset of data, but rather to the whole.

View workstation status

View the status of screen recordings to obtain statistics relating to any Workstations that are configured to perform screen capture. You can configure Workstations for screen recording in Enterprise Manager.

Procedure

1. Click **Status > Capture Status > Screen Workstations Status**.

The screenshot shows the 'Capture Status' section of the application. At the top, there's a navigation bar with links to STATUS, SYSTEM MANAGEMENT, OPERATIONS, SYSTEM MONITORING, ALARMS, and GENERAL SETUP. Below that is a secondary navigation bar with links to Recorder Status, IP Extensions Status, and Screen Workstations Status. The main content area is titled 'SCREEN WORKSTATION: Last Updated 05/11/2014 1:57:05 PM'. It features a table with the following data:

Host Name	Terminal Session ID	Recording Status	Last Seen INUM	Last Call Seen Time	Member Group	Channel
ptedkw71	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp01	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp02	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp03	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp04	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp05	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp06	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp07	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp08	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp09	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp10	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp11	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp12	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp13	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp14	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp15	N/A	Idle	0	N/A	Screen Workstation Group	0
vtdktp16	N/A	Idle	0	N/A	Screen Workstation Group	0

At the bottom right of the table, there are 'Update' and 'Clear Filter' buttons.

2. The status screen displays the following information:

Field	Description
Hostname	Shows the name of the Workstation being recorded, or the name of the Terminal Server whose session is being recorded.
Terminal Session ID	Shows the session ID if a Terminal Server is being recorded.
Recording Status	Shows the status of the extension: <ul style="list-style-type: none"> Recording—The extension is currently being recorded. Idle—The extension is not being recorded. Call Seen—An active call for the extension is present, but is not being recorded yet.
INUM	Applies only to pre- Version 11 databases. Applies to only to databases that pre-date this release. Shows the INUM of the last call consolidated to the database.

Field	Description
Call Seen Time	Last call start time on this workstation.
Member Group	Lists the member group associated with the screen data source.
Channel	Shows the Recorder-assigned ID for the resource, that will be used for recording the Workstation screen.

3. To view a subset of the status information, in the **Filter** section, select the criteria by which you want to filter the results, then click **Update**.

The screenshot shows the 'SCREEN WORKSTATION' status page. At the top, there are navigation links: STATUS, SYSTEM MANAGEMENT, OPERATIONS, SYSTEM MONITORING, ALARMS, and GENERAL SETUP. Below these are three status indicators: Recorder Status, IP Extensions Status, and Screen Workstations Status. The main area displays a table of workstations with columns: Host Name, Terminal Session ID, Recording Status, Last Seen INUM, Last Call Seen Time, Member Group, and Channel. Above the table is a 'Filter' section with fields for Terminal Session ID, Last Seen INUM, Channel, Recording Status (Idle or Recording), Host Name, and Member Group. There are also 'From' and 'To' date/time input fields for each of these filters. At the bottom right of the filter section are 'Update' and 'Clear Filter' buttons.

i Your filter settings apply to the entirety of data available on the Recorder at the time you click the Update button. That is, if you filter the results once, additional changes to the filter settings do not apply to that subset of data, but rather to the whole.

View Integration Service status

The information that appears on the Integration Service status page depends on what has been configured and whether there is any information to report.

Procedure

- Click **Status > Integration Status**.
- The Integration Status includes the following information:

Name	Description
Refresh Rate	Allows you to set the refresh rate for the Integration Status screen, to between one (the default) and 20 minutes. Longer refresh rates lessen the impact on system performance.
Business Rules	Business Rules
Number of Active Rules	The total number of business rules managed by the system.
Evaluation Rate	The previous and maximum hourly rate at which rules are being evaluated.
Average Rules Per Event	The average rate at which rules are firing.
Trigger Rate (Current/Max)	The current and maximum hourly rate at which evaluated rules are being triggered.
Adapters	Adapters
Name	Lists the names of the CTI Adapters.
Server Name	The server source for the adapter. Adapters can be either local or remote. Local adapters are identified as such. Remote adapters identify the remote server host that registered the adapter with this local server.
Startup Type	Shows the startup type of the CTI adapter. Options include: Automatic, Manual, and unavailable. This time is shown in the local time zone of the user.
Status	Shows the status of the CTI adapter. Statuses include Started, Stopped, Starting, Stopping.
Last Startup Time	Shows the last time that the CTI adapter was started.
Event Rate	Shows the current and maximum hourly incoming rate of events that the CTI adapter is processing.
Data Sources	Data Sources
Name	Shows the name of the data source to which the Recorder Integration Service is associated.
Lines (Registered/Tracked)	Shows the number of devices registered to, and tracked by, the data source. Registered lines include both configured and dynamic lines used for call modeling and recording. Tracked lines include all lines that the data source is tracking.
Calls	Shows the total number of calls per data source.

Name	Description
Call Rate (Current/Max)	Shows the number of calls recorded in the previous hour, followed by the highest number that occurred in any hour.
Event In Rate (Current/Max)	Shows the number of switch events that came into the Integration Service in the previous hour, compared to the highest value in any given hour during this run of the Integration Service.
Event Out Rate (Current/Max)	Shows the number of switch events that were relayed from the Integration Service in the previous hour, expressed as the current number compared to the highest value in any given hour during this run of the Integration Service.
Real Time Monitor	
Session	Identifies which MAS connection the line is for.
App Server Name	The configured host name of the application server hosting the client connection.
Monitored Lines	Number of extensions/employees the MAS server is monitoring.
Active Streams	The number of Real Time Monitoring audio streams currently in progress.
Active Monitors	The number of Real Time Monitoring sessions/interactions currently in progress. The Recorder Integration Service attempts to actively proxy any associated desktop through a screen Recorder for each monitoring session/interaction. In Speech Analytics, an interaction represents a single part of the contact between one employee and the same customer. In Text Analytics, an interaction is the communication between one or more employees and the same customer with a unifying contextual element.
Policy Manager	
Tracked Sessions	The number of current and maximum concurrent Sessions/Interactions, active and old, that the system is tracking.
Session Rate	The current and maximum hourly rate of Sessions/Interactions that the system is building and managing.
Tracked Contacts	The number of current and maximum concurrent Contacts that the system is tracking.
Contact Rate	The current and maximum hourly rate of Contacts that the system is building and managing.
Recorders	Recorders

Name	Description
Name	Lists the names of all Recorders associated with the Integration Service.
Role	Shows the Recorder server roles.
Status	Shows the connection status of the Recorder. Options include Connected and Not Connected.
Last Connect Time	Shows the last time that the Recorder was connected to the Integration Service.
Channels (Rec/High/Max)	Displays a channel count for each of the following: <ul style="list-style-type: none"> • Rec—current number of tracked recordings on this particular recording role • High—the largest number of concurrent recordings seen for this recorder role since the Last Connect Time • Max—the maximum number of concurrent recordings (the license count for that role)
Controlled Devices	The total number of controlled devices for this role.
Recording Rate	Shows the calculated rate at which recordings are taking place, in the format current rate/maximum rate to date.
Message Rate	Shows the calculated rate at which system messages are taking place, in the format current rate/maximum rate to date.
API Resources	
Provides status for client connectivity and message rates for various API resources registered within the server.	
Resource	The API resource being accessed.
Clients	The current and maximum concurrent clients connected to the resource.
Message Receive Count	The total number of messages received for this resource from all connected clients.
Message Receive Rate	The current hourly and maximum hourly message receive rate from all connected clients.
Data Receive Rate	The current hourly and maximum hourly data receive rate from all connected clients. This rate is not directly convertible to network data rate (for example, Kbps), but is related to the average message size received.
Message Send Count	The total number of messages sent for this resource from all connected clients.

Name	Description
Message Send Rate	The current hourly and maximum hourly message send rate to all connected clients.
Data Send Rate	The current hourly and maximum hourly data send rate to all connected clients. This rate is not directly convertible to network data rate (for example, Kbps), but is related to the average message size sent.
System Info	
Provides status of various aspects of the system run time information for reference.	
Statistic	The specific statistic or run time element being referenced.
System Value	The specific system level value for this item.

The following fields are optional and only appear in some environments.

Name	Description
Correlation Recorder	
Provides information on the dynamic identifiers that the system is tracking to correlate recordings to CTI in environments where recording does not provide definitive station information. Only appears when using Gateway Correlation Pool.	
DataSource	The DataSource name tracking the dynamic devices.
Member Group	The Member Group name on the DataSource tracking the dynamic devices.
Dynamic CTI Keys	The total number of dynamic keys generated from the CTI feed.
Dynamic Recorder Keys	The total number of dynamic keys generated from the started recordings.
Redundancy	
This section covers the per-DataSource redundancy of the system. Only appears in 1+1 Recorder Integration Service Implementations.	
Name	Server name, either local or peer.
Type	Main or backup role indicator.
Status	Current redundancy state.
DataSource	The DataSource name in this redundancy.
Active CTI Count	The current active and total number of CTI adapters for this data source on the referenced server.

Name	Description
Version	The build version information for the reported role.
SIP / SIPREC	This section covers the SIP calls tracked by the system. Only appears when using a SIP adapter.
Adapter	The adapter name for these SIP statistics.
Request Recv Rate	The current and maximum hourly rate at which SIP requests are received.
Request Send Rate	The current and maximum hourly rate at which SIP requests are sent.
Response Recv Rate	The current and maximum hourly rate at which SIP responses are received.
Response Send Rate	The current and maximum hourly rate at which SIP responses are sent.
Total Calls	The total number of SIP calls seen by the adapter.
Open Calls	The current and maximum number of open calls seen by the adapter.
Call Rate	The current and maximum hourly rate at which the adapter manages new call dialogs.
Transaction Timeouts	The total number of transaction timeouts seen by the adapter.
Avaya DMCC (CMAPI)	
This section covers the softphones controlled by the system in DMCC recording. Only appears when using a DMCC adapter.	
Member Group	The member group of softphones for these statistics.
Usage Type	The recording type for the member group. This type designates either Dedicated or Selective, and the mode of Service Observe, Single Step Conference, or Multiple Registration. A secondary usage of Recorder Allocation provides a per-recorder view of how the softphones are registered for each member group.
Recorder	The IP Recorder name and site information for softphone registrations within the Member Group.
Idle	The number of registered softphones that are not currently assigned to any station for recording. These softphones are free to be assigned at-will by the system.

Name	Description
Used	The number of registered softphones that are assigned to a station, but are not actively recording a call. The system may break these associations as necessary to record other stations.
Recording	The number of registered softphones that are assigned to a station and are actively recording a call. The system will not break these associations.
Unavailable	The number of softphones that are not registered and cannot be used for recording.
Peak Usage (Lifetime)	The maximum number of softphones concurrently recording a call.
Recorder Adapter Proxy Services	
Provides the controller node status for Recorder Adapter Proxy Service (RAPS) clients that have registered with the local server.	
Proxy FQDN	The RAPS client node name.
RAPS Connection	The connection state of the RAPS client.
Recorder FQDN	The name of the recorder to which the adapter on the RAPS client node is connecting.
Recorder Connection	The connection state of the adapter on RAPS client to the recorder.
Last Connect Time	The last time the adapter was connected to the recorder.
Adapter Name	The adapter name proxied at the RAPS client.
Adapter Status	The status of the proxied adapter. Statuses include Started, Stopped, Starting, Stopping.
Startup Time	Shows the last time that the adapter was started
Active Calls	The total number of active calls across all media types, as reported by the recorder connection.
Active Recordings	The total number of active recordings across all media types, as reported by the recorder connection.
Local Adapter Proxy	
Provides the proxy node status for a RAPS client running on the local server.	
Adapter Name	The adapter name proxied at the RAPS client.
Role	The recorder role to which the adapter is connected.
FQDN	The recorder name to which the adapter on RAPS is connected.

Name	Description
Status	The connection state of the adapter to the recorder.
Last Connect Time	The last time the adapter was connected to the recorder.
Health	The reported health state of the connected recorder. If disconnected, reports Not Applicable (N/A).
Audio Calls Recording / Licensed	The current count of audio calls actively recorded, and the total licensed audio recording capacity. The recorder may be generating multiple audio inums for a single call.
Video Calls Recording / Licensed	The current count of video calls actively recorded, and the total licensed video recording capacity. The recorder may be generating multiple video inums for a single call.

Query Integration Service status

If you have Administrator privileges you can query the status of the integration service to learn more about workspaces, by extension, employee ID, workstation or employee, and current call information by extension.

Procedure

1. Click **Status > Integration Queries**.

2. Specify the following for your query:

Criteria	Values
Query Types	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Workspaces—returns information about the workspace. A workspace is the conceptual entity of a phone tied to a workstation. (Extended attributes will not be available.) • Current Calls—returns information about current calls. • Current Recordings—returns information about current recordings. • Current Contacts—returns information about contacts (ID, ANI, DNIS, direction, current duration), interactions (ID, device, current duration), and recordings (INUM, type, current duration). • Failed Devices—returns information about failed devices only. (Extended attributes will not be available.) • Current SIP Calls—returns active SIP calls. You may further refine the query by selecting "Extension" or "SIP CallId" as the Criteria Type, then specifying an extension or SIP call ID respectively in the Criteria Field. Search by extension is applicable only when the Recorder Integration Service is capable of tagging extensions from SIP messages. In environments with gateway correlation, for example, no extension will be provided as part of the SIP INVITE, and therefore a search by extension will not return any results.
Criteria Types	<p>Select one of the following, to be applied to the Query Type selected above. You must also complete the Criteria Field described below.</p> <p>For example, if you select a Query Type of Workspace with a Criteria Type of Extension, type the extension number in the Criteria Field, and the query will provide status information for that workspace extension.</p> <ul style="list-style-type: none"> • Extension • AgentId • Workstation • Employee • SIP CallId
Data Source	<p>The list of data sources is derived from those set up in Enterprise Manager. Select one of these or alternatively, select *(All Datasources) to query the complete list.</p>

Criteria	Values
Criteria Field	Specify a value for the particular Criteria Type you selected above. For example, if you selected AgentID as the Criteria Type, enter the actual AgentID here.
Extended Attribute	Select this check box to include CTI and custom attribute information about displayed calls. (Disabled by default as this data may occupy a large amount of screen space.) You cannot use Extended Attributes with the Workspaces and Failed Devices as the Query Type.

3. Click **Submit**.
4. The query results will appear in the lower half of the page. If a query fails, it may mean that the system is unable to contact the Integration Service.



For each new query you must click **Submit** again to view the results.

View the status of other components

View a status summary of remaining Recorder components to understand how these key components are operating. You can view statistics on four key areas: Archive, Database Consolidation, Disk, and Compressor.

Procedure

1. Click **Status > Other Status**.

The screenshot shows the 'Other Status' page under the 'Status' menu. At the top, there are tabs for STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP, with 'STATUS' being the active tab. Below the tabs, a 'Refresh Rate' dropdown is set to '1 Minute'. The main content area is divided into several sections:

- Archive:** Shows fields for Drive Name, Select Attached Device(s), Current Media, Drive Status, and Total files archived. For example, 'Drive Name' is 'PTECON1.TELAB.LOCAL'.
- Compressor:** Shows 'Calls Compressed' count, which is 0.
- Database Consolidation:** Shows 'Server' and counts for Completed Jobs (0) and Failed Jobs (0).
- Disk:** Shows 'Drive Name' (C), Call Buffer Location (C:\Calls), Percentage Space Used (84.38), and Space Remaining(MB) (15991).
- NIC Cards:** Shows 'Name' (Application NIC), Packets Dropped By Driver (0), Packets Received By Driver (29102728), and Packets per Second (2).

An 'Update' button is located at the bottom right of the page.

2. The following fields appear:

Field	Description
Archive	
Drive Name	Lists the user-defined name for the drive.
Select Attached Device	Shows attached archive media, such as DVD-RW or Tape.
Current Media	Shows the archive media device currently being used or last used.

Field	Description
Drive Status	Shows the status of the archive drive.
Total Files Archived	Shows the total number of files archived to date since last reset.
Database Consolidation	
Server	The logical name of the database server (such as ATL Media Server).
Completed Jobs	The number of database consolidations that have completed successfully.
Failed Jobs	The number of database consolidations that were unsuccessful.
Disk	
Drive Name	Drive name on the disk.
Call Buffer Location	Shows the path/location to the Recorder's call buffer on the disk, such as F:\Calls.
Percentage Space Used	Shows the percentage of hard disk space used for a hard drive in the list.
Space Remaining (MB)	Shows the amount of hard disk space, in megabytes (MB), not being used for a hard drive in the list.
NIC Cards	
Name	The name assigned to the NIC card.
Packets Dropped By Driver	Number of packets dropped by the driver.
Packets Received By Driver	Number of packets received by the driver.
Packets per Second	Total number of packets per second.
Compressor	
Calls Compressed	The total number of contacts processed by the Compressor component.

3. Do one of the following:

- Click another screen to continue.
- Click **Update** to get the latest system data and reload the page.

A system update is more current than the system refresh. With system refresh, data is updated automatically according to the Refresh Rate setting. Click **Update** to obtain the latest data at a particular instant in time.

System logs

Use system logs in Recorder Manager to manage configuration files, view logs, and view audit trails for the local Recorder. Logs and files for other subsystems in the solution are managed elsewhere.

If there are any system issues, a message will appear in red at the top of your screen.

Related topics

[System log manager \(page 511\)](#)

[View system logs \(page 513\)](#)

[Customize the log viewer display \(page 514\)](#)

System log manager

Use the Log Manager to access log file configuration options to enable or disable the generation of selected log files.

Procedure

1. Click **System Monitoring**, then under **Log**, click **WFO Log Manager**.
2. Select a **Log Server** in the upper right-hand corner.

The screenshot shows the 'LOG' tab selected in the top navigation bar. The top menu includes STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP. Below the menu, 'Log Viewer' and 'Log Manager' are listed. A sub-header 'LOG MANAGER: Available Log Configurations for selected Server.' is displayed. On the right, a 'Log Server:' dropdown is set to 'localhost:RM'. A table lists two log configurations:

Name	Active	Description
core.xml	Yes	This is the default log configuration file that ships with the Suite
debugFile.xml	No	This configuration will log messages of all severities to the log file. Warning: The overall system performance will be greatly affected.

An 'Activate' button is located in the bottom right corner of the main content area.

3. The following fields will appear for the selected server and its log files:

Item	Description
Name	Shows the name of the log file.
Active	Toggles between Yes and No , which are options that enable or disable the generation of logs for the named file.
Descriptions	Shows a description of each named file.

4. To activate a log file, highlight the log configuration file and click **Activate**.
5. The log file for IntegrationServiceWrapper is managed independently of Log Manager, as this Integration Service (IS) log file cannot use the common logging components facility used by all other program components. To locate IntegrationServiceWrapper (on an IS Server) do this:
 - a. In Windows Explorer, navigate to the <install software dir>\conf directory.
 - b. Open the file **IntegrationServiceWrapper.conf**.
 - c. Locate the following line:
wrapper.logfile=../log files/IFwrapper-YYYYMMDD.ROLLNUM.log

View system logs

Use this page to configure and view System Logs. All actions that will result in a modification or change to the configuration are tracked here, and all error and warning conditions that occur within Recorder Manager. (Administrators accessing a configuration will not be logged.)

Procedure

1. Click **System Monitoring**, then under **Log**, click **WFO Log Viewer**.

The screenshot shows the 'LOG' tab selected in the top navigation bar. Below it, the 'Log Viewer' configuration section is displayed. The configuration form includes fields for Log Server (localhost:RM), Log Type (Default), User Name, Message Contains, Category, Component, Number of Lines Shown (10), Severity (Fatal, Error, Warning, Information, Debug), Time (None, For the Last, FromTo), and a date range (05/10/2014 2:42 PM - 05/11/2014 2:42 PM). At the bottom right are 'View' and 'Revert' buttons.

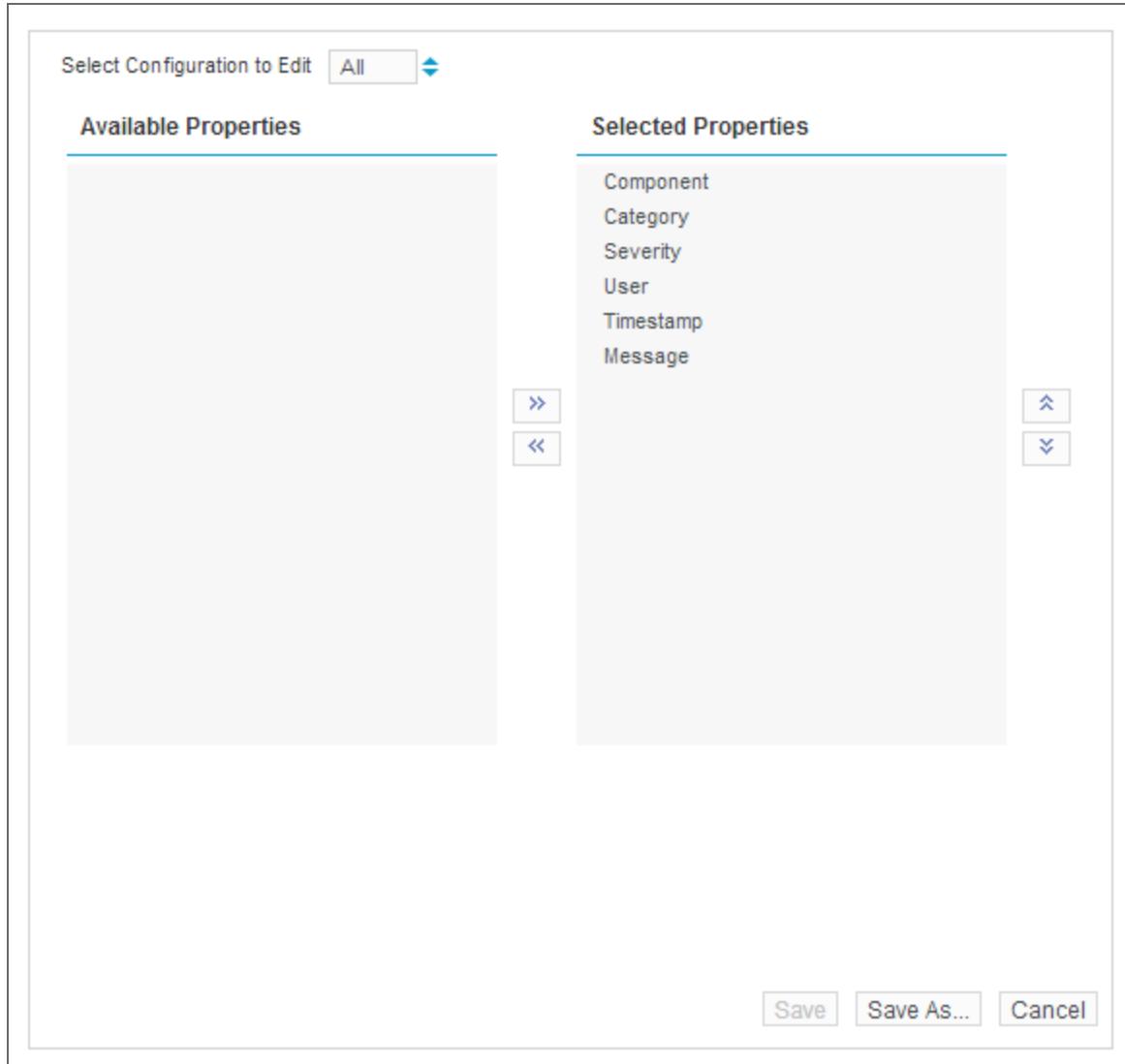
2. Select a **Log Server** from the dropdown list, then select the type of log.
3. Type the criteria to filter by (User Name, Message Contains, and so on). If you choose to filter by category, please note the following:
 - The category is a specific Java class name that logged the error. For example:
ejb.bpx.am.msgProcessor.MessageQueueConnector
 - The component is the package or area of the application that contain the class that logged the error. For example:
web.bbm, bpx, ejb.am
4. Type the number of lines to be displayed at one time.
5. Check the severities of the errors you want displayed. Choices include Fatal, Error, Warning, Information, and Debug.
6. Select the time period to be displayed. Select **None** to display events for all time periods covered by the log, or select a time range.
7. Click **View** to view logs with the displayed settings.

Customize the log viewer display

You can choose the log file properties you want to display and the order in which the properties are displayed.

Procedure

1. Follow the steps described in [View system logs \(page 513\)](#), and then click **Edit** in the **Customize** drop down menu.



2. Select properties and use the left/right arrows to move them between the **Available** and **Selected Properties** panes.
3. Click **Save** to save the default customization, or click **Save As** to save under a different name.

Alarms

Use alarms in the Recorder Manager to monitor system status and performance. Alarms are triggered by predefined events and conditions.



The Enterprise Manager also includes alarms and mechanisms to configure alarms and set up notifications.

Related topics

- [View active alarms \(page 515\)](#)
- [Clear alarm history \(page 516\)](#)

Related information

Enterprise Manager Online Help

System Monitoring Messages and Alarms Guide

View active alarms

View active alarms to obtain information that you can use to take corrective actions.



You can set the **Refresh Rate** in the upper right corner to specify the frequency (in minutes) with which the system checks for alarms. Setting the Refresh Rate too low may affect system performance, as frequent checks will use more system resources.

Procedure

1. Click **Alarms > View Alarms > Active Alarms**.
2. Review the following fields:

Item	Description
Alarm Name	The name of the alarm.
Last Triggered	The time at which the last instance of this alarm occurred.
Alarm Summary	A brief description of the alarm.
Priority	Shows the priority of the alarm.
Count	The number of times this alarm has been raised.
Last Alarm Instance Details	Provides additional details about the last instance of this alarm, which may assist in troubleshooting.
Component	Identifies the particular component to which this alarm relates.

3. Select an alarm and do one of the following:

- Click **View** to view the full text and any resolution suggestions.
- Click **Acknowledge** to acknowledge the alarm; this will move it from this screen to the **Alarms History** screen.



If an alarm is raised for a server role, and you deactivate the server role without acknowledging the alarm, the system continues to raise the alarm even after the server role is deactivated. After deactivating a server role, you must manually acknowledge all active alarms related to the server role to prevent this problem.

Clear alarm history

You can review a cumulative list of acknowledged alarms and remove records that are no longer useful. Some alarms may be resolved automatically, in which case they are listed as being resolved by a system component.

Procedure

1. Choose **Alarms > View Alarms > Alarm History**.
2. Click **Clear All** to remove all alarm instances from the Alarm History screen. If you do not clear alarms, they are cleared automatically according to **Maximum days to store alarm history** set in Enterprise Manager.

Recorder troubleshooting

This section describes how to troubleshoot the Recorder.

Topics

Troubleshooting Recorder issues	518
Configuration reports	551
Log Manager utility	552

Troubleshooting Recorder issues

The following sections describe issues and possible resolutions.

- General issues (page 518)
- Software issues (page 522)
- Hardware issues (page 545)

General issues

Possible ways to resolve issues are provided.

Related topics

- Discrepancy in displayed call duration or percentage recorded (page 519)
- No employee ID tagged (page 519)
- Workstation not recording (page 519)
- Workstation recorded does not appear to match voice recording (page 519)
- Recordings occur when none are required (page 520)
- Integration Service not tagging (page 520)
- Cisco DMS not recording (page 520)
- All Cisco recordings are “noise” (page 520)
- Long calls (page 520)
- Missing recordings (page 520)
- Connect API events not being processed (page 520)
- Recorder fails to update components (page 520)
- Interaction playback between two employees, when one is on hold, has replay issues during hold times (page 521)
- One or more of the media files that are part of the interaction are not found (page 521)
- Unable to delete workstation (page 523)
- Find lost calls (page 523)
- Activity auditing (page 523)
- Short IP call segments are not being recorded (page 525)
- TDM recording issues with NGX cards (page 525)
- Reset channel mechanisms for NGX cards (page 541)

- Checksum mismatches (page 542)
- Network Interface Card (NIC) name displays symbols (page 545)

Discrepancy in displayed call duration or percentage recorded

The recording end time is calculated from the start of a time-out event. Silence is not inserted into a recording if there is no audio at the end of a call, so the displayed recording duration or percentage recorded may not match the amount of *actual* audio recorded. A recording error alarm will identify this condition.

No employee ID tagged

If logins are not being received, verify the following items.

- Employee IDs are configured.
- Data Source Groups are configured.
- The Data Source Group Name is the number of the skill/hunt group.

Workstation not recording

If screen recording is not functioning for a particular workstation or workstations, verify the following items.

- The Workstation Group for the LAN Data Source is associated with the recorder.
- The Workstations to be recorded are configured and assigned to the correct Workstation Group.
- A business rule is configured to record screens.

You can also locate the REQUESTWORKSTATIONLIST message in the Integration Service log [DebugHigh logging level] for more information.

Workstation recorded does not appear to match voice recording

There may be an incorrect association between Workstations and Phone extensions.

Related topics

[Define workstations \(page 112\)](#)

Recordings occur when none are required

This may occur when fallback is enabled and the Integration Service has not received CTI.

Integration Service not tagging

The Integration Service matches CTI to Inums based on extension, so verify that the extension was received from the Recorder.

Cisco DMS not recording

This may be due to one of the following items.

- Incorrect Cisco CM configuration (Route Pattern, Recording Profile, SIP Trunk, Devices).
- Phones were not reset after configuration.

All Cisco recordings are “noise”

CallManager is set up for encrypted RTP.

Long calls

Non-CTI screen recording enabled.

Missing recordings

Check for the following items.

- NGA messages for an unconfigured channel in the Integration Service log. If found, the cache files are out of sync.
- You may have configured a Generic switch type that is not understood by the adapter.

Connect API events not being processed

There may be insufficient information to identify the device.

Recorder fails to update components

If a component cannot be updated, do the following tasks.

- Verify that an active network connection exists.
- Verify that you have security privileges to make the change.

- Verify that the recording subsystem is installed correctly.
- Make sure that Recorder Web Services are up and running.
- Make sure the call buffer location has not been changed. See [Relocate the call buffer \(page 187\)](#).

Interaction playback between two employees, when one is on hold, has replay issues during hold times

For Cisco SRTP Interception environments, replay of hold times for an interaction between two employees results in stuttering or white noise instead of hold music or silence. The playback issue only exists when one of the employees is on hold.

Procedure

1. Launch Recorder Manager.
2. Go to **General Setup > Capture Settings > IP Recording**.
3. Set **Detect RTP** to **Never**.
4. Save the configuration changes.

Related topics

[Configure IP recording settings \(page 249\)](#)

One or more of the media files that are part of the interaction are not found

When the **Recorder IP CaptureEngine** service starts, the system automatically searches the Recorder for open media files during the start sequence. The service starts when manually stopped/started and when the Recorder is powered on or restarted. If open media files are found, they are either closed or removed. Open media files are WAV (audio) and MP4 (video).



Open MP4 files do not result from stopping the capture service or when powering off a server in a controlled manner.

The result of the restart sequence varies by environment. The status of related XML metadata files also varies by environment. When possible, the XML files are preserved as a record of the interaction and can be archived. See the following tables for the results by environment:

Open file handling when data-at-rest encryption is used

Environment	Action on open media during start sequence	XML file status
TDM audio	Remains open; cannot be closed or removed	Not created, not available
IP audio	Remains open; cannot be closed or removed	Not created, not available
IP video	Removed	Preserved

Open file handling when data-at-rest encryption is not used

Environment	Action on open media during start sequence	XML file status
TDM audio	Closed	Preserved
IP audio	Closed	Preserved
IP video	Removed	Preserved

Reason for removal of open MP4 files

Open MP4 files are unrecoverable (unplayable and incomplete). For example, if a Recorder shuts down unexpectedly, such as from a power outage, open MP4 files can potentially be a side-effect of the outage.

Effect of removed open MP4 files in Interactions

If open MP4 files are removed, the interactions display in the Interactions application. If you attempt to replay the video, the following message displays: "One or more of the media files that are part of the interaction is not found."

Related topics

[General issues \(page 518\)](#)

Software issues

Identifying and resolving software-related issues are described.

Related topics

[Unable to delete workstation \(page 523\)](#)

[Find lost calls \(page 523\)](#)

[Activity auditing \(page 523\)](#)

[Short IP call segments are not being recorded \(page 525\)](#)

[TDM recording issues with NGX cards \(page 525\)](#)

[Reset channel mechanisms for NGX cards \(page 541\)](#)

[Checksum mismatches \(page 542\)](#)

[Network Interface Card \(NIC\) name displays symbols \(page 545\)](#)

Unable to delete workstation

If you are unable to delete a workstation, check to see whether the workstation has been mapped to an employee (see [Add employee mappings \(page 146\)](#)). If so, remove the association (see [Edit employee mappings \(page 147\)](#)) and attempt to delete the workstation again.

Find lost calls

Use the following procedure to recover data from a call that has been received at the switch, but does not appear in the Interactions application. Tracing for the lost call should be done in the reverse order of the call life cycle.

The life cycle of a call is as follows: **Switch > CTI Logs > Capture Logs > Workflow Service > Calls Consolidator > Interactions**. To find a lost call, start with a search in the Interactions application, and then work back (see [To examine trace logs \(page 524\)](#) to learn how to access logs):

1. Gather as much information as possible about the missing call, such as approximate time the call was received, and the extension, employee, channel, and trunk.
2. Prepare a **Query** in the Interactions application, using the above information, and then retrieve the contact.
3. If the call is not in the system database, check the **Calls Consolidator** logs and **Windows Event** logs for any errors. **Consolidator** posts an entry to the **Windows Event** log if there is any problem consolidating a call.
4. If there are no errors in the **Calls Consolidator** logs, check the **Workflow Service** logs.
5. If there are no errors in the **Workflow Service** check in the **Capture** component logs.
6. If the call is not in the **Capture** component logs, check for the call in the **Integration Service** logs.
7. If the call is not found in the **Integration Service** logs check for the call in the **Switch** call logs.

Activity auditing

User activities are reported in the recorder to allow you to track and audit configuration changes. These changes appear in log files from the Recorder Manager, from the Interactions application, from trace logs, alarms history, and Windows event viewer.

Audit information is stored centrally in the audit database in Enterprise Manager, and you can use Audit Viewer to configure search criteria for querying audit trail entries. This information may be useful for troubleshooting purposes or can be periodically reviewed and monitored as part of an auditing process.

To review audit logs from Recorder Manager

Recorder Manager audits all the user operations (except for data retrieval) and provides the ability to search and view those events. You can also use Enterprise Manager to configure auditing criteria.

1. In Recorder Manager, click **System > Log Viewer**
2. Review the **Severity** section of the log viewer.

To view audit trails from Enterprise Manager

1. In Enterprise Manager, click **System Monitoring > Audit Viewer**.
2. Required. In the **Time of Event** field, click the calendar icons and specify the date range when the audited event or action occurred.
 - When the range exceeds 30 days, system performance may be affected.
 - The range cannot exceed 180 days (6 months).
3. Optional. Do any of the following:
 - Specify search criteria in any of the fields (**User Name, Module, Action, Object Name, Impact Time Frame**).
4. Click **View**. (You can customize the fields that appear by clicking **Customize > Edit** in the upper right corner.)

 To search for more than six months of data, perform multiple searches and export the results to a single XLS file.

For example, to retrieve the last two years of audit logs, you can perform four queries of six months each

-  You can control the number of entries shown on the page using the pagination controls at the bottom of the page. The default number of entries shown is 20.
3. Optional. Do any of the following:
 - Specify search criteria in any of the fields (**User Name, Module, Action, Object Name, Impact Time Frame**).
 4. Click **View**. (You can customize the fields that appear by clicking **Customize > Edit** in the upper right corner.)

To examine trace logs

Each of the recorder components generates log files which you can view using the following procedure.

1. In Recorder Manager, click **Operations > Component Logs**.
2. Set an **Export Date Range**.
3. Click **Export**.



The Log Manager utility sets the size of these log files and limits the number of days of sign in information to be retained before rolling over.

Entries in the component log files take the following form:

<component><module><threadID><DateTime><TextMessage>

The following is an example from a TDM Capture log:

**[Service|WTelephone|03F0|I] 2005/07/19 00:00:04:484 ECordSync
(eRecorderSync) - initialization complete**

To review alarm history

Alarm history contains some of the events that the recorder components have triggered and logged.

1. In Recorder Manager and click **Alarms > Alarm History**.
2. Review any alarms and events raised by the recorder components.

To review Windows event viewer

Certain messages are logged into the Windows event log. In addition each alarm is also logged into the Event Viewer.

1. Access the Windows event log by clicking **Start > Control Panel > Administrative Tools**.
2. Review any events related to the recorder.

Short IP call segments are not being recorded

The default configuration for the IP Recorder will omit call segments that are shorter than two seconds long. This configuration exists because some IP phones have a tendency to continue to transmit RTP after the call has ended, and this causes problems with recording new calls that start immediately following a previous call.

By default, a phone must transmit two seconds worth of RTP before the IP Recorders views it as a real call. Because of this, segments shorter than two seconds will not be recorded.

This duration can be changed by adjusting the PacketsToIgnore setting in the IPCaptureConfig.xml located in %IMPACT360SOFTWAREDIR%\ContactStore. Most VoIP systems transmit 50 packets per second, so adjust this setting accordingly. It is recommended that you avoid making this setting smaller than 20 to avoid missing back-to-back call segments. Avaya NES systems are particularly problematic in this area so It is recommended leaving Avaya NES systems at 100 unless absolutely necessary.

```
<x:RTP>
<x:CallManagerExpress>disabled</x:CallManagerExpress>
<x:UseG729UntransmittedFrameCode>enabled</x:UseG729UntransmittedFrameCode>
<x:ActOnSSRCChange>enabled</x:ActOnSSRCChange>
<x:BreakOnSSRCChange>RTPDetection</x:BreakOnSSRCChange>
<x:PacketsToIgnore>100</x:PacketsToIgnore>
</x:RTP>
```

TDM recording issues with NGX cards

Contacts are not being recorded, or recording starts but doesn't stop, though the handset is connected correctly to the NGX card and no LOS alarms are generated. This can occur when D-channel recording control is selected, the Audio Detection Method is not "Human Voice" (Vox), and tap events are enabled for "Start on Tap" and "Stop on Tap".

This issue is caused by default "light" events not suitable for recording a particular handset type. The default trigger for D-channel recording in the TDM Recorder, when fitted with NGX cards, is the state of the handset function lights. If any function light is on, recording starts and will continue until all function lights have been turned off.

To resolve this, you can alter the handset events that start and stop recording away from the function light state, to the hook status, for example. The example below uses the "off hook" event to start recording, and the "on hook" event to stop recording.

Before changing the events used for recording control you must ascertain what events this particular handset type generates.

Procedure

1. Use the Log Manager utility to increase the Recorder logging level to level 5/DebugHigh (see [System log manager \(page 511\)](#)).
2. Restart the TDM capture service using Windows service control.
3. To make it easier to read the log files, disable all channels except the one being used to make the test calls.
4. For the channel used to generate the test logs, set,
 - the Audio Detection Method for the NGX card properties to "Signalling"
 - the Recorder Fallback Type for the Member Group to "Never (Application)"
5. Make several types of test calls (for example, inbound, outbound, extension to extension, with a transfer, with conferencing and so on), ensuring that you cover all scenarios where calls must be recorded, and those in which calls must not be recorded. Make note of the call start and stop times and extensions used — this will help you find the relevant logging for that call.
6. Examine the Capture Service log file (*eRecAudioSvc.....log*) and examine the events generated at the start and end of each test call.
7. Look for an event common to all scenarios that can be used to start recording, and one for stopping recording.

The events in the log file will be of the form EVT_xxxx. For example **EVT_OFF_HOOK** or **EVT_FUNCTION_LIGHT_ON** (refer to the Ai-Logix documentation on the TDM install discs for explanations of these events).

8. In a text editor such as Notepad, edit the TDMConfig.xml file (under %IMPACT360SOFTWAREDIR%\ContactStore\), inserting the events identified above in the STARTEVENTS and STOPEVENTS tags.

```
<x:startrevents>
  <x:event x:eventname="EVT_OFFHOOK">
    <x:subreason/>
  </x:event>
</x:startrevents>

<x:stopevents>
  <x:event x:eventname="EVT_ONHOOK">
    <x:subreason>REASON_A</x:subreason>
  </x:event>
</x:stopevents>
```

Subreason codes attached to each event can carry some additional meaning in certain cases. For instance, the 'light' events have the handset light number embedded in the event subreason. You may also include a subreason in the TDMConfig.xml file (as in the example above), to further refine either the start or stop event. If the subreason field in the .xml file is left blank it will be ignored.

The events and subreasons chosen to be used to start or stop recording must belong to a pre-approved set, which is contained in the appendix below.

More than one event can be used for either start or stop event by adding more tags to the event blocks. In this case the events are used to control the recording, meaning any of the defined start events will trigger recording, and similarly any stop event occurring terminate recording. You may mix different events for different handsets, so that some may use the default settings, while others each use a different start/stop event pair.



Events and subreasons used to start or stop recording must belong to a pre-approved set—see the table at the bottom of this section.

9. Stop and start the TDM Recorder Capture Service.
10. Reconfigure the test channel. Set,
 - the Audio Detection Method for the NGX card properties to “Signalling”
 - the Recorder Fallback Type for the Member Group to “On CTI Disconnection (Performance)”
11. Make test calls in all scenarios where recording is required, and verify that recording has taken place, and that all audio has been recorded.
12. Make test calls in all scenarios where recording is not required, verify recording has not taken place.
13. If Step 11 and Step 12 are successful, you can apply the new start and stop events to other handsets experiencing the same issues.



After testing is complete, return the logging level to 0, and restart the TDM Recorder Capture Service.

Events and Subreasons

The following are the events you may use to start or stop recording.

Events	
EVT_OFFHOOK	EVT_CFWD_CANCELED
EVT_ONHOOK	EVT_AUTO_ANSWER
EVT_LIGHT_ON	EVT_AUTO_ANSWER_CANCELED
EVT_FUNCTION_LIGHT_ON	EVT_SET_BUSY
EVT_LIGHT_OFF	EVT_SET_BUSY_CANCELED
EVT_FUNCTION_LIGHT_OFF	EVT_DESTINATION_BUSY
EVT_LIGHT_FLASHING	EVT_REORDER
EVT_FUNCTION_LIGHT_FLASHING	EVT_LIGHT VERY_FASTFLASHING
EVT_DIGIT_PRESSED	EVT_FUNCTION_LIGHT VERY_FASTFLASHING

Events	
EVT_DIGIT_RELEASED	EVT_SPEAKER_BUTTON_RELEASED
EVT_MESSAGE_CHANGE	EVT_REDIAL_BUTTON_RELEASED
EVT_STARTSTOP_ON	EVT_TRANSFER_BUTTON_RELEASED
EVT_STARTSTOP_OFF	EVT_CONF_BUTTON_RELEASED
EVT_LIGHT_FASTFLASHING	EVT_DISCONNECTED
EVT_FUNCTION_LIGHT_FASTFLASHING	EVT_CONNECTED
EVT_DOWNLOAD_STATUS	EVT_ABANDONED
EVT_FINISHED_PLAY	EVT_SUSPENDED
EVT_FUNCTION_BUTTON_PRESSED	EVT_RESUMED
EVT_FUNCTION_BUTTON_RELEASED	EVT_HELD
EVT_HOLD_BUTTON_PRESSED	EVT_RETRIEVED
EVT_HOLD_BUTTON_RELEASED	EVT_REJECTED
EVT_RELEASE_BUTTON_PRESSED	EVT_MESSAGE_BUTTON_PRESSED
EVT_RELEASE_BUTTON_RELEASED	EVT_MESSAGE_BUTTON_RELEASED
EVT_TRANSFER_BUTTON_PRESSED	EVT_SUPERVISOR_BUTTON_PRESSED
EVT_ANSWER_BUTTON_PRESSED	EVT_SUPERVISOR_BUTTON_RELEASED
EVT_SPEAKER_BUTTON_PRESSED	EVT_WRAPUP_BUTTON_PRESSED
EVT_REDIAL_BUTTON_PRESSED	EVT_WRAPUP_BUTTON_RELEASED
EVT_CONF_BUTTON_PRESSED	EVT_READY_BUTTON_PRESSED
EVT_CONference_BUTTON_PRESSED	EVT_READY_BUTTON_RELEASED
EVT_RECALL_BUTTON_PRESSED	EVT_LOGON_BUTTON_PRESSED
EVT_FEATURE_BUTTON_PRESSED	EVT_BREAK_BUTTON_PRESSED
EVT_UP_DOWN	EVT_AUDIO_CHANGE
EVT_EXIT_BUTTON_PRESSED	EVT_DISPLAY_MESSAGE
EVT_HELP_BUTTON_PRESSED	EVT_WORK_BUTTON_PRESSED
EVT_SOFT_BUTTON_PRESSED	EVT_TALLY_BUTTON_PRESSED
EVT_RING_ON	EVT_PROGRAM_BUTTON_PRESSED

Events	
EVT_RING_OFF	EVT_MUTE_BUTTON_PRESSED
EVT_LINE_BUTTON_PRESSED	EVT_ALERTING_AUTO_ANSWER
EVT_MENU_BUTTON_PRESSED	EVT_MENU_BUTTON_RELEASED
EVT_PREVIOUS_BUTTON_PRESSED	EVT_EXIT_BUTTON_RELEASED
EVT_NEXT_BUTTON_PRESSED	EVT_NEXT_BUTTON_RELEASED
EVT_LIGHT_QUICKFLASH	EVT_PREVIOUS_BUTTON_RELEASED
EVT_FUNCTION_LIGHT_QUICKFLASH	EVT_SHIFT_BUTTON_PRESSED
EVT_AUDIO_ON	EVT_SHIFT_BUTTON_RELEASED
EVT_AUDIO_OFF	EVT_PAGE_BUTTON_PRESSED
EVT_DISPLAY_CLOCK	EVT_PAGE_BUTTON_RELEASED
EVT_DISPLAY_TIMER	EVT_SOFT_BUTTON_RELEASED
EVT_DISPLAY_CLEAR	EVT_LINE_LIGHT_OFF
EVT_CFWD	EVT_LINE_LIGHT_ON
EVT_LINE_LIGHT_FLASHING	EVT_LINE_LIGHT_FASTFLASHING
EVT_LINE_LIGHT VERY_FASTFLASHING	EVT_LINE_LIGHT_QUICKFLASH
EVT_LINE_LIGHT_WINK	EVT_FEATURE_LIGHT_OFF
EVT_LINE_LIGHT_SLOW_WINK	EVT_FEATURE_LIGHT_ON
EVT_FEATURE_LIGHT_FLASHING	EVT_FEATURE_LIGHT_FASTFLASHING
EVT_FEATURE_LIGHT VERY_FASTFLASHING	EVT_FEATURE_LIGHT_QUICKFLASH
EVT_FEATURE_LIGHT_WINK	EVT_FEATURE_LIGHT_SLOW_WINK
EVT_SPEAKER_LIGHT_OFF	EVT_SPEAKER_LIGHT_ON
EVT_SPEAKER_LIGHT_FLASHING	EVT_SPEAKER_LIGHT_FASTFLASHING
EVT_SPEAKER_LIGHT VERY_FASTFLASHING	EVT_SPEAKER_LIGHT_QUICKFLASH
EVT_SPEAKER_LIGHT_WINK	EVT_SPEAKER_LIGHT_SLOW_WINK
EVT_MIC_LIGHT_OFF	EVT_MIC_LIGHT_OFF
EVT_MIC_LIGHT_FLASHING	EVT_MIC_LIGHT_ON
EVT_MIC_LIGHT VERY_FASTFLASHING	EVT_MIC_LIGHT_FASTFLASHING

Events	
EVT_MIC_LIGHT_QUICKFLASH	EVT_MIC_LIGHT_WINK
EVT_MIC_LIGHT_SLOW_WINK	EVT_HOLD_LIGHT_OFF
EVT_HOLD_LIGHT_ON	EVT_HOLD_LIGHT_FLASHING
EVT_HOLD_LIGHT_FASTFLASHING	EVT_HOLD_LIGHT_VERY_FASTFLASHING
EVT_HOLD_LIGHT_QUICKFLASH	EVT_RELEASE_LIGHT_OFF
EVT_RELEASE_LIGHT_ON	EVT_RELEASE_LIGHT_FLASHING
EVT_RELEASE_LIGHT_FASTFLASHING	EVT_RELEASE_LIGHT_VERY_FASTFLASHING
EVT_RELEASE_LIGHT_QUICKFLASH	EVT_HELP_LIGHT_OFF
EVT_HELP_LIGHT_ON	EVT_HELP_LIGHT_FLASHING
EVT_HELP_LIGHT_FASTFLASHING	EVT_HELP_LIGHT_VERY_FASTFLASHING
EVT_HELP_LIGHT_QUICKFLASH	EVT_SUPERVISOR_LIGHT_OFF
EVT_SUPERVISOR_LIGHT_ON	EVT_SUPERVISOR_LIGHT_FLASHING
EVT_SUPERVISOR_LIGHT_FASTFLASHING	EVT_SUPERVISOR_LIGHT_VERY_FASTFLASHING
EVT_SUPERVISOR_LIGHT_QUICKFLASH	EVT_READY_LIGHT_OFF
EVT_READY_LIGHT_ON	EVT_READY_LIGHT_FLASHING
EVT_READY_LIGHT_FASTFLASHING	EVT_READY_LIGHT_VERY_FASTFLASHING
EVT_READY_LIGHT_QUICKFLASH	EVT_LOGON_LIGHT_OFF
EVT_LOGON_LIGHT_ON	EVT_LOGON_LIGHT_FLASHING
EVT_LOGON_LIGHT_FASTFLASHING	EVT_LOGON_LIGHT_VERY_FASTFLASHING
EVT_LOGON_LIGHT_QUICKFLASH	EVT_WRAPUP_LIGHT_OFF
EVT_WRAPUP_LIGHT_ON	EVT_WRAPUP_LIGHT_FLASHING
EVT_WRAPUP_LIGHT_FASTFLASHING	EVT_WRAPUP_LIGHT_VERY_FASTFLASHING
EVT_WRAPUP_LIGHT_QUICKFLASH	EVT_RING_LIGHT_OFF
EVT_RING_LIGHT_ON	EVT_RING_LIGHT_FLASHING
EVT_RING_LIGHT_FASTFLASHING	EVT_RING_LIGHT_VERY_FASTFLASHING
EVT_ANSWER_LIGHT_OFF	EVT_RING_LIGHT_QUICKFLASH
EVT_ANSWER_LIGHT_ON	EVT_ANSWER_LIGHT_FLASHING

Events	
EVT_ANSWER_LIGHT_FASTFLASHING	EVT_ANSWER_LIGHT_VERY_FASTFLASHING
EVT_ANSWER_LIGHT_QUICKFLASH	EVT_PROGRAM_LIGHT_OFF
EVT_PROGRAM_LIGHT_ON	EVT_PROGRAM_LIGHT_FLASHING
EVT_PROGRAM_LIGHT_FASTFLASHING	EVT_PROGRAM_LIGHT_VERY_FASTFLASHING
EVT_PROGRAM_LIGHT_QUICKFLASH	EVT_PROGRAM_LIGHT_WINK
EVT_PROGRAM_LIGHT_MEDIUM_WINK	EVT_MESSAGE_LIGHT_OFF
EVT_MESSAGE_LIGHT_ON	EVT_MESSAGE_LIGHT_FLASHING
EVT_MESSAGE_LIGHT_FASTFLASHING	EVT_MESSAGE_LIGHT_VERY_FASTFLASHING
EVT_MESSAGE_LIGHT_QUICKFLASH	EVT_MESSAGE_LIGHT_WINK
EVT_TRANSFER_LIGHT_OFF	EVT_MESSAGE_LIGHT_SLOW_WINK
EVT_TRANSFER_LIGHT_ON	EVT_TRANSFER_LIGHT_FLASHING
EVT_TRANSFER_LIGHT_FASTFLASHING	EVT_TRANSFER_LIGHT_VERY_FASTFLASHING
EVT_TRANSFER_LIGHT_QUICKFLASH	EVT_TRANSFER_LIGHT_WINK
EVT_TRANSFER_LIGHT_MEDIUM_WINK	EVT_CONFERENCE_LIGHT_OFF
EVT_CONFERENCE_LIGHT_ON	EVT_CONFERENCE_LIGHT_FLASHING
EVT_CONFERENCE_LIGHT_FASTFLASHING	EVT_CONFERENCE_LIGHT_VERY_FASTFLASHING
EVT_CONFERENCE_LIGHT_QUICKFLASH	EVT_CONFERENCE_LIGHT_WINK
EVT_CONFERENCE_LIGHT_MEDIUM_WINK	EVT_SOFT_LIGHT_OFF
EVT_SOFT_LIGHT_ON	EVT_SOFT_LIGHT_FLASHING
EVT_SOFT_LIGHT_FASTFLASHING	EVT_SOFT_LIGHT_VERY_FASTFLASHING
EVT_SOFT_LIGHT_QUICKFLASH	EVT_MENU_LIGHT_OFF
EVT_MENU_LIGHT_ON	EVT_MENU_LIGHT_FLASHING
EVT_MENU_LIGHT_FASTFLASHING	EVT_MENU_LIGHT_VERY_FASTFLASHING
EVT_MENU_LIGHT_QUICKFLASH	EVT_CALLWAITING_LIGHT_OFF
EVT_CALLWAITING_LIGHT_ON	EVT_CALLWAITING_LIGHT_FLASHING
EVT_CALLWAITING_LIGHT_FASTFLASHING	EVT_CALLWAITING_LIGHT_VERY_FASTFLASHIN
EVT_CALLWAITING_LIGHT_QUICKFLASH	EVT_REDIAL_LIGHT_OFF

Events	
EVT_REDIAL_LIGHT_ON	EVT_REDIAL_LIGHT_FLASHING
EVT_REDIAL_LIGHT_FASTFLASHING	EVT_REDIAL_LIGHT_VERY_FASTFLASHING
EVT_REDIAL_LIGHT_QUICKFLASH	EVT_PAGE_LIGHT_OFF
EVT_PAGE_LIGHT_ON	EVT_PAGE_LIGHT_FLASHING
EVT_PAGE_LIGHT_FASTFLASHING	EVT_PAGE_LIGHT_VERY_FASTFLASHING
EVT_PAGE_LIGHT_QUICKFLASH	EVT_CTRL_BUTTON_PRESSED
EVT_CTRL_BUTTON_RELEASED	EVT_CANCEL_BUTTON_PRESSED
EVT_CANCEL_BUTTON_RELEASED	EVT_MIC_BUTTON_PRESSED
EVT_FLASH_BUTTON_PRESSED	EVT_MIC_BUTTON_RELEASED
EVT_DIRECTORY_BUTTON_PRESSED	EVT_FLASH_BUTTON_RELEASED
EVT_HANDSFREE_BUTTON_PRESSED	EVT_DIRECTORY_BUTTON_RELEASED
EVT_RINGTONE_BUTTON_PRESSED	EVT_HANDSFREE_BUTTON_RELEASED
EVT_SAVE_BUTTON_PRESSED	EVT_RINGTONE_BUTTON_RELEASED
EVT_SAVE_BUTTON_RELEASED	EVT_SAVE_BUTTON_RELEASED
EVT_MUTE_LIGHT_OFF	EVT_MUTE_LIGHT_ON
EVT_MUTE_LIGHT_FLASHING	EVT_MUTE_LIGHT_FASTFLASHING
EVT_MUTE_LIGHT_VERY_FASTFLASHING	EVT_MUTE_LIGHT_QUICKFLASH
EVT_MUTE_LIGHT_WINK	EVT_MUTE_LIGHT_SLOW_WINK
EVT_MUTE_LIGHT_MEDIUM_WINK	EVT_HANDSFREE_LIGHT_OFF
EVT_HANDSFREE_LIGHT_ON	EVT_HANDSFREE_LIGHT_FLASHING
EVT_HANDSFREE_LIGHT_FASTFLASHING	EVT_HANDSFREE_LIGHT_VERY_FASTFLASHING
EVT_HANDSFREE_LIGHT_QUICKFLASH	EVT_DIRECTORY_LIGHT_OFF
EVT_DIRECTORY_LIGHT_ON	EVT_DIRECTORY_LIGHT_FLASHING
EVT_DIRECTORY_LIGHT_FASTFLASHING	EVT_DIRECTORY_LIGHT_VERY_FASTFLASHING
EVT_DIRECTORY_LIGHT_QUICKFLASH	EVT_RINGTONE_LIGHT_OFF
EVT_RINGTONE_LIGHT_ON	EVT_RINGTONE_LIGHT_FLASHING
EVT_RINGTONE_LIGHT_FASTFLASHING	EVT_RINGTONE_LIGHT_VERY_FASTFLASHING

Events	
EVT_RINGTONE_LIGHT_QUICKFLASH	EVT_SAVE_LIGHT_OFF
EVT_SAVE_LIGHT_ON	EVT_SAVE_LIGHT_FLASHING
EVT_SAVE_LIGHT_FASTFLASHING	EVT_SAVE_LIGHT_VERY_FASTFLASHING
EVT_SAVE_LIGHT_QUICKFLASH	EVT_FUNCTION_LIGHT_WINK
EVT_FUNCTION_LIGHT_SLOW_WINK	EVT_FUNCTION_LIGHT_MEDIUM_WINK
EVT_CALLWAITING_BUTTON_RELEASED	EVT_PARK_BUTTON_PRESSED
EVT_PARK_BUTTON_RELEASED	EVT_NEWCALL_BUTTON_PRESSED
EVT_NEWCALL_BUTTON_RELEASED	EVT_PARK_LIGHT_OFF
EVT_PARK_LIGHT_ON	EVT_PARK_LIGHT_FLASHING
EVT_PARK_LIGHT_FASTFLASHING	EVT_PARK_LIGHT_VERY_FASTFLASHING
EVT_PARK_LIGHT_QUICKFLASH	EVT_SCROLL_BUTTON_PRESSED
EVT_SCROLL_BUTTON_RELEASED	EVT_DIVERT_BUTTON_PRESSED
EVT_DIVERT_BUTTON_RELEASED	EVT_GROUP_BUTTON_PRESSED
EVT_GROUP_BUTTON_RELEASED	EVT_SPEEDDIAL_BUTTON_PRESSED
EVT_SPEEDDIAL_BUTTON_RELEASED	EVT_DND_BUTTON_PRESSED
EVT_DND_BUTTON_RELEASED	EVT_ENTER_BUTTON_PRESSED
EVT_ENTER_BUTTON_RELEASED	EVT_CLEAR_BUTTON_PRESSED
EVT_CLEAR_BUTTON_RELEASED	EVT_DESTINATION_BUTTON_PRESSED
EVT_DESTINATION_BUTTON_RELEASED	EVT_DND_LIGHT_OFF
EVT_DND_LIGHT_ON	EVT_DND_LIGHT_FLASHING
EVT_DND_LIGHT_FASTFLASHING	EVT_DND_LIGHT_VERY_FASTFLASHING
EVT_DND_LIGHT_QUICKFLASH	EVT_DND_LIGHT_WINK
EVT_DND_LIGHT_SLOW_WINK	EVT_DND_LIGHT_MEDIUM_WINK
EVT_GROUP_LIGHT_OFF	EVT_GROUP_LIGHT_ON
EVT_GROUP_LIGHT_FLASHING	EVT_GROUP_LIGHT_FASTFLASHING
EVT_GROUP_LIGHT_VERY_FASTFLASHING	EVT_GROUP_LIGHT_QUICKFLASH
EVT_DIVERT_LIGHT_OFF	EVT_DIVERT_LIGHT_ON

Events	
EVT_DIVERT_LIGHT_FLASHING	EVT_DIVERT_LIGHT_FASTFLASHING
EVT_DIVERT_LIGHT_VERY_FASTFLASHING	EVT_DIVERT_LIGHT_QUICKFLASH
EVT_SCROLL_LIGHT_OFF	EVT_SCROLL_LIGHT_ON
EVT_SCROLL_LIGHT_FLASHING	EVT_SCROLL_LIGHT_FASTFLASHING
EVT_SCROLL_LIGHT_VERY_FASTFLASHING	EVT_SCROLL_LIGHT_QUICKFLASH
EVT_CALLBACK_BUTTON_PRESSED	EVT_CALLBACK_BUTTON_RELEASED
EVT_FLASH_LIGHT_OFF	EVT_FLASH_LIGHT_ON
EVT_FLASH_LIGHT_FLASHING	EVT_FLASH_LIGHT_FASTFLASHING
EVT_FLASH_LIGHT_VERY_FASTFLASHING	EVT_FLASH_LIGHT_QUICKFLASH
EVT_FLASH_LIGHT_WINK	EVT_MODE_BUTTON_RELEASED
EVT_SPEAKER_LIGHT_MEDIUM_WINK	EVT_MESSAGE_LIGHT_MEDIUM_WINK
EVT_OFFHOOK	EVT_ONHOOK
EVT_LIGHT_ON	EVT_FUNCTION_LIGHT_ON
EVT_LIGHT_OFF	EVT_FUNCTION_LIGHT_OFF
EVT_LIGHT_FLASHING	EVT_FUNCTION_LIGHT_FLASHING
EVT_DIGIT_PRESSED	EVT_DIGIT_RELEASED
EVT_MESSAGE_CHANGE	EVT_STARTSTOP_ON
EVT_STARTSTOP_OFF	EVT_LIGHT_FASTFLASHING
EVT_FUNCTION_LIGHT_FASTFLASHING	EVT_DOWNLOAD_STATUS
EVT_FINISHED_PLAY	EVT_FUNCTION_BUTTON_PRESSED
EVT_FUNCTION_BUTTON_RELEASED	EVT_HOLD_BUTTON_PRESSED
EVT_HOLD_BUTTON_RELEASED	EVT_RELEASE_BUTTON_PRESSED
EVT_RELEASE_BUTTON_RELEASED	EVT_TRANSFER_BUTTON_PRESSED
EVT_ANSWER_BUTTON_PRESSED	EVT_SPEAKER_BUTTON_PRESSED
EVT_REDIAL_BUTTON_PRESSED	EVT_CONF_BUTTON_PRESSED
EVT_CONFERENCE_BUTTON_PRESSED	EVT_RECALL_BUTTON_PRESSED
EVT_FEATURE_BUTTON_PRESSED	EVT_UP_DOWN

Events	
EVT_EXIT_BUTTON_PRESSED	EVT_HELP_BUTTON_PRESSED
EVT_SOFT_BUTTON_PRESSED	EVT_RING_ON
EVT_RING_OFF	EVT_LINE_BUTTON_PRESSED
EVT_MENU_BUTTON_PRESSED	EVT_PREVIOUS_BUTTON_PRESSED
EVT_NEXT_BUTTON_PRESSED	EVT_LIGHT_QUICKFLASH
EVT_FUNCTION_LIGHT_QUICKFLASH	EVT_AUDIO_ON
EVT_AUDIO_OFF	EVT_DISPLAY_CLOCK
EVT_DISPLAY_TIMER	EVT_DISPLAY_CLEAR
EVT_CFWD	EVT_CFWD_CANCELED
EVT_AUTO_ANSWER	EVT_AUTO_ANSWER_CANCELED
EVT_SET_BUSY	EVT_SET_BUSY_CANCELED
EVT_DESTINATION_BUSY	EVT_REORDER
EVT_LIGHT VERY_FASTFLASHING	EVT_FUNCTION_LIGHT VERY_FASTFLASHING
EVT_SPEAKER_BUTTON_RELEASED	EVT_REDIAL_BUTTON_RELEASED
EVT_TRANSFER_BUTTON_RELEASED	EVT_CONF_BUTTON_RELEASED
EVT_DISCONNECTED	EVT_CONNECTED
EVT_ABANDONED	EVT_SUSPENDED
EVT_RESUMED	EVT_HELD
EVT_RETRIEVED	EVT_REJECTED
EVT_MESSAGE_BUTTON_PRESSED	EVT_MESSAGE_BUTTON_RELEASED
EVT_SUPERVISOR_BUTTON_PRESSED	EVT_SUPERVISOR_BUTTON_RELEASED
EVT_WRAPUP_BUTTON_PRESSED	EVT_WRAPUP_BUTTON_RELEASED
EVT_READY_BUTTON_PRESSED	EVT_READY_BUTTON_RELEASED
EVT_LOGON_BUTTON_PRESSED	EVT_BREAK_BUTTON_PRESSED
EVT_AUDIO_CHANGE	EVT_DISPLAY_MESSAGE
EVT_WORK_BUTTON_PRESSED	EVT_TALLY_BUTTON_PRESSED
EVT_PROGRAM_BUTTON_PRESSED	EVT_MUTE_BUTTON_PRESSED

Events	
EVT_ALERTING_AUTO_ANSWER	EVT_MENU_BUTTON_RELEASED
EVT_EXIT_BUTTON_RELEASED	EVT_NEXT_BUTTON_RELEASED
EVT_PREVIOUS_BUTTON_RELEASED	EVT_SHIFT_BUTTON_PRESSED
EVT_SHIFT_BUTTON_RELEASED	EVT_PAGE_BUTTON_PRESSED
EVT_PAGE_BUTTON_RELEASED	EVT_SOFT_BUTTON_RELEASED
EVT_LINE_LIGHT_OFF	EVT_LINE_LIGHT_ON
EVT_LINE_LIGHT_FLASHING	EVT_LINE_LIGHT_FASTFLASHING
EVT_LINE_LIGHT VERY_FASTFLASHING	EVT_LINE_LIGHT_QUICKFLASH
EVT_LINE_LIGHT_WINK	EVT_LINE_LIGHT_SLOW_WINK
EVT_FEATURE_LIGHT_OFF	EVT_FEATURE_LIGHT_ON
EVT_FEATURE_LIGHT_FLASHING	EVT_FEATURE_LIGHT_FASTFLASHING
EVT_FEATURE_LIGHT VERY_FASTFLASHING	EVT_FEATURE_LIGHT_QUICKFLASH
EVT_FEATURE_LIGHT_WINK	EVT_FEATURE_LIGHT_SLOW_WINK
EVT_SPEAKER_LIGHT_OFF	EVT_SPEAKER_LIGHT_ON
EVT_SPEAKER_LIGHT_FLASHING	EVT_SPEAKER_LIGHT_FASTFLASHING
EVT_SPEAKER_LIGHT VERY_FASTFLASHING	EVT_SPEAKER_LIGHT_QUICKFLASH
EVT_SPEAKER_LIGHT_WINK	EVT_SPEAKER_LIGHT_SLOW_WINK
EVT_MIC_LIGHT_OFF	EVT_MIC_LIGHT_ON
EVT_MIC_LIGHT_FLASHING	EVT_MIC_LIGHT_FASTFLASHING
EVT_MIC_LIGHT VERY_FASTFLASHING	EVT_MIC_LIGHT_QUICKFLASH
EVT_MIC_LIGHT_WINK	EVT_MIC_LIGHT_SLOW_WINK
EVT_HOLD_LIGHT_OFF	EVT_HOLD_LIGHT_ON
EVT_HOLD_LIGHT_FLASHING	EVT_HOLD_LIGHT_FASTFLASHING
EVT_HOLD_LIGHT VERY_FASTFLASHING	EVT_HOLD_LIGHT_QUICKFLASH
EVT_RELEASE_LIGHT_OFF	EVT_RELEASE_LIGHT_ON
EVT_RELEASE_LIGHT_FLASHING	EVT_RELEASE_LIGHT_FASTFLASHING
EVT_RELEASE_LIGHT VERY_FASTFLASHING	EVT_RELEASE_LIGHT_QUICKFLASH

Events	
EVT_HELP_LIGHT_OFF	EVT_HELP_LIGHT_ON
EVT_HELP_LIGHT_FLASHING	EVT_HELP_LIGHT_FASTFLASHING
EVT_HELP_LIGHT_VERY_FASTFLASHING	EVT_HELP_LIGHT_QUICKFLASH
EVT_SUPERVISOR_LIGHT_OFF	EVT_SUPERVISOR_LIGHT_ON
EVT_SUPERVISOR_LIGHT_FLASHING	EVT_SUPERVISOR_LIGHT_FASTFLASHING
EVT_SUPERVISOR_LIGHT_VERY_FASTFLASHING	EVT_SUPERVISOR_LIGHT_QUICKFLASH
EVT_READY_LIGHT_OFF	EVT_READY_LIGHT_ON
EVT_READY_LIGHT_FLASHING	EVT_READY_LIGHT_FASTFLASHING
EVT_READY_LIGHT_VERY_FASTFLASHING	EVT_READY_LIGHT_QUICKFLASH
EVT_LOGON_LIGHT_OFF	EVT_LOGON_LIGHT_ON
EVT_LOGON_LIGHT_FLASHING	EVT_LOGON_LIGHT_FASTFLASHING
EVT_LOGON_LIGHT_VERY_FASTFLASHING	EVT_LOGON_LIGHT_QUICKFLASH
EVT_WRAPUP_LIGHT_OFF	EVT_WRAPUP_LIGHT_ON
EVT_WRAPUP_LIGHT_FLASHING	EVT_WRAPUP_LIGHT_FASTFLASHING
EVT_WRAPUP_LIGHT_VERY_FASTFLASHING	EVT_WRAPUP_LIGHT_QUICKFLASH
EVT_RING_LIGHT_OFF	EVT_RING_LIGHT_ON
EVT_RING_LIGHT_FLASHING	EVT_RING_LIGHT_FASTFLASHING
EVT_RING_LIGHT_VERY_FASTFLASHING	EVT_RING_LIGHT_QUICKFLASH
EVT_ANSWER_LIGHT_OFF	EVT_ANSWER_LIGHT_ON
EVT_ANSWER_LIGHT_FLASHING	EVT_ANSWER_LIGHT_FASTFLASHING
EVT_ANSWER_LIGHT_VERY_FASTFLASHING	EVT_ANSWER_LIGHT_QUICKFLASH
EVT_PROGRAM_LIGHT_OFF	EVT_PROGRAM_LIGHT_ON
EVT_PROGRAM_LIGHT_FLASHING	EVT_PROGRAM_LIGHT_FASTFLASHING
EVT_PROGRAM_LIGHT_VERY_FASTFLASHING	EVT_PROGRAM_LIGHT_QUICKFLASH
EVT_PROGRAM_LIGHT_WINK	EVT_PROGRAM_LIGHT_MEDIUM_WINK
EVT_MESSAGE_LIGHT_OFF	EVT_MESSAGE_LIGHT_ON
EVT_MESSAGE_LIGHT_FLASHING	EVT_MESSAGE_LIGHT_FASTFLASHING

Events	
EVT_MESSAGE_LIGHT_VERY_FASTFLASHING	EVT_MESSAGE_LIGHT_QUICKFLASH
EVT_MESSAGE_LIGHT_WINK	EVT_MESSAGE_LIGHT_SLOW_WINK
EVT_TRANSFER_LIGHT_OFF	EVT_TRANSFER_LIGHT_ON
EVT_TRANSFER_LIGHT_FLASHING	EVT_TRANSFER_LIGHT_FASTFLASHING
EVT_TRANSFER_LIGHT_VERY_FASTFLASHING	EVT_TRANSFER_LIGHT_QUICKFLASH
EVT_TRANSFER_LIGHT_WINK	EVT_TRANSFER_LIGHT_MEDIUM_WINK
EVT_CONFERENCE_LIGHT_OFF	EVT_CONFERENCE_LIGHT_ON
EVT_CONFERENCE_LIGHT_FLASHING	EVT_CONFERENCE_LIGHT_FASTFLASHING
EVT_CONFERENCE_LIGHT_VERY_FASTFLASHING	EVT_CONFERENCE_LIGHT_QUICKFLASH
EVT_CONFERENCE_LIGHT_WINK	EVT_CONFERENCE_LIGHT_MEDIUM_WINK
EVT_SOFT_LIGHT_OFF	EVT_SOFT_LIGHT_ON
EVT_SOFT_LIGHT_FLASHING	EVT_SOFT_LIGHT_FASTFLASHING
EVT_SOFT_LIGHT_VERY_FASTFLASHING	EVT_SOFT_LIGHT_QUICKFLASH
EVT_MENU_LIGHT_OFF	EVT_MENU_LIGHT_ON
EVT_MENU_LIGHT_FLASHING	EVT_MENU_LIGHT_FASTFLASHING
EVT_MENU_LIGHT_VERY_FASTFLASHING	EVT_MENU_LIGHT_QUICKFLASH
EVT_CALLWAITING_LIGHT_OFF	EVT_CALLWAITING_LIGHT_ON
EVT_CALLWAITING_LIGHT_FLASHING	EVT_CALLWAITING_LIGHT_FASTFLASHING
EVT_CALLWAITING_LIGHT_VERY_FASTFLASHIN	EVT_CALLWAITING_LIGHT_QUICKFLASH
EVT_REDIAL_LIGHT_OFF	EVT_REDIAL_LIGHT_ON
EVT_REDIAL_LIGHT_FLASHING	EVT_REDIAL_LIGHT_FASTFLASHING
EVT_REDIAL_LIGHT_VERY_FASTFLASHING	EVT_REDIAL_LIGHT_QUICKFLASH
EVT_PAGE_LIGHT_OFF	EVT_PAGE_LIGHT_ON
EVT_PAGE_LIGHT_FLASHING	EVT_PAGE_LIGHT_FASTFLASHING
EVT_PAGE_LIGHT_VERY_FASTFLASHING	EVT_PAGE_LIGHT_QUICKFLASH
EVT_CTRL_BUTTON_PRESSED	EVT_CTRL_BUTTON_RELEASED
EVT_CANCEL_BUTTON_PRESSED	EVT_CANCEL_BUTTON_RELEASED

Events	
EVT_MIC_BUTTON_PRESSED	EVT_MIC_BUTTON_RELEASED
EVT_FLASH_BUTTON_PRESSED	EVT_FLASH_BUTTON_RELEASED
EVT_DIRECTORY_BUTTON_PRESSED	EVT_DIRECTORY_BUTTON_RELEASED
EVT_HANDSFREE_BUTTON_PRESSED	EVT_HANDSFREE_BUTTON_RELEASED
EVT_RINGTONE_BUTTON_PRESSED	EVT_RINGTONE_BUTTON_RELEASED
EVT_SAVE_BUTTON_PRESSED	EVT_SAVE_BUTTON_RELEASED
EVT_MUTE_LIGHT_OFF	EVT_MUTE_LIGHT_ON
EVT_MUTE_LIGHT_FLASHING	EVT_MUTE_LIGHT_FASTFLASHING
EVT_MUTE_LIGHT_VERY_FASTFLASHING	EVT_MUTE_LIGHT_QUICKFLASH
EVT_MUTE_LIGHT_WINK	EVT_MUTE_LIGHT_SLOW_WINK
EVT_MUTE_LIGHT_MEDIUM_WINK	EVT_HANDSFREE_LIGHT_OFF
EVT_HANDSFREE_LIGHT_ON	EVT_HANDSFREE_LIGHT_FLASHING
EVT_HANDSFREE_LIGHT_FASTFLASHING	EVT_HANDSFREE_LIGHT_VERY_FASTFLASHING
EVT_HANDSFREE_LIGHT_QUICKFLASH	EVT_DIRECTORY_LIGHT_OFF
EVT_DIRECTORY_LIGHT_ON	EVT_DIRECTORY_LIGHT_FLASHING
EVT_DIRECTORY_LIGHT_FASTFLASHING	EVT_DIRECTORY_LIGHT_VERY_FASTFLASHING
EVT_DIRECTORY_LIGHT_QUICKFLASH	EVT_RINGTONE_LIGHT_OFF
EVT_RINGTONE_LIGHT_ON	EVT_RINGTONE_LIGHT_FLASHING
EVT_RINGTONE_LIGHT_FASTFLASHING	EVT_RINGTONE_LIGHT_VERY_FASTFLASHING
EVT_RINGTONE_LIGHT_QUICKFLASH	EVT_SAVE_LIGHT_OFF
EVT_SAVE_LIGHT_ON	EVT_SAVE_LIGHT_FLASHING
EVT_SAVE_LIGHT_FASTFLASHING	EVT_SAVE_LIGHT_VERY_FASTFLASHING
EVT_SAVE_LIGHT_QUICKFLASH	EVT_FUNCTION_LIGHT_WINK
EVT_FUNCTION_LIGHT_SLOW_WINK	EVT_FUNCTION_LIGHT_MEDIUM_WINK
EVT_CALLWAITING_BUTTON_RELEASED	EVT_PARK_BUTTON_PRESSED
EVT_PARK_BUTTON_RELEASED	EVT_NEWCALL_BUTTON_PRESSED
EVT_NEWCALL_BUTTON_RELEASED	EVT_PARK_LIGHT_OFF

Events	
EVT_PARK_LIGHT_ON	EVT_PARK_LIGHT_FLASHING
EVT_PARK_LIGHT_FASTFLASHING	EVT_PARK_LIGHT_VERY_FASTFLASHING
EVT_PARK_LIGHT_QUICKFLASH	EVT_SCROLL_BUTTON_PRESSED
EVT_SCROLL_BUTTON_RELEASED	EVT_DIVERT_BUTTON_PRESSED
EVT_DIVERT_BUTTON_RELEASED	EVT_GROUP_BUTTON_PRESSED
EVT_GROUP_BUTTON_RELEASED	EVT_SPEEDEDIAL_BUTTON_PRESSED
EVT_SPEEDEDIAL_BUTTON_RELEASED	EVT_DND_BUTTON_PRESSED
EVT_DND_BUTTON_RELEASED	EVT_ENTER_BUTTON_PRESSED
EVT_ENTER_BUTTON_RELEASED	EVT_CLEAR_BUTTON_PRESSED
EVT_CLEAR_BUTTON_RELEASED	EVT_DESTINATION_BUTTON_PRESSED
EVT_DESTINATION_BUTTON_RELEASED	EVT_DND_LIGHT_OFF
EVT_DND_LIGHT_ON	EVT_DND_LIGHT_FLASHING
EVT_DND_LIGHT_FASTFLASHING	EVT_DND_LIGHT_VERY_FASTFLASHING
EVT_DND_LIGHT_QUICKFLASH	EVT_DND_LIGHT_WINK
EVT_DND_LIGHT_SLOW_WINK	EVT_DND_LIGHT_MEDIUM_WINK
EVT_GROUP_LIGHT_OFF	EVT_GROUP_LIGHT_ON
EVT_GROUP_LIGHT_FLASHING	EVT_GROUP_LIGHT_FASTFLASHING
EVT_GROUP_LIGHT_VERY_FASTFLASHING	EVT_GROUP_LIGHT_QUICKFLASH
EVT_DIVERT_LIGHT_OFF	EVT_DIVERT_LIGHT_ON
EVT_DIVERT_LIGHT_FLASHING	EVT_DIVERT_LIGHT_FASTFLASHING
EVT_DIVERT_LIGHT_VERY_FASTFLASHING	EVT_DIVERT_LIGHT_QUICKFLASH
EVT_SCROLL_LIGHT_OFF	EVT_SCROLL_LIGHT_ON
EVT_SCROLL_LIGHT_FLASHING	EVT_SCROLL_LIGHT_FASTFLASHING
EVT_SCROLL_LIGHT_VERY_FASTFLASHING	EVT_SCROLL_LIGHT_QUICKFLASH
EVT_CALLBACK_BUTTON_PRESSED	EVT_CALLBACK_BUTTON_RELEASED
EVT_FLASH_LIGHT_OFF	EVT_FLASH_LIGHT_ON
EVT_FLASH_LIGHT_FLASHING	EVT_FLASH_LIGHT_FASTFLASHING

Events	
EVT_FLASH_LIGHT_VERY_FASTFLASHING	EVT_FLASH_LIGHT_QUICKFLASH
EVT_FLASH_LIGHT_WINK	EVT_MODE_BUTTON_RELEASED
EVT_SPEAKER_LIGHT_MEDIUM_WINK	EVT_MESSAGE_LIGHT_MEDIUM_WINK

The following are the subreasons you may use in conjunction with the events above. Please note that many of these are environment-specific. In addition to the codes above numbers 0 through to 256 may be entered (as text) into the subreason field.

Subreasons	
ASPECT_L10_GREEN_ON (258)	ASPECT_L10_GREEN_OFF (1794)
LUCENT_GREEN_LIGHT (256)	DONT_CARE (-1)
GREEN_FUNCTION_LAMP_ON (256)	RED_FUNCTION_LAMP_ON (512)
AMBER_FUNCTION_LAMP_ON (1024)	LUCENT_GREEN_LIGHT (256)
ASPECT_L8_GREEN_LIGHT (256)	LUCENT_GREEN_LIGHT_1 (257)
ASPECT_L9_GREEN_LIGHT (257)	LUCENT_GREEN_LIGHT_2 (258)
ASPECT_L10_GREEN_LIGHT (258)	LUCENT_GREEN_LIGHT_3 (259)
ASPECT_L10_GREEN_ON (258)	
ASPECT_L10_GREEN_OFF (1794)	
ASPECT_GREEN_LAMP_OFF (1792)	

Reset channel mechanisms for NGX cards

In the event of EVT_MAXTIME, edit the TDMConfig.xml file and enable/disable the Reset Channel mechanism for NGX cards. The reset channel is enabled by default.

Procedure

1. In a text editor such as NotePad, edit the following file:
`%IMPACT360SOFTWAREDIR%\ContactStore\TDMConfig.xml`
2. Find the following setting in the TDMConfig.xml file:
`<x:maskingtoneamplitude>0.25</x:maskingtoneamplitude>`
3. To enable the reset channel, after the maskingtoneamplitude setting found in step 2, add the following:
`<x:enableresetchannel>true</x:enableresetchannel>`
`<x:maxresetchanneldelay>3600</x:maxresetchanneldelay>`
4. Save the TDMConfig.xml file.

5. Go to the following location:

`%IMPACT360SOFTWARE%\ContactStore\Tools\`

6. To prevent file tampering alarms, run the following command:

`checksumutil -g %IMPACT360SOFTWAREDIR%\ContactStore\<TDMConfig.xml>`

Related topics

[Correct Tampering from a Command Line \(page 544\)](#)

Checksum mismatches

Correcting checksum mismatches is part of the tamper-proofing recovery procedure. A checksum string is inserted for security into all configuration files, and upon detection, should be examined and corrected if necessary.

- [Correct Tampering \(page 542\)](#)
- [Correct Tampering from a Command Line \(page 544\)](#)

Correct Tampering

Use Enterprise Manager to correct configuration files that have been identified, through system alarms, as potentially tampered with. All files are tamper-proofed automatically, using a checksum string inserted into configuration files, allowing the detection and reporting of mismatched checksums. The following table lists common files and the action to take.



The following is a partial list. In most cases, the solution is to save the settings in the application area associated with the xml file. For a complete list contact Verint Field Services.

File	To update the checksum
Recorder configuration files (all XML files in <Install Directory>\ContactStore)	
RecorderGeneral.xml	Recorder Manager > General Setup > Recorder Settings > Save
AlarmConfig.xml	Recorder Manager > Alarms > Alarm Settings or Notification Profile > Save
ArchiverConfig.xml	Recorder Manager > Operations > Archive > Save
DiskManagerConfig.xml	Recorder Manager > General Setup > Disk Management > Save
CompressorConfig.xml	Recorder Manager > General Setup > Compression > Save
ConsolidatorConfig.xml	Recorder Manager > General Setup > Database Settings > Save
IPCaptureConfig.xml	Recorder Manager > General Setup > Capture Settings > Save
ScreenConfig.xml	Recorder Manager > General Setup > Recorder Settings > Save
SFIConfig.xml	Enterprise Manager > System Management > Enterprise > Security > Save
TDMConfig.xml	Recorder Manager > General Setup > Voice Cards > Card > Save
Integration Service configuration files (all XML files in <Install directory>\conf)	
Integrationservice.xml	Recorder Manager > General Setup > Integration Framework > Save
SecurityConfig.xml	Enterprise Manager > System Management > Enterprise > Security > Save
Data cache files (all XML files in <Install directory>\conf\cache)	
Cache-Manifest.xml	Enterprise Manager > Any change that will trigger a data cache update > Save
datasource-<data source identifier>.xml	Enterprise Manager > Recording Management > Data Sources > Save
servers.xml	Enterprise Manager > System Management > Enterprise > Settings > Save
organization--<organization id>.xml	Enterprise Manager > User Management > Employees > Profiles > Save
attributes.xml	Enterprise Manager > System Management > Data Sources > Save
businessrules.xml	Enterprise Manager > Recording Management > Recording Rules > Settings > Save
RM configuration files (all XML files in <Install directory>\TomCat\config)	
ConfigManager.xml	Enterprise Manager > System Management > General Settings > Enterprise Manager Location > Save

You must correct the following configuration using the ChecksumUtil command line utility, as described in [Correct Tampering from a Command Line \(page 544\)](#), as they cannot be corrected in Recorder Manager or Enterprise Manager:

- MaintainerConfig.xml
- wsconfig.xml
- RecorderComponentsConfiguration.xml
- ComponentManagementConfig.xml
- IPCaptureProtocolConfig.xml
- MasterConfig.xml
- KMCLocalProviderConfig.xml
- KMCRSAProviderConfig.xml
- RecorderController.xml
- AdapterData.xml
- LogServerManager.xml
- ListConfigManager.xml
- adapter.xml

Correct Tampering from a Command Line

The following procedure outlines how to use a command line to correct tampering (see [Correct Tampering \(page 542\)](#) for more information).

1. Open a DOS window, and navigate to the folder containing the Checksum utility (typically **%IMPACT360SOFTWAREDIR%\ContactStore\Tools**).
2. Make sure that **Console Enabled** is selected in the Log Manager utility (accessed when you type **logmanager.exe** at the command prompt. If Console Enabled is not selected, the checksumutil.exe utility will not display anything.)
3. Type **checksumutil.exe** followed by one or more of the following parameters:

Parameter	Description
-gall	Create the checksum for all files.
-g <FileName>	Create the checksum for the specified file.
-gd <DirName>	Create the checksums for all the files in the specified directory.
-vall	Validate the checksum for all files.
-v <FileName>	Validate the checksum for the specified file.
-vd <DirName>	Validate the checksums for all the files in the specified directory.

For example, to correct the checksum string in the file AlarmConfig.xml, you would type the following in the DOS window:

```
checksumutil -g <AlarmConfig.xml>
```

If XML file is in a different directory you need to give complete path details, such as

```
checksumutil -g<path to XML file ... /AlarmConfig.xml>
```

The checksum digit in the specified configuration file(s) is corrected.



The ChecksumUtil utility corrects only .xml files. To see a list of all parameters, enter **ChecksumUtil**.

Network Interface Card (NIC) name displays symbols

On an IP Recorder, when you navigate to **General Setup > Capture Settings > Cards and Filters** the network interface card name displays symbols. For example, the card name is all question marks.

By default, NIC card names use the language of the installed operating system. However, a card name with non-Latin characters, such as Chinese or Korean, is not supported.

Solution

Change the card name to use the Latin alphabet.

Related topics

[Configure network cards and filters \(page 243\)](#)

Hardware issues

Tasks that can help you identify and resolve issues with hardware components are provided.

Related topics

[Voice cards \(page 545\)](#)

[Wiring \(page 547\)](#)

[Channel assignment \(page 548\)](#)

Voice cards

Use the following procedure to check each voice card to make sure that it has been recognized by the recorder and is properly installed and initialized. See also: [Voice Card Issues \(page 546\)](#).



To have the voice cards and drivers recognized properly, make sure that the "Secure Boot" BIOS option is disabled.

Procedure

1. In Recorder Manager, click **Alarms** to see if any 'voice card added/removed' alarm(s) have been triggered.
2. Choose **General Setup > Voice Cards > Card**. The pane on the left displays the serial number for all cards that have been recognized by the recorder.
3. Select the card that needs to be identified and then click **Identify**.
4. Do one of the following:
 - Look for a flashing LED light on the card inside the chassis. If the card is properly installed and initialized, the LED on the card will flash.



It might be necessary to remove the chassis cover to view the LED.

- Launch the appropriate software tool (that accompanies the voice card) to check the card. If the card(s) of interest is not visible on the Voice Cards Tab, then it is possible that the Recorder did not recognize the card.

Voice Card Issues

Issue	Solution
New settings do not take effect, even after saving.	Reboot computer, as not all voice cards update configurations dynamically.
The voice card supports dynamic configuration but new settings are not taking effect immediately.	Make sure the Capture engine is up and running (go to Operations > Start and Stop).
The recorder is not detecting all of the Smartworks series of cards installed in the system.	Run the SmartView utility and re-initialize all voice cards. You can also uninstall all voice cards from the Windows device manager, then reboot the system. The cards will then be recognized and Windows will load the drivers. When the drivers are loaded normally during installation, the firmware is automatically updated on the cards. If the cards are not detected, the firmware on the cards will not be automatically updated during the recorder software installation. In this case you should run the utility, "SmartWF.exe /u" after taking corrective action to update the firmware on the cards.
After replacing a voice card, the new card is duplicated and both cards have Newly Added statuses.	To resolve this issue: <ol style="list-style-type: none">1. Delete all cards with a Removed status.2. Go to Operations > Start/Stop and restart the Recorder TDM CaptureEngine.

Related topics

[Delete a voice card \(page 233\)](#)

Wiring

Wiring changes for Trunk and Extension tapping are necessary when there are any hardware changes such as adding, removing and replacing voice cards in the recorder. Wiring changes include replacing input cables and wires into the card from telephone tapping sources.

In each of the following scenarios you can use the SmartView Tool to detect whether there are any **Framer Errors** on the card. **Framer Errors** occur when time synchronization is lost between the local clock and the start of a frame signal. In addition to any loss of signal, the recorder's Capture components raise a loss of signal alarm.

Suggested cable lengths for T1 and E1 DP cards are 15 meters (52 feet) and 30 meters (98 feet) respectively, from the tap to the card. For wiring diagrams refer to the Smartworks/Audiocodes documentation.



All voice cards should also be visible in the device manager, under Windows.

To add a new voice card

1. Restart the Capture Component and let it detect the newly added card.
2. In Recorder Manager select **General Setup > Voice Cards** and configure the card as described in [TDM recording setup \(page 198\)](#).
3. Make sure the Card has been initialized properly and identify the card with in the host as described in [Voice cards \(page 545\)](#).
4. Plug in the wiring/cables into the voice card you just added. Refer to the appropriate card documentation to ensure that a crossover cable is not required.
5. Add the associated extensions as described in [TDM recording setup \(page 198\)](#).

To replace an existing voice card

1. Restart the Capture Component and let it detect the replaced card.
2. In Recorder Manager select **General Setup > Voice Cards** and configure the card as described in [TDM recording setup \(page 198\)](#).
3. Make sure the card has been initialized properly and identify the card with in the host as described in [Voice cards \(page 545\)](#).
4. Copy the configuration from the removed card onto the replaced card.
5. Delete the removed card.
6. Plug in the wiring/cables into the voice card that was replaced.

To remove an existing voice card

1. Restart the Capture Component and let it detect the removed card.
2. In Recorder Manager select **General Setup > Voice Cards** and configure the card as described in [TDM recording setup \(page 198\)](#).
3. Delete the configuration of the removed card from the capture configuration as described in [Delete a voice card \(page 233\)](#).
4. Copy the configuration from the removed card onto the replaced card.

To move an existing voice card

1. Restart the Capture Component and let it detect the moved card.
2. In Recorder Manager select **General Setup > Voice Cards** and configure the card as described in [TDM recording setup \(page 198\)](#).
3. Make sure the card has been initialized properly and identify the card with in the host as described in [Voice cards \(page 545\)](#).
4. Copy the configuration from the **Removed** instance of this card onto the **Newly Added** instance of this card.
5. Plug in the wiring/cables into the voice card that was moved.
6. Delete the removed card.

Channel assignment

The following are some frequently asked questions related to channel assignment.

What does the Channel ID Column represent?

The Channel ID column represents the media channel number. The media channel is identified in the recording request from the Command Control Engine, and is globally unique to a Recorder.

What is the Channel Number?

The Channel Number represents the channel number index on a particular card and is unique to each card. This number is not used externally to the recorder.

When are Channel IDs assigned?

Channel IDs are assigned to a card when the card is first saved, at which time the channel IDs are locked to that serial number and will not change unless the number of channels changes.

How are Channel IDs assigned?

Channel IDs are assigned sequentially based on the number of channels that will be active on the card when it is first saved. For example if the trunks on the card are configured for Robbed Bit or the protocol is set to none it will show 24 channels per trunk. If the card is configured for ISDN it will be 23 channels per trunk. For E1 trunks it will be 30 channels per trunk. If this configuration is later changed, the channel IDs for the configured card will be added or removed to reflect the new number of channels.

How are channels added when protocols are changed?

If channel IDs are to be added, for example in changing an existing card from ISDN to Robbed Bit (going from 23 to 24 channels) and there is no room in the channel IDs for the recorder to insert a new channel number, then the existing channel IDs for the changed card will be moved to the end of the channel IDs for the recorder. See [Example 3: After initial save, modify Card Set 1 from Robbed Bit to ISDN \(page 549\)](#).

How do you configure channel IDs from Recorder Manager?

If the channel IDs are not configured as desired because of a protocol or configuration change, you can delete the cards from the Recorder Manager. You must then restart the recorder and add the

cards again, after they are auto-detected, to save the channel IDs in the correct order and configuration.

How is channel numbering started for new cards?

Any new cards added to a system start their channel ID numbering from the highest channel number in the system plus one.

How are channel IDs renumbered?

Channel IDs are renumbered or moved across a whole card at a time. For dual trunk cards the channels are renumbered across both trunks even if the protocol on one of the trunks has changed.

What if there is no room on the channel ID listing for additional channels?

The same rules apply to changing the configuration of a card from E1 to T1 or T1 to E1; if channels are added and there is no room in the channel ID listing, the card will be renumbered to the end of the channel ID listing. If channels are removed then there will be allowable holes in the channel ID list.

How can you check channel IDs?

You can view channel IDs through the Recorder Manager Voice Card configuration screen.

Example 1: Card Set 1 - Initial save

Card #1-DP3209-Robbed Bit - Channel IDs 1-24

Card #2-DP3209-Robbed Bit - Channel IDs 25-48

Card #3-DP3209-Robbed Bit - Channel IDs 49-72

Example 2: Card Set 2 - Initial save

Card #1-DP3209-ISDN - Channel IDs 1-23 (24 is reserved)

Card #2-DP3209-ISDN - Channel IDs 25-47 (48 is reserved)

Card #3-DP3209-ISDN - Channel IDs 49-71 (72 is reserved)

Example 3: After initial save, modify Card Set 1 from Robbed Bit to ISDN

Card #1-DP3209-ISDN - Channel IDs 1-23

Card #2-DP3209-ISDN - Channel IDs 25-47

Card #3-DP3209-ISDN - Channel IDs 49-71

In this example, the last channel IDs for each D-channel were removed, and the channel IDs assigned to the existing channels did not change. There are now gaps in the logical channel ID listing (numbers 24 and 48) but this will not cause any issues. The system should be updated so that it does not attempt recording on channels 24 and 48 because they no longer exist from the recorder's perspective. If a record command comes in for these channel numbers, the recorder will return an error message stating that there is no channel by that number.

Example 4: After initial save, Card #1 from Card Set 2 is changed from ISDN to Robbed Bit

Card #1-DP3209-Robbed Bit - Channel IDs 1-24

Card #2-DP3209-ISDN - Channel IDs 25-47

Card #3-DP3209-ISDN - Channel IDs 49-71

Channel ID 24 is reused when the protocol is changed to Robbed Bit. The Command Control Engine mapping table should be updated to add channel 24.

Example 5: Starting with the result of Example 1, the configuration of Card #1 is changed to E1 Robbed Bit

Card #1-DP3209- E1 Robbed Bit - Channel IDs 73-102

Card #2-DP3209- T1 Robbed Bit - Channel IDs 25-48

Card #3-DP3209- T1 Robbed Bit - Channel IDs 49-72

Example 6: Starting with the result at the end of Example 5, a new card is added and configured for T1 Robbed Bit

After saving the card the channel IDs will result in the following:

Card #1-DP3209- E1 Robbed Bit - Channel IDs 73-102

Card #2-DP3209- T1 Robbed Bit - Channel IDs 25-48

Card #3-DP3209- T1 Robbed Bit - Channel IDs 49-72

Card #4-DP3209- T1 Robbed Bit - Channel IDs 103 - 126

As you can see, the newly added card is added to the end of the channel ID list starting with the highest existing channel ID on the system plus 1 ($102+1=103$). Since it is initially saved as Robbed Bit, it is saved with 24 channel IDs.

Configuration reports

Configuration Reports allow you to view information about specific aspects of your setup, including installation, rules, data sources and member groups.

Procedure

1. To view configuration reports, click **Recording Management > Data Sources > Settings** or **Recording Management > Recording Rules > Settings**.
2. Click the **Reports** button on the bottom right of the screen.
3. On the Select a Configuration Report menu, click any button to view the associated report.



Log Manager utility

The Log Manager utility provides a way to configure properties of common logging for certain Recorder components, including Integration Service, IP Capture, TDM Recorder, Screen Capture, and Recorder. Properties that can be configured include retention period for the logs, log level, and directory location of the logs. Typically this utility is used to change the log retention period and logging levels.

Within Log Manager you can also add components and edit the registry.



The Log Manager utility cannot be used to configure Recorder Manager and Enterprise Manager log files. Each of these applications contain Log Viewer and Log Manager sections through which you can monitor logs.

To provide technical support personnel with key information and to reduce time-to-resolution of issues, the default debug levels of key Recorder components have been changed as follows:

- IP Capture: From Info to Debug
- TDM Capture: From Info to Debug
- Recorder Integration Service: From Info To Debug High



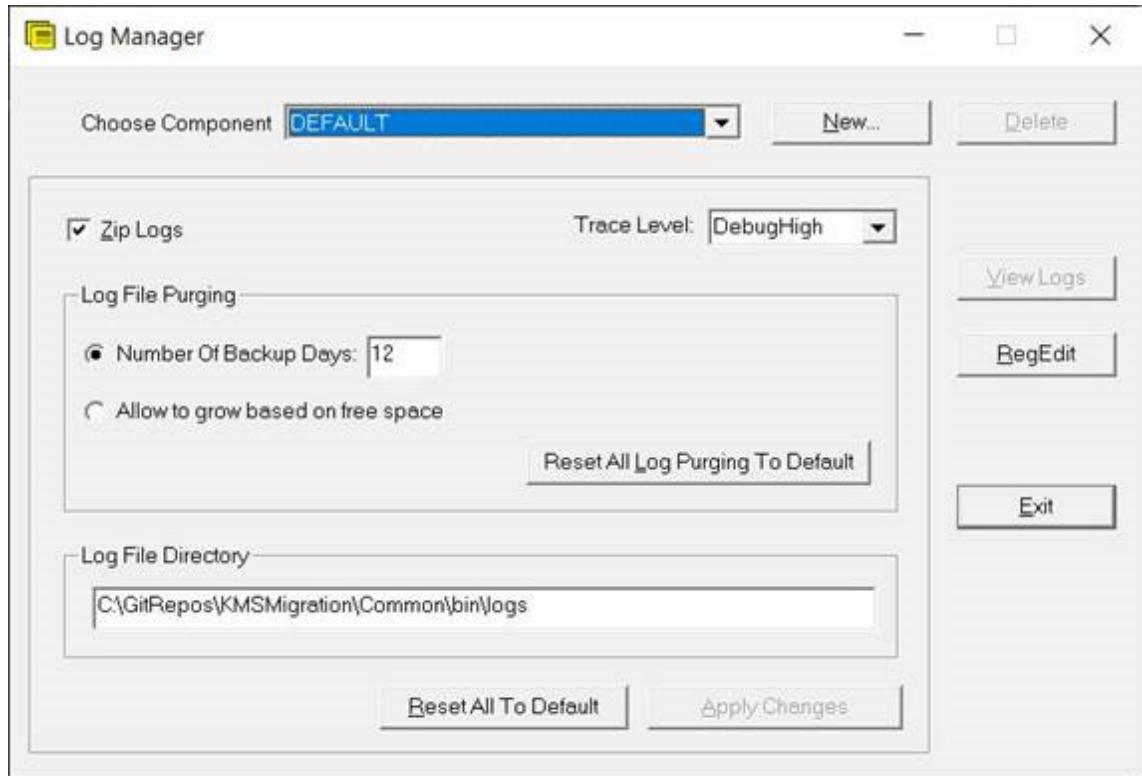
These debug levels can require additional disk space.

Related topics

[Use Log Manager \(page 552\)](#)

Use Log Manager

1. Go to %IMPACT360SOFTWAREDIR%\ContactStore.
2. Run **LogManager.exe** as Administrator.



3. Set the properties as required.
4. To close the Log Manager, select **Exit**.

Log Manager properties

Property or Button	Description
Choose Component	List of available components.
New	Adds a new component to the Log Manager.
Zip logs	Compresses log files.
Trace Level	Determines the level of information included in the log file.
Number of Backup Days	It is recommended that you not change the default value.

Property or Button	Description
Allow Grow based on free space	<p>Allows component logs to grow based on the free space on the log drive. If this option is not enabled, logs are purged after 14 days, which can remove historical log files that can be needed for troubleshooting.</p> <p>When the WDLS allow grow feature is enabled, by default it maintains a minimum free disk space of:</p> <ul style="list-style-type: none"> • 1. 1 GB on non-consolidated boxes • 2. 10 GB for consolidated boxes <p>If the call buffer is on the same partition as the logs, the minimum free space is the disk threshold + 1GB to make sure the call buffer does not overwrite logs.</p> <p>These default free disk space thresholds are typically sufficient.</p> <p>However, if your disk is filling up faster than expected, use the following registry settings to override the free disk space thresholds:</p> <ul style="list-style-type: none"> • DWORD FreeSpaceMBConsolidated - Free 'Allow Grow' space maintained by DiskManager for Consolidated installation. • DWORD FreeSpaceMBNonConsolidated - Free 'Allow Grow' space maintained by DiskManager for Non Consolidated installation. <p>WDLS reads its Windows registry settings based on the x64/x32 installed version. On a x64 version of windows this is usually located in the windows registry under: HKLM\Wow6432Node\Witness\Tracing\<ComponentName></p>
Reset All Log Purging To Default	<p>Removes LogPurgeOption and NumBackupDays from the component configuration.</p> <ul style="list-style-type: none"> • If the DEFAULT target is selected, these options are removed from ALL components. • If a specific target is selected, these options are removed for the selected component only.
Log File Directory	The path to the selected component log file.
View Logs	Enables you to open a specific log file for the selected component. A component can have more than one log file.
RegEdit	Enables you to view or set the registry settings for the component log file.
Reset All To Default	<p>Removes ALL component configuration options, leaving only the target subkey.</p> <ul style="list-style-type: none"> • If the DEFAULT target is selected, options are removed from ALL components. • If a specific target is selected, then options are removed for the selected component only.
Apply Changes	Saves the configuration. Select this button before selecting another component. It takes about one minute to apply the changes.

Related topics

[Log Manager utility \(page 552\)](#)

Import formats for data sources

Use the Data Source Import utility to efficiently create, update, or delete data source configurations—especially when managing large numbers of phones, extensions, or workstations. The import utility is ideal for:

- Adding or updating large volumes of phones, extensions, and workstations.
- Managing data sources such as Phone, Application, LAN (Screen), Radio, or Trader.
- Automating data source creation and configuration.

Topics

General guidelines for importing data sources	557
Use the data source import utility	559
Data source import formats	561
Data source group import/export formats	564
Application data source import formats	565
Sample Application data source import formats	571
Phone and Trader data source import formats	573
Switch-specific data source import formats	586
LAN data source import formats	600

General guidelines for importing data sources

A CSV file must follow specific formatting rules to ensure successful import into the system. You can prepare the files using spreadsheet tools like Microsoft Excel. Follow these general guidelines for a successful import.

Export CSV as template

As a best practice, create the data source in the system, export it, and use the exported CSV as your template. Make your changes directly in this CSV and import it when done.

Use the API

Advanced users are encouraged to use the Data Source Configuration API for managing repetitive or large numbers of data sources updates. For more information, see the **Related Information** section below.

General guidelines

To ensure a successful import, follow these guidelines:

- Follow the required format for each type of data source (Station-side Extension, IP Extension Pool).
- Use parentheses to group multiple items.
- Enclose fields containing commas in double quotation marks (").
- Include the values of required fields, which are marked with an asterisk (*).
- Leave a field empty when it is not applicable for the switch type.
- Leave a field empty when it is optional and you want the default value applied.
- To annotate sections, include lines that start with #, as they are ignored during import.
- Limit the file size to a maximum of 40 MB.

File Structure

Malformed files are rejected. Each file must:

- Be saved in UTF-8 encoded CSV format with a .csv extension.
- Include fields in the order specified in the documentation.
- Contain valid, case-sensitive values for each field, using the exact spelling, capitalization, and formatting shown in the import format tables.

Related topics

[Use the data source import utility \(page 559\)](#)

[Import formats for data sources \(page 556\)](#)

Related information

[Data Source Configuration API overview \(Verint Connect Developer Portal\)](#)

[Data Source Configuration API reference \(Verint Connect Developer Portal\)](#)

Use the data source import utility

Use the data source import utility to create, update, or delete data sources by importing their data. You can import any of the following of Data Sources: Trader, Phone, Application, LAN (Screen), Radio, or Trader. The import utility is useful for managing extensions, which is not done from the Installations pane, but is done through data sources and member groups, where extensions are associated with Recorders.

Related topics

[Import into a data source \(page 559\)](#)

[Schedule a data source import \(page 559\)](#)

[Delete existing data source members while importing \(page 560\)](#)

Import into a data source

Use the following procedure to import data into a data source. If a target data source does not exist, see [Create/Update Phone data source import formats \(page 573\)](#). The maximum file size you can import is 40 MB.

Procedure

1. In Enterprise Manager, click **Recording Management > Data Sources**.
2. Click **Import**.
3. Type a name, and select **Browse** to browse to the file that has the import information.
4. If you need to import the file at a scheduled time, check the **Import Using Specified Date and Time** option. Here, the information is imported according to the date and time in the file.
5. Click **Import**.



If the data source name entry exists in the import file, the file is imported into that data source, and not into the selected data source. For example, if you export a data source, the name of the data source is embedded into the file. The next time you import this file, the file will be imported into the data source that exported this file, and not the currently selected data source.

Schedule a data source import

Schedule data source imports to specify in the import file the exact time and date when an import is to take place. If the CSV file contains schedule information and you select the Schedule option, then the import will be scheduled at the time specified in the file, providing the file is in the correct file format.

File format

The following table lists the fields that you must insert in the CSV file to create a scheduled import. The table includes example values. In the example, the import into the data source starts on **Schedule at 14:45 (2.45 p.m.)** on the 15th of May, 2007. (**2007-15-04**).

Field Number	Field Name	Description	Example
1*	Object Type	Schedule	Schedule
2*	Date	Date of import in the format YYYY-MM-DD	2007-15-04
3*	Time	Time of import in the format HH:MM	14:45

* Required field

Sample Line in .csv file

Schedule, 2007-15-04, 14:45

Delete existing data source members while importing

You can specify in the import file to either delete and re-import, or to simply update the members if they already exist. This is shown in the following table:

CSV File statement	What elements are deleted before import
Property, Reset Datasource, TRUE	For a Phone data source: Phones/Extensions, member groups. For a LAN data source: Workstations, Workstation Groups.
Property, Reset Membergroup, TRUE	For a Phone data source: member groups. For a LAN data source, Workstation Groups.

Data source import formats

To create a data source or update an existing data source, refer to the following list of fields to include in the CSV file you plan to import.

* Required field

** Only required for a Phone switch type

*** Only required for an Application data source

Field #	Field Name	Description	Allowed Values	Examples
1*	Object Type	This indicates that this is an operation on data source settings	Datasource	Datasource
2*	Data Source Name	Name of the data source	General rules for a data source name, such as no special characters.	Cisco Switch
3	Integration Service Associations	Name of the server node that hosts the Recorder Integration Service. This is the name for Installations that use the server role of Recorder Integration Service.	No special characters allowed.	ISServer1
4	Type	Type of data source	Phone, Application, LAN (Screen), Radio, or Trader	Phone
5	Description	Optional description	Text	
6**	Seating Type	Type of seating arrangement (used only for a Phone switch)	Fixed, Free, Hybrid	Free

Field #	Field Name	Description	Allowed Values	Examples
7**	Switch Type	Phone Switch Type	<ul style="list-style-type: none"> • Alcatel 4400 • Aspect • Avaya Definity G3/S8300/S8700 • Cisco IP • Generic Switch • Avaya NES CS1000/Meridian1/Succession • Avaya NES CS2000/CS2100/DMS-100 • Intecom 	Cisco IP
8*	Time zone	Time zone	Text	America/New_York
9	Local Time Tagging Mode	Two options : Organization - Select this option to base the time zone tagging on that of the organization. This setting is useful in scenarios where agents are working in different regions. The setting allows you to unify tagging across multiple time zones. Data Source - Select this option to base time zone tagging on the time zone specified in step 9.	Text	DataSource

Field #	Field Name	Description	Allowed Values	Examples
10***	Associated role	The service or services that this Application data source uses to capture interactions.	InternalServerID_RoleName	"{855001_INTEGRATION_FRAMEWORK,855001_TEXT_INGESTION}"

Example: First line in the CSV for a Phone data source

Datasource, Cisco Switch, ISServer1 ,Phone , , Free, Cisco IP

When imported, this creates (or updates) a data source called **Cisco Switch**, associates it to an integration server named **ISServer1**, of type **Phone** data source, and sets the seating type to **Free** seating and switch type of **Cisco IP**.

Related topics

[General guidelines for importing data sources \(page 557\)](#)

[Application data source import formats \(page 565\)](#)

[Trader data source import formats \(page 584\)](#)

Data source group import/export formats

The following fields provide the details of the import statement needed in a CSV file to import a data source group. Five fields are required in the import.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you want to create or update a data source group	Datasource Group
2*	Group Name	Name of the group to update or create	Sac Group 1
3	Description (Optional)	Description of the member group	Description of skills, such as French, or Spanish.
4*	Type of Data Source Group	The data source group types vary by data source (switch). For example, a Genesys switch supports Trunk Group, Agent Group and Route Points.	Route Points Trunk Group
5*	Average Work Time	This value refers to the average daily or weekly work time of an agent (not used in recording)	11

* Required fields. Other fields are not required.

Sample Line in .csv file:

Datasource Group, Sac Group 1, French, Agent Groups, 11



Automatic Export and Import (and formatting) of data source groups is done by clicking **Export** and **Import** in the data source Settings window. Then a typical .CSV file resembles the above format. Data source group settings always appear at the end of the file.

66 # Following are the Data Source Groups				
67 Datasource Group	Sac Group 1	French	Agent Groups	11
68 Datasource Group	Sac Group 2	Spanish DS Group	Agent Groups	11
69 #End of Export				
70				
71				
72				

Application data source import formats

Follow these guidelines and formats when creating or updating an Application data source using a CSV import. The defined rows, fields, and values configure the data source's settings, properties, member groups, employee mappings, and recording profiles.

Guidelines

- Follow the general guidelines, see the **Related Topics** section at the end of this topic.
- Each row in the CSV must begin with a row type (for example, Datasource, Employee Mapping, etc.). The system interprets and organizes the data based on the specified row type.
- The DataSource row must be first. The remaining rows can be in any order.
- The DataSource name is in the Datasource row and is implicitly associated with all subsequent rows.
- Required fields (indicated by *) must contain a value.
- Values are case sensitive. To get the valid values, export the data source to a CSV.

Settings

Defines the settings for an Application data source.

Field #	Field Name	Description	Allowed Values	Examples
1*	Row Type	Indicates the purpose of this row in the CSV file, which is to define the settings of the data source. Must be the first row in the CSV.	Datasource	Datasource
2*	Data Source Name	Name of the data source. Uniquely identifies the data source.	Follows the same general rules for any data source name, such as it must not include special characters.	myAmazonConnectDS01

Field #	Field Name	Description	Allowed Values	Examples
3	Integration Service Associations	Name of the server node that hosts the Recorder Integration Service. This is the name for Installations that use the server role of Recorder Integration Service.	Text. No special characters allowed.	myServer
4	Type	Type of data source	Application	Application
5	Description	Optional description	Text	Description of my data source
6*	Seating Type	Type of seating arrangement (used only for a Phone switch)	Fixed, Free, Hybrid	Free
7*	Switch Type	The external system this Application data source integrates for recording.	Must match what the Verint platform exports to a CSV file.	Amazon Connect
8*	Time zone	Time zone	Text	America/New_York
9	Local Time Tagging Mode	What provides the time zone.	Only two options: Organization, Data Source	DataSource
10*	Associated role	The service or services that this Application data source uses to capture interactions. Includes the internal ID number of the host server and the name of the server role.	{InternalServerID_RoleName}	"{855001_INTEGRATION_FRAMEWORK,855001_TEXT_INGESTION}"

Example: First line in the CSV for the settings of an Application data source

```
Datasource,myAmazonConnectDS01,myServer,Application,Description of my data source,Free,Amazon Connect,America/New_York,DataSource,"{855001_INTEGRATION_FRAMEWORK,855001_TEXT_INGESTION}",
```

Properties

Defines the settings that are specific for this switch type.

Field #	Field Name	Description	Allowed Values	Examples
1*	SwitchType DS Property	Indicates the purpose of this row in the CSV file, which is to define one of the properties for this data source.	It must start with the Switch Type and then "DS Property".	Amazon Connect DS Property
2	PropertyName	Each line of the CSV is for a different property.	Depends on the data source type. Each type of integration has specific properties.	AWSRegion
3-8	Value	For each property, there can be up to eight values.	Text and numbers depending on the property.	us-east-1

Example: Properties

Amazon Connect DS Property,MINIMUM_SESSION_LENGTH,1,,,,,,

Amazon Connect DS Property,AWSRegion,us-east-1,,,,,,

Member Groups

Define the member groups for this specific switch type. The different types of member groups have a different number of fields.

Field #	Field Name	Description	Allowed Values	Examples
1*	Row type	Indicates the purpose of this row in the CSV file is to define a member group for this data source.	Each row specifies a member group, and must start with SwitchType Group .	Amazon Connect Group
2*	Group Name	The name of the member group.	Text and numbers.	AmzGroup01
3	Description	Optional. Describes the member group.	Text and numbers.	Description of this member group.
4	Recorder control type	A property for this member group.	Refer to the documentation for this type of switch.	Duplicate Streamed
5	Recorder Load Balancing Type	A property for this member group.	Refer to the documentation for this type of switch.	NONE

Field #	Field Name	Description	Allowed Values	Examples
6	Recorder Fallback Type	A property for this member group.	Refer to the documentation for this type of switch.	Never
7	Associated role	The service or services that this Application data source uses to capture interactions. Includes the internal ID number of the host server and the name of the server role.	"{InternalServerID_RoleName}"	"{855001_IP_RECORDER,855001_RECORDER_ADAPTER_PROXY_SERVICE}"

Example: A member group

```
Amazon Connect Group,AmzGroup01,"Description of this member group.",Duplicate Streamed,NONE,Never,"{855001_RECORDER_ADAPTER_PROXY_SERVICE,855001_IP_RECORDER}",
```

Employee Mapping

Define the employees mapped to this Application data source.

Field #	Field Name	Description	Allowed Values	Examples
1*	Row type	Indicates the purpose of this row in the CSV file is to define a member group for this data source.	It must be "Employee Mapping"	Amazon Connect Group
2*	Internal ID	The internal ID that uniquely identifies this employee in the system.	Number	147
3*	Employee ID	The employee ID for this employee that creates a link between the employee and the data source.	Text or number	123

Example: Employee mapping

```
Employee Mapping,147,123
```

Recording profile

Define recording profiles for this Application data source.

Field #	Field Name	Description	Allowed Values	Examples
1*	Row type	The purpose of this row in the CSV file is to define a member group for this data source.	It must be "Recording Profile".	Recording Profile
2*	Name	The name of the profile.	Any text.	ProfileName
3	Description	Optional. Description of the profile.	Any text.	ProfileDescription
4	Associated organization ID	The organizations that this profile records.	The internal ID of organizations within {}, and separated by commas.	{-3002}
5	Associated Employee ID	The internal IDs of the employees that this profile is set to record.	Put IDs within "{}", and separate them by commas.	"{243,244,245}"
6	Record audio	The value set for this option. Refer to the related <i>Integration Guide</i> for details. If the option is not available for this switch type, leave the field empty.	Record, DoNotRecord, ApplicationControlled, StartOnTrigger	DoNotRecord
7	Record video		RecordAlways, DoNotRecord	
8	Record screen share		RecordAlways, DoNotRecord	
9	Record chat		RecordAlways, DoNotRecord	RecordAlways
10	Record email		RecordAlways, DoNotRecord	
11	Record social media		RecordAlways, DoNotRecord	
12	Record direct messaging		RecordAlways, DoNotRecord	

Example: Recording profile

```
Recording Profile,ProfileName,ProfileDescription,{-3002},"  
{243,244,245}",DoNotRecord,,,RecordAlways,,
```

Related topics

[General guidelines for importing data sources \(page 557\)](#)

[Sample Application data source import formats \(page 571\)](#)

[Use the data source import utility \(page 559\)](#)

Related information

Creating Application data sources (WFO Online help)

Refer to the specific Integration with Recorder Guide for your data source, visit [Verint Connect](#).

Sample Application data source import formats

Refer to this sample for an Amazon Connect Application data source to help you review your own CSV. Lines preceded by # are ignored by the import utility.

Following are the DataSource Settings and the properties specific for Amazon Connect switch types.

Datasource,myAmazonConnect,,Application,"Description of my data source.",Free,Amazon Connect,America/New_York,DataSource,

Amazon Connect DS Property,MINIMUM_SESSION_LENGTH,0

Amazon Connect DS Property,LongHoldDuration,30

Amazon Connect DS Property,REQUIRE_REPLAY_AUDIO_REDACTION,DISABLED

Amazon Connect DS Property,AWSEnablePauseResume,false

Amazon Connect DS Property,AWSRegion,us-east-1

Amazon Connect DS Property,AWSContactTraceRecordsStreamName,ctrtest

Amazon Connect DS Property,AWSAccessKeySecret,198C8BDB39FF4C42B88F09ADBE7ACD05

Amazon Connect DS Property,AWSEnableIAMRole,false

Amazon Connect DS Property,Proxy,false

Amazon Connect DS Property,REQUIRE_REPLAY_AUDIO_MORPHING_CHANNEL,DISABLED

Amazon Connect DS Property,REQUIRE_REPLAY_AUDIO_MORPHING,DISABLED

Amazon Connect DS Property,TEXT_LANGUAGE,en-us

Amazon Connect DS Property,LongCallDuration,120

Amazon Connect DS Property,TIMEZONE,America/New_York

Amazon Connect DS Property,SEATING_TYPE,Free

Amazon Connect DS Property,USEACTUALSTAFFING,false

Amazon Connect DS Property,AWSEnableAppCredentials,true

Amazon Connect DS Property,AWSAgentEventsStreamName,aestest

Amazon Connect DS Property,AWSAccessKeyId,JustATest

Amazon Connect DS Property,AuditingPolicy,Disabled

Amazon Connect DS Property,REQUIRE_REPLAY_AUDIO_REDACTION_ENUM,0

Amazon Connect DS Property,REQUIRE_REPLAY_AUDIO_MORPHING_ENUM,0

Following are the Member groups in the Datasource

Amazon Connect Group,Amz Member group test jlong,"description of my mg for amz.",Duplicate Streamed,NONE,Never,"{855001_RECORDER_ADAPTER_PROXY_SERVICE,855001_IP_RECORDER}",

Following are the Employee Mappings in the Datasource

Employee Mapping,147,123

Employee Mapping,149,345

Employee Mapping,201,456

Following are the Recording Profiles in the Datasource

Recording Profile,AmzRecProfile01,description of my rec profile for amz."{-
3002,101,102,1,51,52,167,168,161,162,163,151,164,165,166,152,153,154,169,170,155,156,157,158,159
,160,53,56,58,59,57,60,54,61,63,64,62,65,66,55,67,69,68,70,71}"",RecordAlways,,,RecordAlways,,,

End of File

Phone and Trader data source import formats

Refer to the Phone data source format for creating and updating IP and Station-side data sources. Use the Trader import formats for creating and updating PCM32 trunks spans into a Trader data source.

In all cases, an import example is provided. Required fields are shown with an asterisk (*) and must be specified in the import statement. Non-required fields may be omitted. The maximum file size you can import is 40 MB.

Trader

The following section relates to Trader data sources:

- [Trader data source import formats \(page 584\)](#)

Phone

The following sections describe the various types of phone switch data imports, including .csv file import examples of each, as described in the following topics:

- [Create/Update Phone data source import formats \(page 573\)](#)
- [Create/update IP Extension Pool member group \(page 576\)](#)
- [Create/update IP Extension Pool phones/extensions \(page 577\)](#)
- [Create/update Station-side Extension member group \(page 578\)](#)
- [Create/update Station-side extensions \(page 579\)](#)
- [Create/update Extension Trunk Span \(page 580\)](#)
- [Create/update Extension Trunk Span members \(page 581\)](#)
- [Create/update Trunk Group Trunk Span \(page 582\)](#)
- [Create/update Trunk Group Trunk Span members \(page 583\)](#)
- [Create/update Multiple Registration Extension Pool group members \(page 584\)](#)

Related topics

[General guidelines for importing data sources \(page 557\)](#)

[Switch-specific data source import formats \(page 586\)](#)

[LAN data source import formats \(page 600\)](#)

[Application data source import formats \(page 565\)](#)

[Data source group import/export formats \(page 564\)](#)

Create/Update Phone data source import formats

The following fields must be in a CSV file and imported to create a data source or update an existing data source.

* Required field

**** Only required for a Phone switch type**

***** Only required for an Application data source**

Field #	Field Name	Description	Allowed Values	Examples
1*	Object Type	This indicates that this is an operation on data source settings	Datasource	Datasource
2*	Data Source Name	Name of the data source	General rules for a data source name, such as no special characters.	Cisco Switch
3	Integration Service Associations	Name of the server node that hosts the Recorder Integration Service. This is the name for Installations that use the server role of Recorder Integration Service.	No special characters allowed.	ISServer1
4	Type	Type of data source	Phone, Application, LAN (Screen), Radio, or Trader	Phone
5	Description	Optional description	Text	
6**	Seating Type	Type of seating arrangement (used only for a Phone switch)	Fixed, Free, Hybrid	Free

Field #	Field Name	Description	Allowed Values	Examples
7**	Switch Type	Phone Switch Type	<ul style="list-style-type: none"> Alcatel 4400 Aspect Avaya Definity G3/S8300/S8700 Cisco IP Generic Switch Avaya NES CS1000/Meridian1/Succession Avaya NES CS2000/CS2100/DMS-100 Intecom 	Cisco IP
8*	Time zone	Time zone	Text	America/New_York
9	Local Time Tagging Mode	Two options : Organization - Select this option to base the time zone tagging on that of the organization. This setting is useful in scenarios where agents are working in different regions. The setting allows you to unify tagging across multiple time zones. Data Source - Select this option to base time zone tagging on the time zone specified in step 9.	Text	DataSource
10***	Associated role	The service or services that this Application data source uses to capture interactions.	InternalServerID_RoleName	"{855001_INTEGRATION_FRAMEWORK,855001_TEXT_INGESTION}"

Example: First line in the CSV for a Phone data source

Datasource, Cisco Switch, ISServer1 ,Phone , , Free, Cisco IP

When imported, this creates (or updates) a data source called **Cisco Switch**, associates it to an integration server named **ISServer1**, of type **Phone** data source, and sets the seating type to **Free** seating and switch type of **Cisco IP**.

Create/update IP Extension Pool member group

A line in the CSV file which contains the fields in the following order and format should be present in the file being imported.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you want to create or update an IP Extension Pool	IP ExtensionPool
2*	Group Name	Name of the group to update or create	IP Agent Pool1
3	Description	Description of the member group.	This has all the employee extensions in ATL
4	Recorder Control Type	Recording Control Type to use for the member group.	"Recorder Controlled"
5	Site	Associates the member group to the site names specified here. You can specify one or more sites. The recorders in the site will be associated to the member group.	My Site or {My Site1, My Site2}
6.	Recorder Serial Numbers	Associates the member group to the specified Recorders in this field. One or more Recorder serial numbers can be specified. However, if the Recorder is clustered, the site has to be used instead. A Recorder belonging to a clustered site cannot be used here.	Use the format "62393" for single serial numbers, or "{62393, 65353, 63732}" for multiple serial numbers.
* Required fields. Other fields are not required.			
Sample Line in .csv file:			
IP ExtensionPool, IP Agent Pool1, This has all the agents extensions in ATL, Recorder Controlled, "{My Site1, My Site2}", "{ 62393, 65353, 63732}"			

The example above creates an IP Extension Pool with name **IP Agent Pool1** with recording control type set to **Recorder Controlled** and associates this member group to **My Site1** and **My Site2** and Recorders with the serial numbers **62393**, **65353** and **63732**.

Create/update IP Extension Pool phones/extensions

The import feature allows you to import phones and extensions, and then associate the phones to an IP Extension Pool. These import lines can appear anywhere in the CSV file, except that if there is any association to member groups needed, the member group definition should appear before this definition. Any number of phones-related .csv lines can exist in the import file. A maximum of 5000 extensions can be created or updated in one import.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you want to create an IP Extension and associate it to an IP Extension Pool if needed.	Extension
2*	Primary Extension	Name of the extension.	1000
3	Recording Mode	Recording mode of the extension	Record
4	Member Group Name	IP Extension Pool member group name	"My Agent Pool1"
5	Secondary Extensions and its recording mode.	List of secondary extensions associated to this primary. Each secondary extension and associated mode will be enclosed within parenthesis separated by comma. If there are multiple secondary extensions, recording mode pairs, the whole field must be enclosed in another parenthesis.	<ul style="list-style-type: none"> • "{1001, Do Not Record}" • "{{1001, Do Not Record}, {1002, Application Controlled}}"
* Required fields. Other fields are not required.			
Sample Line in .csv file: Extension, 1000, Record, "My Agents Pool1", "{1001, Do Not Record}"			

The above example creates or updates a Phone named **IP Extension** with primary extension **1000** with record mode set to **Record** in the member group **My Agents Pool1**, in which a secondary extension of **1001** with recording mode set to **Do Not Record** is also created or updated.

Create/update Station-side Extension member group

The import allows you to create a Station-side member group, and then associate it to one or more TDM Recorders. The following table describes how to update or create extensions in the member group.

A line in the **.csv** file being imported should contain the following fields to create or update the Station-side extension member group.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you want to create or update a Station-side Extension Group	Stationside Group
2*	Group Name	Name of the group to update or create	Extension Group1
3	Description	Description of the member group.	Extensions of cubes 1-20 on 4th floor
4*	Number of Ports	Number of Ports	8
5	Recorder Control Type	Recorder Control Type	Recorder Controlled
6	Recorder Serial Numbers	Associates the member group to the specified recorders in this field. One or more recorder serial numbers can be specified.	Use the format "62393" for single serial numbers, or "{62393, 65353, 63732}" for multiple serial numbers.
7	Enable Fallback	Allows Fallback mode to be enabled or disabled (when value is False)	True (Default is False)
* Required fields. Other fields are not required.			
Sample Line in .csv file: Stationside Group, Extension Group1, Extensions of cubes 1-20 on 4th floor, 8, Recorder Controlled, "{ 62393, 65353, 63732}"			

The above example creates/updates a Station-side Extension Group named **Stationside Group** in the **Extension Group1** group, (a group within a group) consisting of **Extensions of cubes 1-20 on 4th floor** (extensions in cubicles 1 through 20 on the building's 4th floor) with **8** ports that are **Recorder Controlled** with Recorder serial numbers **62393, 65353, and 63732**.

Create/update Station-side extensions

Create or update station-side extensions to assign the Phones to a Station-side Extension group.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you want to create or update a Phone/Extension and assign it to a Station-side group	Extension
2*	Primary Extension	Primary extension	1000
3	Recording Mode	Specifies the recording mode of the Extension	Record
4	Member Group Name	Station-side Extension member group name	Extension Group1
5.	Secondary Extensions	List of secondary extensions associated to this primary extension. Each secondary extension and associated mode will be enclosed within parenthesis separated by a comma. If there are multiple secondary extensions, recording mode pairs, the whole field will be enclosed in another parenthesis.	"{{1001, Do Not Record}, {1002, Application Controlled}}"
6**	Port Number	The port number in the group this primary extension has to be assigned to.	1
* Required fields. Other fields are not required. ** If Member Group Name is specified, this field is required.			
Sample Line in .csv file: Extension, 1000, Record, Extension Group1, "{1001, Do Not Record}", 1			

The above example assigns a phone/extension named **Extension** with an ID of **1000** using **Record** as the Recording Mode to member group **Extension Group1**, using port **1** and specifying not to record extension 1001 in the statement **1001, Do Not Record**.

Create/update Extension Trunk Span

You can create/update an Extension Trunk Span and import the Trunk members of the Extension Trunk Span. The following fields provide the details of the import statement needed in a CSV file to import an Extension Trunk Span.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates to create or update a Aspect Trunk Span	Extension TrunkSpan
2*	Group Name	Name of the group to update or create	Group1
3	Description	Description of the member group	Trunk span cubes 1-24 on 4th floor
4*	Number of Ports	Number of Ports	24
5	Associated Dialer Data Source	The name of the Dialer data source, if any, associated with the trunk span	Sacramento
6	Recorder Control Type	Recorder Control Type	"Recorder Controlled"
7	Recorder Serial Numbers	Associates the member group to the specified recorders in this field. One or more recorder serial numbers can be specified.	Use the format "62393" for single serial numbers, or "{62393, 65353, 63732}" for multiple serial numbers.
8	Enable Fallback	Allows Fallback mode to be enabled or disabled (when value is False)	True (Default is False)

* Required fields. Other fields are not required.

Sample Line in .csv file:

```
Extension TrunkSpan, Group1, Trunk span cubes 1-24 on 4th floor,
Sacramento, 24, Recorder Controlled, 62393
```

The above example creates or updates an Extension Trunk Span named **Extension TrunkSpan** in the member group **Group1**, consisting of **Trunk span cubes 1-24 on 4th floor** (that is, extensions in cubicles 1 through 24 on the building's 4th floor) from **24** ports that are **Recorder Controlled** from Recorder serial number **62393**.

Create/update Extension Trunk Span members

You must import the trunk span members along with the Trunk Group. Any member not specified is deleted.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates to create or update a Trunk Span member	Extension
2*	Primary Extension	Primary Extension Number	1000
3	Record Mode	Record Mode of the extension	Record
4	Member Group Name	Trunk Span member group name	Group1
5	Port Number	The port number in the group to which this primary extension must be assigned.	1
6	Secondary Extensions and their recording mode.	List of secondary extensions associated to this primary extension. Each secondary extension and associated mode will be enclosed within parenthesis, separated by comma. If there are multiple secondary extensions, recording mode pairs, the whole field will be enclosed in another parenthesis.	{"1001, Do Not Record}" or "{{1001, Do Not Record}, {1002, Application Controlled}}"

* Required fields. Other fields are not required.

Sample Line in .csv file:

```
Extension, 1000
```

In the above example, a Trunk Span member group named **Extension** with primary extension number **1000** is created or updated. The absence of the remaining fields in the example reflects that they are optional: an * (asterisk) indicates a required field. The example could have been **Extension, 1000, Record, Group1, 1, "{{1001, Do Not Record}, {1002, Record}}"**

Create/update Trunk Group Trunk Span

You can create or update a Trunk Group Trunk Span and then import the Trunk members of the Trunk Span. The following fields provide the details of the import statement needed in a **.csv** file to import a Trunk Group Trunk Span.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you will create or update a Aspect Trunk Span	TrunkGroup TrunkSpan
2*	Group Name	Name of the group to update or create	Group1
3	Description	Description of the member group	Trunk span cubes 1-24 on 4th floor
4*	Number of Ports	Number of Ports	24
5	Associated Dialer Data Source	The name of the Dialer data source, if any, associated with the trunk span	Sacramento
6	Recorder Control Type	Recorder Control Type	"Recorder Controlled"
7	Recorder Serial Numbers	Associates the member group to the specified recorders in this field. One or more recorder serial numbers can be specified.	Use the format "62393" for single serial numbers, or "{62393, 65353, 63732}" for multiple serial numbers.
8	Enable Fallback	Allows Fallback mode to be enabled or disabled (when value is False)	True (Default is False)
* Required fields. Other fields are not required.			
Sample Line in .csv file:			
TrunkGroup TrunkSpan, Group1, Trunk span cubes 1-24 on 4th floor, Sacramento, 24, Recorder Controlled, 62393			

The above example creates or updates Trunk Group Trunk Span named **TrunkGroup TrunkSpan** in the member group **Group1**, consisting of **Trunk span cubes 1-24 on 4th floor** (that is, extensions in cubicles 1 through 24 on the building's 4th floor) from **24** ports that are **Recorder Controlled** from Recorder serial number **62393**.

Create/update Trunk Group Trunk Span members

You must import the trunk span members along with the Trunk Group. Any member not specified is deleted.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates to create or update a Trunk Span member	Trunk Member
2*	Member Group Name	The Trunk Group member group name	Group1
3*	Port Number	The port number in the group this primary extension has to be assigned to.	1
4	Trunk Group	Trunk Group	4
5	Member Name	The trunk member.	60

* Required fields. Other fields are not required.

Sample Line in CSV:

Trunk Member, Group1, 1, 4

The above example creates or updates a Trunk Group Trunk Span member, as indicated by **Trunk Member**, which belongs to member group **Group1** using port number **1** within Trunk Group **4**. The member name does not appear, as this is an optional field.

Create/update Multiple Registration Extension Pool group members

Use the following settings when importing/exporting Multiple Registration Extension Pool member groups.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates to create or update a Multiple Registration Extension Pool.	Multiple Registration ExtensionPool
2*	Group Name	Name of the group to update or create. May not contain special characters.	Multiple Registration Extension Pool 1
3	Description	Description of the member group. May not contain special characters.	
4	Recorder Fall Back Type	Recorder fallback type for the specified Extension pool. Can be Never, OnCTIDisconnection, or Always (the default is OnCTIDisconnection).	OnCTIDisconnection
5	Dedicated Recorder Serial Numbers	<p>These are the serial numbers of the dedicated recorders that must be associated with the parent extension pool member group. Automatic rebalancing will occur for all extensions associated with the parent member group to the sub- member groups created for every dedicated recorder serial number.</p> <p>Serial numbers must match the serial numbers of the installed recorders. These recorders should have IP Recorder Server Role.</p>	Use the format "62393" for single serial numbers, or "{62393, 65353, 63732}" for multiple serial numbers.

* Required fields. Other fields are not required.

Sample Line in CSV:

Multiple Registration ExtensionPool, Multiple Registration Extension Pool 1, This has all the agents extensions in ATL, OnCTIDisconnection, "{326001}"

The above will create a Multiple Registration Extension Pool with the name "Multiple Reg Pool1" and a Recorder Fallback Type of "On CTI Disconnection". It associates the dedicated server with a serial number of 326001 to this pool, and discards all abandoned CTI.

Trader data source import formats

The following formats can be used to import PCM32 trunks spans into a Trader data source.

Field #	Field Name	Description	Examples
1*	Object Type		PCM32 TrunkSpan
2*	Trunk Span Name		Span1
3	Description		Span 1 of the 8 spans in 4th floor
4*	Number of Ports		32
5*	Recording Type	Recording Type	Recorder Controlled. Can also be: <ul style="list-style-type: none">• Full Delivery (External Controlled)• CTI Controlled• Selective Delivery (Duplicate Streamed)
6	Associated Recorder Serial Numbers	The serial numbers of Recorders associated with the Trader data source	Use the format "62393" for single serial numbers, or "{62393, 65353, 63732}" for multiple serial numbers.
7*	Megalink Recorder #	Megalink Recorder number	4
8*	Megalink Port #	Megalink Port port number	6
9	Enable Fallback	Allows Fallback mode to be enabled or disabled (when value is False)	True (Default is False)
* Required fields. Other fields are not required.			
Sample Line in .csv file:			
PCM32 TrunkSpan, Span1,,32, Recorder Controlled, , 4, 6			

The above example creates a PCM32 TrunkSpan named Span1 which has 32 members with Megalink Recorder number of 4 and Megalink Port number of 6. This will generate the members automatically. Description and Recorder serial numbers are optional, so do not show.

Switch-specific data source import formats

You can import data source data for different types of Trunk Spans, such as Alcatel, Aspect, Extension, Generic, Avaya NES, Trunk Group, and Trunk Span. In all cases, the number of members statements should not exceed the Number of ports in the Group.

Related topics

- [Create/update Alcatel Trunk Span \(page 586\)](#)
- [Create/update Alcatel Trunk Span members \(page 588\)](#)
- [Create/update Aspect Trunk Span \(page 588\)](#)
- [Create/update Aspect Trunk Span members \(page 590\)](#)
- [Create/update Generic Trunk Span \(page 590\)](#)
- [Create/update Generic Trunk Span members \(page 592\)](#)
- [Create/update Avaya NES Trunk Span \(page 592\)](#)
- [Create/update Avaya NES Trunk Span members \(page 593\)](#)
- [Switch-specific import working examples \(page 594\)](#)

Create/update Alcatel Trunk Span

You can create/update an Alcatel Trunk Span and import the Trunk members of the Trunk Span. The following fields provides the details of the import statement needed in a `.csv` file to import an Alcatel Trunk Span.

Field #	Field Name	Description	Examples
1*	Object Type	Indicates that you will create or update an Alcatel Trunk Span	Alcatel TrunkSpan
2*	Group Name	Name of the group to update or create	Group1
3	Description	Description of the member group.	Trunk span cubes 1-24 on 4th floor
4*	Number of Ports	Number of Ports	24
5	Associated Dialer Data Source	The name of the Dialer data source, if any, associated with the trunk span	Sacramento
6	Recorder Control Type	Recorder Control Type	"Recorder Controlled"

Field #	Field Name	Description	Examples
7	Recorder Serial Numbers	Associates the member group to the specified recorders in this field. One or more recorder serial numbers can be specified.	Use the format "62393" for single serial numbers, or "{62393, 65353, 63732}" for multiple serial numbers.
8*	Coupler	Coupler Value	1
9*	Crystal	Crystal Value	2
10*	First Time Slot	First Time Slot Value	3
11	Enable Fallback	Allows Fallback mode to be enabled or disabled (when value is False)	True (Default is False)

* Required fields. Other fields are not required.

Sample Line in .csv file:

```
Alcatel TrunkSpan, Group1, Trunk span cubes 1-24 on 4th floor,
Sacramento, 24, Recorder Controlled, 62393, 1, 2,3
```

The above example creates or updates a Trunk Span named **Alcatel Trunk Span** in the member group **Group1**, consisting of **Extensions of cubes 1-24 on 4th floor** (that is, extensions in cubicles 1 through 24 on the building's 4th floor) from **24** ports that are **Recorder Controlled** from Recorder serial number **62393**, with Coupler ID **1**, Crystal ID **2**, and first time slot ID **3**.

Create/update Alcatel Trunk Span members

Alcatel trunk span members must be imported along with the Trunk Group. The following fields provide the details of the import statement needed in a **.csv** file to import an Alcatel Trunk Span member into a member group.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you will create or update an Alcatel Trunk Span member	Trunk Member
2*	Member Group Name	Alcatel Trunk Span member group name	Group1
3*	Port Number	The port number in the group this primary extension has to be assigned to.	1

* Required fields. Other fields are not required.

Sample Line in **.csv** file:

```
Trunk Member, Group1, 1
```

The above example creates an Alcatel Trunk Span member named **Trunk Member** in member group **Group1**, assigned to port 1.

Create/update Aspect Trunk Span

You can create/update an Aspect Trunk Span and import the Trunk members of the Trunk Span. The following provides the details of the import statement needed in a **.csv** file to import an Aspect Trunk Span.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you will create or update an Aspect Trunk Span	Aspect TrunkSpan
2*	Group Name	Name of the group to update or create	Group1
3	Description	Description of the member group.	Trunk span cubes 1-24 on 4th floor
4*	Number of Ports	Number of Ports	24
5	Associated Dialer Data Source	The name of the Dialer data source, if any, associated with the trunk span.	Sacramento

Field #	Field Name	Description	Examples
6	Recorder Control Type	Recorder Control Type	"Recorder Controlled"
7	Recorder Serial Numbers	Associates the member group to the specified recorders in this field. One or more recorder serial numbers can be specified.	Use the format "62393" for single serial numbers, or "{62393, 65353, 63732}" for multiple serial numbers.
8*	Trunk Group	Trunk Group	1
9*	Starting Device Number	Starting Device Number	10
10	Enable Fallback	Allows Fallback mode to be enabled or disabled (when value is False)	True (Default is False)

* Required fields. Other fields are not required.

Sample Line in .csv file:

```
Aspect TrunkSpan, Group1, Trunk span cubes 1-24 on 4th floor,
Sacramento,24, Recorder Controlled, 62393, 1, 10
```

The above example creates or updates an Aspect Trunk Span named **Aspect Trunk Span** in the member group **Group1**, consisting of **Trunk span cubes 1-24 on 4th floor** (that is, extensions in cubicles 1 through 24 on the building's 4th floor) from **24** ports that are **Recorder Controlled** from Recorder serial number **62393**, in Trunk Group **1**, with a starting device number **3**.

Create/update Aspect Trunk Span members

Aspect trunk span members must be imported along with the Aspect Trunk Group. The following fields provide the details of the import statement needed in a **.csv** file to import Aspect Trunk Span members.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you will create or update a Trunk Span member	Trunk Member
2*	Member Group Name	Aspect Trunk Span member group name	Group1
3*	Port Number	The port number in the group this primary extension has to be assigned to.	1
4	Member Name	The member name.	60

* Required fields. Other field is not required.

Sample Line in **.csv** file:

```
Trunk Member, Group1, 1, 60
```

The above example creates or updates an Aspect Trunk Span member named **Trunk Member** in member group **Group1**, assigned to port **1**, with a member name **60**.

Create/update Generic Trunk Span

You can create/update a Generic Trunk Span and import the Trunk members of the Trunk Span. The following fields provides the details of the import statement needed in a CSV file to import a Generic Trunk Span.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you will create or update a Generic Trunk Span	Generic TrunkSpan
2*	Group Name	Name of the group to update or create	Group1
3	Description	Description of the member group.	Trunk span cubes 1-24 on 4th floor
4*	Number of Ports	Number of Ports	24

Field #	Field Name	Description	Examples
5	Associated Dialer Data Source	The name of the Dialer data source, if any, associated with the trunk span	Sacramento
6	Recorder Control Type	Recorder Control Type	"Recorder Controlled"
7	Recorder Serial Numbers	Associates the member group to the specified recorders in this field. One or more recorder serial numbers can be specified.	Use the format "62393" for single serial numbers, or "{62393, 65353, 63732}" for multiple serial numbers.
8	Enable Fallback	Allows Fallback mode to be enabled or disabled (when value is False)	True (Default is False)

* Required fields. Other fields are not required.

Sample Line in .csv file:

```
Generic TrunkSpan, Group1, Trunk span cubes 1-24 on 4th floor,,24,
Recorder Controlled, 62393
```

The above example creates or updates a Generic Trunk Span named **Generic Trunk Span** in the member group **Group1**, consisting of **Trunk span cubes 1-24 on 4th floor** (that is, extensions in cubicles 1 through 24 on the building's 4th floor) from **24** ports that are **Recorder Controlled** from Recorder serial number **62393**.

Create/update Generic Trunk Span members

You must import Trunk span members along with the Trunk Group. Any member not specified is deleted.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you will create or update a Trunk Span member	Trunk Member
2*	Member Group Name	The Trunk Span member group name	Group1
3*	Port Number	The port number of the group to which this primary extension has been assigned	1
4	Hardware Specific	First of the hardware specific columns	TGA
5	Hardware Specific	Second Hardware specific columns	TGB
6*	Trunk Member	The trunk member	60
* Required fields. Other fields are not required.			
Sample Line in .csv file:			
Trunk Member, Group1, 1, TGA, TGB, 60			

The above example creates or updates a Generic Trunk Span member named **Trunk Member** in member group **Group1**, assigned to port **1**, using **TGA** and **TGB** hardware items, with a Trunk member ID of **60**.

Create/update Avaya NES Trunk Span

You can create/update an Avaya NES Trunk Span and import the Trunk members of the Trunk Span. The following fields provide details of the import statement needed in a .csv file to import an Avaya NES Trunk Span.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you will create or update an Avaya NES Trunk member	Avaya NES Loop TrunkSpan
2*	Group Name	Name of the group to update or create	Group1

Field #	Field Name	Description	Examples
3	Description	Description of the member group.	Trunk span cubes 1-24 on 4th floor
4*	Number of Ports	Number of ports	24
5	Associated Dialer Data Source	The name of the Dialer data source, if any, associated with the trunk span	Sacramento
6	Recorder Control Type	Recorder Control Type	"Recorder Controlled"
7	Recorder Serial Numbers	Associates the member group to the specified recorders in this field. One or more recorder serial numbers can be specified.	Use the format "62393" for single serial numbers, or "{62393, 65353, 63732}" for multiple serial numbers.
8*	Loop Number	Loop Name of the Trunk Span	3
9	Enable Fallback	Allows Fallback mode to be enabled or disabled (when value is False)	True (Default is False)

* Required fields. Other fields are not required.

Sample Line in .csv file:

```
NES TrunkSpan, Group1, Trunk span cubes 1-24 on 4th floor,
Sacramento, 24, Recorder Controlled, 62393, 3
```

The above example creates or updates an Avaya NES Trunk Span named **NES TrunkSpan** in the member group **Group1**, consisting of **Trunk span cubes 1-24 on 4th floor** (that is, extensions in cubicles 1 through 24 on the building's 4th floor) from **24** ports that are **Recorder Controlled** from Recorder serial number **62393**, in loop number **3**.

Create/update Avaya NES Trunk Span members

You must import the trunk span members along with the Trunk Group. Any member not specified is deleted.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you will create or update a Trunk Span member	Trunk Span
2*	Member Group Name	The Avaya NES Trunk Span member group name	Group1

Field #	Field Name	Description	Examples
3*	Port Number	The port number of the group to which this primary extension has been assigned.	1
4	Member Name	The trunk member	1000
* Required fields. Other fields are not required.			
Sample Line in .csv file:			
Trunk Span, Group1, 1			

In the above example, an Avaya NES Trunk Span member is created or updated, as indicated by **Trunk Span**, which belongs to member group **Group1** using port **1**.

Switch-specific import working examples

You can use the examples in this section to better understand the import syntax, or as the foundation for importing for the various data sources. Each example contains a statement of import formats preceded with the comment symbol (#) followed by actual examples.

Alcatel Import Example

```
#Object Type,Name,Trunk Group Name, Description,NumberOfPorts,Recording Control
Type,Recorder Serial Numbers,Coupler, Crystal, First Time slot
Alcatel TrunkSpan, Atlanta Alcatel, "this is the atlanta alcatel description", 30, Recorder Controlled,
673653, 4, 33, 9
#Object Type, Trunk Group, Port, Member Name (Optional)
Trunk Member, Atlanta Alcatel, 1,
Trunk Member, Atlanta Alcatel, 2, 4_33_38
```

Aspect Import Example

```
#Object,Name,Description,NumberOfPorts,RecordingControlType,Recorder,TrunkGroup,Starting
Device Number
Aspect TrunkSpan, AtlantaAspect, "this is the atlanta aspect description", 24, Recorder
Controlled,REPLACE_WITH_RECORDER, tg1, 3
```

```
#object type, Trunk Span Group Name, Port, Member (Optional)
Trunk Member, AtlantaAspect, 1,
Trunk Member, AtlantaAspect, 2, 2_9
```

Cisco Import Example

```
#Object, Extension, RecordingMode, Recording Control Type, Secondary Extension
Datasource, Cisco
Property, Cisco Import, TRUE,
```

```
#Object Type, Primary Extension, Recording mode, Recording Control Type, Secondary Extensions  
Extension, 1000, Record, CTI Controlled , "{2000,Record}"  
Extension, 1001, Record, "Recorder Controlled" , "{2001,Record}"  
Extension, 1002, Record, CTI Controlled , "{2002, Do Not Record}"  
Extension, 7002, Record, Selective Delivery (Duplicate Streamed) , "{2002, Do Not Record}"
```

IP (Auto-create) Import Example

```
#Object, DataSource Name, IF associations, Type, Description, Seating Type, Switch Type,  
Datasource, AutoCreated IP Phone, ,Phone , , Free, Cisco IP
```

```
#Object Type, Pool Name, Description, Recording Type, Site, Recorders
```

```
IP ExtensionPool,IPPool1, updated pool1, CTI Controlled,"{REPLACE_WITH_SERIAL1,REPLACE_WITH_  
SERIAL2}",  
IP ExtensionPool,IPPool2, IPPool2 Description, CTI Controlled,REPLACE_WITH_SITE,,  
IP ExtensionPool,IPPool3, new pool2, Recorder Controlled,,REPLACE_WITH_SERIAL1,  
IP ExtensionPool,IPPool3, new pool4, Recorder Controlled,,,
```

```
#Object Extension RecordingMode Member Group Secondary Extension/Mode  
Extension, 1000, Do Not Record, "IPPool1","{1001, Application Controlled}",  
Extension, 1001, Application Controlled , IPPool1,"{{2001, Record }, { 2002, Do Not Record }}",
```

```
Extension, 1003, Record, IPPool2,,  
Extension, 1004, Record, IPPool2,,
```

```
Extension, 2948, Record, IPPool2,,  
Extension, 2949, Record, IPPool2,,  
Extension, 2950, Record, IPPool2,,  
Extension, 2951, Record, IPPool2,,  
Extension, 2952, Record, IPPool2,,  
Extension, 2953, Record, IPPool2,,  
Extension, 2954, Record, IPPool2,,  
Extension, 2955, Record, IPPool2,,  
Extension, 2956, Record, IPPool2,,  
Extension, 2957, Record, IPPool2,,
```

```
Extension, 2958,  
Extension, 2959,
```

IP Import Example

```
#Object Type, Pool Name, Description, Recording Type, Site, Recorders
IP ExtensionPool,IPPool1, updated pool1, CTI Controlled,"{REPLACE_WITH_SERIAL1,REPLACE_WITH_
SERIAL2}",
IP ExtensionPool,IPPool2, IPPool2 Description, CTI Controlled,REPLACE_WITH_SITE.,
IP ExtensionPool,IPPool3, new pool2, Recorder Controlled,,REPLACE_WITH_SERIAL1,
IP ExtensionPool,IPPool3, new pool4, Recorder Controlled,,,

#Object Extension RecordingMode Member Group Secondary Extension/Mode


- Extension, 1000, Do Not Record, "IPPool1","{1001, Application Controlled}",
- Extension, 1001, Application Controlled , IPPool1,"{{2001, Record }, { 2002, Do Not Record }}",


Extension, 1003, Record, IPPool2.,
Extension, 1004, Record, IPPool2.,
Extension, 2948, Record, IPPool2.,
Extension, 2949, Record, IPPool2.,
Extension, 2950, Record, IPPool2.,
Extension, 2951, Record, IPPool2.,
Extension, 2952, Record, IPPool2.,
Extension, 2953, Record, IPPool2.,
Extension, 2954, Record, IPPool2.,
Extension, 2955, Record, IPPool2.,
Extension, 2956, Record, IPPool2.,
Extension, 2957, Record, IPPool2.,
Extension, 2958,
Extension, 2959,
```

Generic Trunk Span Import Example

```
#Object,Name,Description, NumberOfPorts,RecordingControlType,Recorder(OPTIONAL)
Generic TrunkSpan, GenericAtlantaTrunkSpan, "this is the atlanta Generic Trunk Span description",
24, Recorder Controlled

#Object, MemberGroup Name, Port, Hardware, Hardware, Trunk Member
Trunk Member, GenericAtlantaTrunkSpan, 1,hw1 ,hw2 , 111
Trunk Member, GenericAtlantaTrunkSpan, 2, anotherhw1, anotherhw2, 114
```

Avaya NES Import Example

```
#Object Type, Name, Description(Optional), Number of Ports, Recording Control Type,Recorder
(Optional),Loop Number
NES TrunkSpan, nortel1, This is nortel, 24, Recorder Controlled,,2
```

#Object Type, TrunkSpan Name, Port Number, Member Name(Optional)

Trunk Member, nortel1, 1,

Trunk Member, nortel1, 2,

Trunk Member, nortel1, 3,

Trunk Member, nortel1, 4,

Trunk Member, nortel1, 5,

Trunk Member, nortel1, 6,

Scheduled Import Example

#Example of scheduling Format for schedule is

#Schedule, YYYY-MM-DD, HH:MM

Schedule, 2007-02-16,11:15

#Object Type, Pool Name, Description, Recording Type, Site, Recorders

IP ExtensionPool,IPPool1, updated pool1, CTI Controlled,"{REPLACE_WITH_SERIAL1,REPLACE_WITH_SERIAL2}",

IP ExtensionPool,IPPool2, IPPool2 Description, CTI Controlled,REPLACE_WITH_SITE,,

IP ExtensionPool,IPPool3, new pool2, Recorder Controlled,,REPLACE_WITH_SERIAL1,

IP ExtensionPool,IPPool3, new pool4, Recorder Controlled,,,

#Object Extension RecordingMode Member Group Secondary Extension/Mode

Extension, 1000, Do Not Record, "IPPool1","{1001, Application Controlled}",

Extension, 1001, Application Controlled , IPPool1,"{{2001, Record }, { 2002, Do Not Record }}",

Extension, 1003, Record, IPPool2,,

Extension, 1004, Record, IPPool2,,

Extension, 2948, Record, IPPool2,,

Extension, 2949, Record, IPPool2,,

Extension, 2950, Record, IPPool2,,

Extension, 2951, Record, IPPool2,,

Extension, 2952, Record, IPPool2,,

Extension, 2953, Record, IPPool2,,

Extension, 2954, Record, IPPool2,,

Extension, 2955, Record, IPPool2,,

Extension, 2956, Record, IPPool2,,

Extension, 2957, Record, IPPool2,,

Extension, 2958,

Extension, 2959,

Station-side Import Example

```
#Object Name Number of Ports Recording Control Type Recorder
```

```
Stationside Group, SSCard1Rec1, SS Card Desc, 8, Recorder Controlled ,REPLACE_WITH_RECORDER_SERIAL
```

```
Stationside Group, SSCard1Rec2, SS Card Desc, 8, Recorder Controlled ,REPLACE_WITH_RECORDER_SERIAL
```

```
#Object, Extension, RecordingMode, MemberGroup, Secondary Extension/Mode, MemberGroupPort
```

```
Extension, 11000, Record, SSCard1Rec1,, 1
```

```
Extension, 11001, Record, SSCard1Rec1,, 2
```

Trader Auto-create Import Example

```
#Object, DataSource Name, IF associations, Type, Description, Seating Type, Switch Type,  
Datasource, AutoCreatedTrader, , Trader
```

```
#Object Type (Trunk Span), Group Name, Description, Number of Ports, Recording Type, Associated  
Recorder Serial Numbers, Recorder Number, Starting Recording Channel
```

```
PCM32 TrunkSpan, Test Group1, ,32, Recorder Controlled,{REPLACE_WITH_RECORDER_SERIAL_  
NUMBER} , 6, 1000
```

```
PCM32 TrunkSpan, Test Group2, ,32, CTI Controlled,REPLACE_WITH_RECORDER_SERIAL_NUMBER , 9,  
9000
```

```
PCM32 TrunkSpan, Test Group3, ,32, Recorder Controlled,REPLACE_WITH_RECORDER_SERIAL_  
NUMBER , 92, 19000
```

Trader Non-Auto-create Example

```
#Object Type(DataSource), Data Source Name  
Datasource, Trader DataSource
```

```
#Object Type (Trunk Span), Group Name, Description, Number of Ports, Recording Type, Associated  
Recorder Serial Numbers, Recorder Number, Starting Recording Channel
```

```
PCM32 TrunkSpan, Test Group1, ,32, Recorder Controlled, {REPLACE_WITH_TDM_RECORDER_SERIAL_  
NUMBER}, 6, 1000
```

```
PCM32 TrunkSpan, Test Group2, ,32, CTI Controlled, REPLACE_WITH_TDM_RECORDER_SERIAL_  
NUMBER , 9, 9000
```

```
PCM32 TrunkSpan, Test Group3, ,32, Recorder Controlled, REPLACE_WITH_TDM_RECORDER_SERIAL_  
NUMBER , 92, 19000
```

Trunk Span Extension Import Example

```
#Object,Name,Description,NumberOfPorts,RecordingControlType,Recorder
```

```
Extension TrunkSpan, AtlantaExtensionSpan, Extension Span, 24, CTI Controlled, {REPLACE_WITH_  
RECORDER_SERIAL_NUMBER}
```

```
#Object Type, Extension, RecordingMode, Trunk Span, secondary extensions, port
```

```
Extension, 2000, Record, AtlantaExtensionSpan, "{{2002,Record},{3002, Record}}",1
```

```
Extension, 2001, Record, AtlantaExtensionSpan, "{2004,Record}", 2,
```

```
Extension, 2002, Do Not Record, AtlantaExtensionSpan, , 3
```

Trunk Span Import Example

```
#Object,Name,Description, NumberOfPorts,RecordingControlType,Recorder,Span Number, Start number
```

```
TrunkSpan TrunkSpan, AtlantaTrunkSpan, "this is the atlanta Trunk Span description", 24, Recorder Controlled, REPLACE_WITH_RECORDER, 3, 5
```

```
#object type, Trunk Span Group Name, Port, Member (Optional)
```

```
Trunk Member, AtlantaTrunkSpan, 1,
```

```
Trunk Member, AtlantaTrunkSpan, 2, 2_9
```

Trunk Span Trunk Group Import Example

```
#Object,Name,Description, NumberOfPorts,RecordingControlType,Recorder(OPTIONAL)
```

```
TrunkGroup TrunkSpan, AtlantaTG, "this is the atlanta TG description", 24, Recorder Controlled, REPLACE_WITH_RECORDER
```

```
#object type, Trunk Span Group Name, Port,Trunk Group, Trunk Member
```

```
Trunk Member, AtlantaTG, 1, 3, 99
```

```
Trunk Member, AtlantaTG, 2, 4, 22
```

LAN data source import formats

Use the LAN data source format to import workstations and workstation groups for screen recording into a LAN data source. This forms an efficient alternative to manually adding workstations and workstation groups. In the following tables, an asterisk (*) indicates mandatory fields.

Related topics

[Importing workstation groups \(page 600\)](#)

[Importing workstations \(page 601\)](#)

[LAN-specific import working examples \(page 602\)](#)

Importing workstation groups

The following fields provide the details of the import statement needed in a CSV file to import a workstation group. Nine fields are required in the import, as a result of screen recording requirements.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that you want to create or update a Workstation Group	Workstation Group
2*	Group Name	Name of the group to update or create	High Bandwidth
3	Description (Optional)	Description of the member group.	Group that contains workstations that is in close proximity to Recorder
4*	Recorder Serial Numbers	Associates the member group to the specified recorders in this field. One or more recorder serial numbers can be specified.	62393 or "{62393, 65353, 63732}"
5	Record Port Number	Record Port Number. This field is optional (if omitted the system will use the default of 4001).	4001
6*	Max Recordings	Maximum number of recordings that can occur on the workstations that belong to this group.	20
7	Quality (Optional)	Specifies quality of Screen Recording of the workstations in this group. Options are High, Medium, Low, and Custom.	Custom

Field #	Field Name	Description	Examples
8	Capture Rate (Default High)	Specifies the Screen Capture rate that should be used in Screen Recording of workstations in this group. This can be any number between 50 (high) and 250 (low).	100
9	Reduce Color Quality (Optional)	Specifies if Capture Color Quality has to be reduced. Yes is true, no is false.	true
Sample Line in .csv file:			
Workstation Group, High Bandwidth, Group that contains workstations that is in close proximity to Recorder, "{ 62393, 65353, 63732}", 5001,20,Custom,true,100			

The above example creates or updates a **Workstation Group** named **High Bandwidth** in the member group **Group that contains workstations that is in close proximity to Recorder**, recording from Recorder serial numbers **62393**, **65353** and **63732**, from port **5001**, allowing a maximum number of recordings that can occur in the group of **20**, with a screen recording quality of **Custom**, (others are High, Medium, and Low) screen capture rate of **100** (50 is high, 250 is low) and an instruction to reduce colors of **True** (for yes).

Importing workstations

You must import one or more workstations using a CSV file. Each workstation that has to be imported should be present in the CSV file in the following format.

Field #	Field Name	Description	Examples
1*	Object Type	This indicates that a workstation is to be created or updated.	Workstation
2*	Workstation Name	Hostname	Agent1
3	Workstation Group	Workstation Group to which this workstation belongs.	Atlanta Group
4	Description (Optional)	Description of the workstation	Agent1's Terminal
5	Domain	The domain to which the employee belongs.	witness
6	Platform (Optional)	Operating System Platform of the workstation	Windows
7	Phone Data Source (Optional)	Name of the Phone data source where you can look for the Extension field	CiscoSwitch

Field #	Field Name	Description	Examples
8	Extension (Optional)	Primary Extension to associate this workstation to. The Extension is looked up in the data source as specified in the Phone data source field.	1000

Sample Line in .csv file:

```
Workstation, agent1, Atlanta Group, Agent1's Terminal, witness,
Windows, CiscoSwitch, 1000
```

In the above example a **Workstation** is being created or updated with hostname **Agent 1**, in the **Atlanta Group**, named Agent1's Terminal, in the **witness** domain, using **Windows**, connected to the **CiscoSwitch** data source, with the extension **1000**.

LAN-specific import working examples

Use import working examples for review or to copy and paste text to a file in a text editor and form the foundation for importing for the various data sources. Each example contains a statement of import formats preceded with the comment symbol (#) followed by actual examples.

Auto-create LAN import example

```
#Object,DataSource Name, IF associations, Type, Description, Seating Type, Switch Type,
Datasource, AutoCreated LAN, , LAN, Auto created
#Object Type, WorkStation Group Name, Description, Recorder, Recording Port Number (Default
4001), Max Recordings, Quality, Reduce Quality, Refresh Rate
Workstation Group, group1,, RECORDER_SERIAL_NUMBER,1300 , 25,High,
Workstation Group, group2,, RECORDER_SERIAL_NUMBER,, 25,Low,
Workstation Group, group3,,, 2,Medium,
Workstation Group, group4,,, 25,Custom,true,50-1000
#Object,Host Name, Workstation Group, Description,Domain,Platform,PBX/ACD DS,Extension
Workstation, jdoe,group1, Some Description, Company, Anonymous Terminal Server , REPLACE_
WITH_PBX_DS_NAME, 1001
Workstation, jdoe1, group1, John Doe's Terminal, My Company, Windows , REPLACE_WITH_PBX_DS_
NAME, 1003
Workstation, workstation2
Workstation, workstation3
```

LAN import example

```
#Object Type, WorkStation Group Name, Description, Recorder, Recording Port Number (Default
4001), Max Recordings, Quality, Reduce Quality, Refresh Rate
Workstation Group, group1,, RECORDER_SERIAL_NUMBER,1300 , 25,High,
Workstation Group, group2,, RECORDER_SERIAL_NUMBER,, 25,Low,
Workstation Group, group3,,, 2,Medium,
Workstation Group, group4,,, 25,Custom,true,50-1000
```

#Object,Host Name, Workstation Group, Description,Domain,Platform,PBX/ACD DS,Extension

Workstation, jdoe,group1, Some Description, Company, Anonymous Terminal Server , REPLACE_WITH_PBX_DS_NAME, 1001

Workstation, jdoe1, group1, JohnDoe's Terminal, My Company, Windows , REPLACE_WITH_PBX_DS_NAME, 1003

Workstation, workstation2

Workstation, workstation3

System maintenance

System Maintenance refers to daily or regular system operations you need to do to maintain and troubleshoot the Recorder so it always runs at an optimum performance level.

You can also place a recorder in recorder maintenance mode. Placing a recorder in recorder maintenance mode is a way to gracefully shut down a recorder when you need to perform maintenance on that recorder.

Topics

Perform system maintenance	605
Duplicate and combine Recorders	611
Recorder maintenance mode	612

Perform system maintenance

Perform system maintenance to ensure that all hardware and software components are operating at peak efficiency. These are tasks that you perform on a regular basis, normally weekly, to obtain maximum flexibility with the Recorder with a minimum amount of service disruption.

Related topics

[Perform routine maintenance \(page 605\)](#)

[Follow a preventative maintenance schedule \(page 606\)](#)

[Perform hardware maintenance \(page 608\)](#)



You should also refer to the *Enterprise Suite Maintenance Guide* for important information about system maintenance and backups.

Perform routine maintenance

Perform daily, weekly, monthly, and quarterly maintenance routinely to ensure all calls are being recorded and stored correctly. For guidance on database maintenance see the *Enterprise Suite Maintenance Guide*.

Quick reference routine maintenance guide



All alarms should be addressed and their root conditions cleared.

Daily tasks

Item	Description
Recorder Alarms	Are there any errors?
Confirm Services are running	Are all the Recorder Services running?
Confirm Recording and Replay	Is the system recording calls, do they have the correct tagging and can you play them back?

Weekly tasks

Item	Description
Disk Capacity	Should match the capacity set in the Recorder Manager Disk Manager. 2 GB on all drives other than calls and 10 GB on calls is recommended.

Monthly tasks

Item	Description
Loading Trends	Is the call volume on the server acceptable?

Troubleshooting

Item	Description
User Specific	Is the issue specific to a given user, employee, or extension?
Workstation Specific	Is this related to one workstation? Can you replicate the problem on another workstation?
Environmental	Are you experiencing problems with other applications? You may need to contact your local IT help desk.
Detail	When logging a fault always include as much information as possible, such as the user name, the server you're accessing, what you saw and what you expected to see, your location and anything else you may have noticed. Extension, date, and time are important. This information helps the service desk analyze the issue quickly.

Follow a preventative maintenance schedule

For third party system management tools, consider including the monitoring of Recording components within your other system management regimes.

Examples of Recording components to include

- Microsoft System Management Server
- Microsoft Operations Manager
- CA Unicenter
- HP OpenView

All of the major management tools support the monitoring of Windows Event Logs and SNMP.

Daily tasks

Unless you have fully automated the alerting of these conditions, complete these procedures at the start of each day.

Recorder alarms

Log onto Recorder Manager (or Enterprise Manager) and check for Alarms. Check the contents of the Application/System Event log, and examine any events logged since the previous check. Look at all error and warning messages, not just those generated by the Recorder services. You can also create email alerts for alarms, or view alarms through Enterprise Manager.

Confirm services are running

Ensure that all services are running.

Confirm recording and replay

Check that calls are being uploaded into the database and are searchable and playable. The simplest way to do this is to use Viewer. Confirm that the start time of these calls is as you would expect, namely that they correspond to the most recent calls made on the extensions being recorded.

Confirm the following:

- That these calls are playable and that audio quality is good.
- That the information displayed for each call is reasonable.
- That both inbound and outbound calls are recorded (if applicable).
- Internal calls are recorded (if applicable).

Weekly tasks

As you become more confident with the normal operation of your recording system, you can reduce the frequency of weekly tasks. For example, if you know the rate at which your disk is filling up is much less than the available space, you may check this less often.

Disk capacity in the calls directory

When your recorder is first installed, the disk is almost empty. As it gradually fills, you should note the rate at which it is being used (at least weekly) and extrapolate to estimate when the disk will be full. At this point the Disk Manager Service begins deleting the oldest calls to make room for new ones. If this appears to be about to happen to calls that are younger than planned, check the configuration of the recorder to ensure the correct calls only are being recorded and add additional disk capacity to the partition before it fills.

Disk capacity check in all partitions

On a weekly basis, you should check the available space on any other disk partitions. If your server has more than one disk or partition, for example, your programs are installed on C: but recordings placed on D: you must check that these other drives have sufficient space.

An alert will warn you if the system drops below 2 GBs of free disk space—set up an email alert through Enterprise Manager or check for these warning periodically. This could be caused by accumulated temporary files or log files that may need to be manually purged. When doing so, remember that files you delete go to the recycle bin and their space is not freed till you empty the recycle bin.

Monthly tasks

Examining call volumes and formatting your call drive are tasks that you should perform monthly.

Loading trends

You should note the total call volumes recorded every month in order to be aware of gradually increasing traffic trends. To do this:

1. Note the number of calls recorded. Unless the system has been restarted, this value can be obtained from System Monitor area (under System). In the Capture: Call Control area, note, the Calls Recorded value.
2. Note the age of the oldest call on the disk (only applicable once the disk has filled for the first time).
3. Plot the CPU load during the busy hour.
4. Alarms will appear for high CPU usage; consider increasing the server specification.

Fragmentation

Formatting your calls drive with a cluster size of 64KB will ensure that fragmentation of the drive will be reduced significantly to the point where checks are only needed half yearly. Failure to do so can cause the fragment to affect CPU usage over time.

Perform hardware maintenance

Perform hardware maintenance to ensure that all hardware devices such as media devices and hard drives are working properly and that you can efficiently maintain any component, including replacing that component, at any time. This includes adding an archive device, changing voice cards, changing a hard drive, changing wiring and adding telephone extensions.

Related topics

[Change voice cards/NICs \(page 608\)](#)

[Replace a hard drive \(page 609\)](#)

Change voice cards/NICs

The Voice Card(s) Auto-Detection feature of the Recorder automatically detects any changes to the hardware configuration on the start-up of the capture component. If any voice cards have been added or existing ones replaced they are detected automatically and show in the Recorder Manager with one of the listed statuses.

Card statuses

Card Status	Description
Newly Added	The card did not exist previously.
Removed	The card has been removed from that slot.
Existing	The card has existed in the system before.
Replaced	Previously existing card of the same type has been replaced with a new card of same type.

Procedure

1. Stop all the Recorder components.
2. Shut down the Recorder host and switch off the power supply.

3. Insert new card(s) or replace existing cards from the Recorder host.



An anti-static cuff is recommended to avoid shocks resulting from static electricity.

4. Restart the Recorder components. The capture engine on start-up will automatically detect the hardware changes and raises the appropriate alarm(s).
5. Sign in to Recorder Manager and click **Alarms** to view all alarms for voice cards that have been added or removed.
6. Click **General Setup > Voice Cards > Cards**. The pane on the left displays the slot number and bus number for all the cards that have been recognized by the Recorder.
7. Choose any of the card(s) displayed in the left panel and configure it as necessary and then click **Save**.



Voice cards with a status of **Removed** can be copied but cannot be configured and saved.

8. Restart the Capture Component for the configuration changes to take effect.

Related topics

[Start and stop Recorder components \(page 265\)](#)

Replace a hard drive

Replace a hard drive to increase the capacity of the calls buffer or database storage or to correct a defective hard drive or improve the disk capacity of an existing hard drive. Different procedures exist for the different roles for hard drives. In all cases, you need to initialize, partition, and format the new hard drive. These tasks can usually be completed by using Wizards in the Windows operating system. You can also use DOS commands.



Remember that hard drives must be handled carefully. Avoid static electricity and any magnetic devices such as screwdrivers with magnetic tips. It is strongly recommended that you use an anti-static cuff when handling electronic devices and appliances.

Increase the capacity of the call buffer

1. Back up the Calls as described in [Back up the Recorder configuration \(page 262\)](#).
2. Shutdown the Recorder components as described in [Start and stop Recorder components \(page 265\)](#).
3. Shut down the host and replace the hard drive.
4. Restart the host and restore the Calls from the backup on to the new drive.
5. Restart the Recorder components.
6. Sign in to the Recorder Manager and choose **General Setup > Disk Management > Drives**.
7. Configure the new drive to be monitored.
8. Restart the Disk Manager component.

To swap out a SCSI hard drive

Swap out a hard drive in a RAID setup by removing the old hard drive and inserting and formatting the new one.

1. Follow procedures described in to replace a hard drive containing data only.
2. At the point where you must format the hard drive, launch your RAID user interface and then format and partition the hard drive.
3. Copy all data from the backup source or allow a mirror disk to copy all information.

Duplicate and combine Recorders

You may need to duplicate or combine Recorders if an existing Recorder must be migrated onto a new host for performance, or for reasons such as outdated hardware. Duplicating/cloning preserves the configuration and data of the Recorder.

To duplicate a Recorder and database server that are on the same machine (single-box configuration)

1. Back up the existing Recorder as described in [Back up the Recorder configuration \(page 262\)](#).
2. Move the voice cards and trunks onto the new machine.
3. Install the Recorder software on the new machine.
4. Restore the Recorder on the new host as described in [Recover the Recorder configuration \(page 263\)](#).

To duplicate a Recorder and database server on different machines

1. Back up the existing Recorder as described in [Back up the Recorder configuration \(page 262\)](#). Do not backup the system databases.
2. Move the voice cards and trunks onto the new machine.
3. Install the Recorder software on the new machine.
4. Restore the Recorder on the new host as described in [Recover the Recorder configuration \(page 263\)](#). Do not restore the system databases.

Recorder maintenance mode

Use Maintenance mode to take Recorder server roles offline selectively for planned maintenance. Maintenance might include installing hotfixes, updating software, powering off a Recorder, and replacing hardware. By gracefully winding down server roles, the system can route real-time recording to comparable, redundant servers in the Verint system.

 Although it is possible to shut down a Recorder without first placing it in maintenance mode, doing so means that real-time interactions will not be recorded.

Supported services

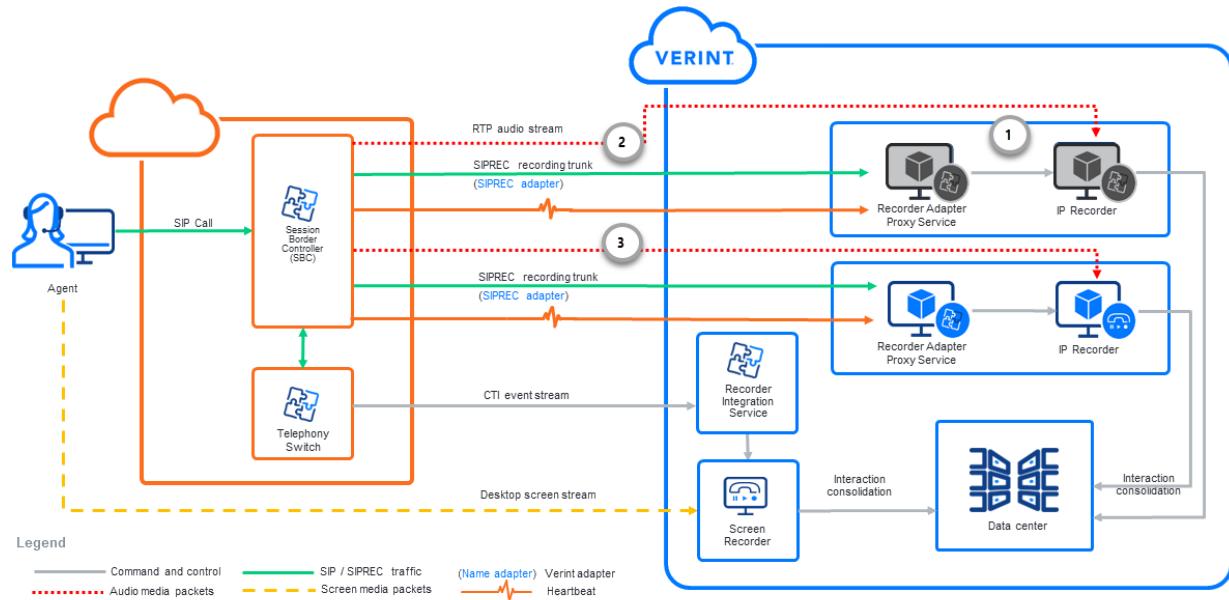
Maintenance mode is supported for the following PBX services and Verint server roles.

PBX service	IP Recorder and IP Recorder Video	Recorder Adapter Proxy Service (RAPS)
SIP/SIPREC VoIP delivery	Yes	Yes
Selective Device Media and Call Control (DMCC)	Yes	No

Requirements

- The RAPS nodes must be co-located with the IP Recorders within the target group.
- There must be enough Recorders with the same server roles and the capacity to handle additional traffic.
- A Verint user must have the **Edit Component Services** user security privilege to put the Recorder in maintenance mode.

Technical overview



1. A user puts the Recorder Adapter Proxy Service (RAPS), IP Recorder, or both server roles on a Verint Recorder into maintenance mode.
2. The roles remain active until all in-progress interactions are completed.
3. New, incoming interactions are routed to other Recorders on the site.

IP Recorder behavior in maintenance mode

The IP Recorder and IP Recorder Video roles enter maintenance mode together. When you put one role in maintenance mode, the other role automatically enters maintenance mode too.

To speed up the transition to maintenance mode, the controlling RIS or RAPS nodes redirect in-progress recordings to available redundant server roles. When a suitable server role cannot be found, the Recorder continues to handle ongoing interactions. Only when all interactions disconnect, does the Recorder enter maintenance mode.

In maintenance mode, the system routes new interactions to other Recorders on the site. If the system cannot find a suitable Recorder, it tries to deliver interactions to the Recorder that is in maintenance mode to avoid losing data. However, if the Recorder is shut down, the interactions are not recorded.

RAPS behavior in maintenance mode

In maintenance mode, the Recorder Adapter Proxy Service (RAPS) role continues to handle the current interactions. New interactions are redirected to a redundant RAPS server. When all interactions have disconnected, the RAPS role enters maintenance mode. If there are no available RAPS roles to handle new interactions, the interactions are not recorded.

Related topics

[Maintenance mode reference \(page 615\)](#)

[Put a server in or out of maintenance mode \(page 614\)](#)

Related information

Recorder redundancy (*Recorder Configuration and Administration Guide*)

Resilience and Redundancy (*Recorder Configuration and Administration Guide*)

Put a server in or out of maintenance mode

You can put the IP Recorder and Recorder Proxy Adapter Service (RAPS) server roles in maintenance mode to avoid losing real-time recordings during planned maintenance of a Recorder server.

Before you begin

- Ensure that there are enough Recorders with the same server roles and the capacity for additional traffic.
- You must have the Edit Component Services user security privilege to perform this procedure.

Procedure

1. In Verint, select **System Management**, under **Enterprise**, select **Settings**.
2. In the Installations pane, select a Recorder server node, then click **Launch**.
3. In Recorder Manager, select **Operations > Recorder Maintenance**.
4. Select the server roles, then click **Enter Maintenance**.

The screenshot shows the 'SERVER MAINTENANCE' section of the Verint interface. At the top, there are navigation links: STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP. Below these are buttons for Recorder Maintenance (with options Start and Stop), Refresh Rate (set to 1 Minute), and a refresh icon. The main area is titled 'SERVER ROLE MAINTENANCE MODE:' and contains a table with the following data:

Role Name	Current Mode	Target Mode	Status Details
IP Recorder	Maintenance		
IP Recorder Video	Maintenance		
Recorder Adapter Proxy Service	Normal		

At the bottom of the table are four buttons: Select All, Select None, Enter Maintenance (which has a mouse cursor over it), and Exit Maintenance.

5. Wait for the **Current Mode** status field to change from **Entering maintenance mode** to **Maintenance**.

A server role enters maintenance mode when it is no longer handling the current interactions.

6. Stop any services or turn off the Recorder, and perform the required maintenance.
7. When maintenance is finished:

- a. Restart the services.
- b. When all services are running, click **Exit Maintenance**.

The **Current Mode** status field changes to **Exiting maintenance mode**, then to **Normal**. When the mode is **Normal**, the Recorder is available to record calls.

Related topics

[Recorder maintenance mode \(page 612\)](#)

Maintenance mode reference

The Server Role Maintenance Mode page displays the current status of the Recorder server roles and provides details about the transition from one mode to the other. You can put roles in and out of maintenance mode from this page.

The screenshot shows the 'VERINT' logo at the top left. To its right is a navigation bar with links: STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP. Below the navigation bar, there's a sub-menu for 'Recorder Maintenance' with options 'Start and Stop'. The main content area is titled 'SERVER ROLE MAINTENANCE MODE:' and contains a table. The table has columns: 'Role Name', 'Current Mode', 'Target Mode', and 'Status Details'. Under 'Role Name', three items are listed: 'IP Recorder' (Maintenance), 'IP Recorder Video' (Maintenance), and 'Recorder Adapter Proxy Service' (Normal). At the bottom of the table are buttons for 'Select All', 'Select None', 'Enter Maintenance' (with a cursor pointing to it), and 'Exit Maintenance'. A 'Refresh Rate' dropdown is set to '1 Minute'.

Role Name	Current Mode	Target Mode	Status Details
IP Recorder	Maintenance		
IP Recorder Video	Maintenance		
Recorder Adapter Proxy Service	Normal		

The page displays the following information:

Column	Description
Role Name	Lists all server roles on the server that can be placed into maintenance mode.

Column	Description
Current Mode	<p>Lists the current mode of the server role. Possible values include:</p> <ul style="list-style-type: none"> • Normal - The server role can record calls. • Maintenance - The server role cannot record calls. You can safely install software or shut down Windows services on the Recorder. • Entering maintenance mode - The server role is transitioning from normal mode to maintenance mode. • Exiting maintenance mode - The server role is transitioning from maintenance mode to normal mode.
Target Mode	<p>The mode to which the server role is currently transitioning; either Normal or Maintenance.</p> <p>This field is only used when the role is in the midst of a transition and will be blank when the Current Mode is Normal or Maintenance. This field may also be blank if there is an error in the transition of the server role from one mode to the other.</p>
Status Details	Displays the relevant details about the transition of a server role from one mode to the other and about any errors.

Sort by column

You can sort the **Role Name**, **Current Mode**, and **Target Mode** columns in ascending or descending order. To sort a column, place your mouse over the column heading and click the small arrow that appears in the heading. By default, the **Role Name** column is sorted in ascending order.

Buttons

Use the **Select All** and **Select None** to quickly choose roles.

Use the **Enter Maintenance** and **Exit Maintenance** buttons to change modes.

Error messages

If an error occurs during the transition from one mode to the other, an error message appears above the **Server Role Maintenance Mode** heading at the top of the page.

Related topics

[Put a server in or out of maintenance mode \(page 614\)](#)

[Recorder maintenance mode \(page 612\)](#)

Recovery procedures for a site Recorder

If necessary, for disaster recovery when replacing a site Recorder, use the steps provided to return a Recorder to an operational state.

Topics

Back up existing settings and data	618
Install software and restore data on the new server	619
Test the new Recorder	621

Back up existing settings and data

Complete these procedures for your Recorder before recovery is required.

Before you begin

For data recovery, you need an offline storage location that is accessible to the new server. The offline storage location is used for the Call Buffer and the Archive directories.

1. Note the software version

Make a note of the software version that is currently running on the server you are going to replace. This includes the major software version, service pack, HFRx, and KBx.

Example: 11.2 HFR3 KB115520

2. Back up the Recorder configuration and document drives

- a. Create a back up of the Recorder configuration, as described in [Back up the Recorder configuration \(page 262\)](#).

- b. Document the Recorder drive letters and associated configuration.

3. Document the Recorder Integration Service adapters and settings

- a. In Recorder Manager, go to **General Setup > Integration Adapters > Settings**.

- b. Write down the name of the Recorder Integration Service Adapters and their settings.

4. Back up the Call Buffer

- a. Log on to the Recorder Manager application.

- b. Navigate to **General Setup > Recorder Settings > Recorder Settings**.

- c. Note the location of the **Call Buffer Path**.

- d. Back up the Call Buffer to an offline location.

5. Back up the Archive directories

Back up all Archive directories (location where calls are archived) to an offline location.



If you archive locally on the server, it is essential that you back up regularly the local locations. Regular backups ensure you have up-to-date Archive information.

Install software and restore data on the new server

When you have backed up the Recorder configuration and data, and documented the required settings, you are ready to install the software and restore the data to the new server.

Before you begin

If replacing the Recorder, you need a server that meets the requirements specified in the Customer Furnished Equipment Guide.

1. Install the software

- a. Shut down the Recorder server you are replacing.
- b. Install the base operating system on the new server.
 - Use the same server hostname as the defunct server.
 - Configure all drive letters and drive configurations the same as used on the defunct server.
- c. Install the Recorder platform to the same software level as the server you are replacing. For detailed instructions, refer to the "Platforms Installation" section of the *Workforce Optimization Installation Guide*.

2. Configure Enterprise Manager

- a. Log on to Enterprise Manager.
- b. Go to **System Management > Enterprise > Settings**, and save the server configuration.
- c. Wait five minutes to allow sufficient time for the configuration to redistribute.

3. Restore the Calls Buffer and Archive directories

 For all restore operations immediately following, be certain you use the same location on the new server as used on the old server.

- a. Copy the backed up call buffer to the new server.
- b. Restore any Archive directories to the new server.

4. Update the last INUM in the server's registry

- a. Get the latest INUM from the Call Path Buffer folder.
- b. Update the server's registry with the next INUM number.
HKLM\Software\Wow6432Node\Witness\eQRecord, NextCallINum = INUM + 1.

5. Restore the Recorder configuration

Restore to the new server the Recorder configuration you backed up in [Back up existing settings and data \(page 618\)](#).

Use the procedure described in [Recover the Recorder configuration \(page 263\)](#).

6. Configure the Recorder Integration Service adapters and settings

- a. In Recorder Manager, go to **General Setup > Integration Adapters > Settings**.
 - b. Configure the Recorder Integration Service Adapters and settings, as captured when completing [Back up existing settings and data \(page 618\)](#).
7. **Update the Archive watermark**

Change the Archive watermark to the point where the last INUM was archived.

Test the new Recorder

To ensure the proper operation of the new Recorder, complete the required tests.

Tests

1. Test replay of calls recorded before and after server recovery.
2. Test replay of archived calls that are no longer on the disc buffer.
3. Test archive of new calls recorded after the server replacement.
4. Test replay from archive of new calls recorded after the server replacement.



Verint Global Headquarters

175 Broadhollow Road
Suite 100
Melville, NY 11747 USA

info@verint.com
1-800-4VERINT

www.verint.com

© 2025 Verint Systems Inc.
All Rights Reserved Worldwide.
Confidential and Proprietary Information of Verint Systems Inc.

The contents of this material are confidential and proprietary to Verint Systems Inc. and may not be reproduced, published, or disclosed to others without express authorization of Verint Systems Inc.