

CDR SEARCH TOOL

USER GUIDE / VERSION 1.1.0

PLATFORM	Cisco CUCM
APPLICATION	Windows
DOCUMENT	Installation, operation and troubleshooting
WEBSITE	scotthudson.com.au

Search, retain and report on Cisco CUCM call detail records without working directly with raw CDR files.

CONTENTS

01	Introduction
02	Installation
03	Initial Configuration
04	CUCM CDR and SFTP
05	Search Records
06	CDR on Demand
07	Report History
08	Users and Roles
09	Retention and Storage
10	Historical Import
11	Updates and Rollback
12	Logs and Troubleshooting

INTRODUCTION

CDR Search Tool is a local Windows application for receiving, indexing, searching and reporting on Cisco Unified Communications Manager (CUCM) call detail records.

The application is intended to make routine call-record investigation easier without requiring an operator to manually locate and interpret raw CDR files. CUCM can deliver CDR files to the application over SFTP, after which the records are indexed and made available through the web interface.

Core functions

The application provides the following core functions:

- Live CDR ingestion over SFTP.
- Search by calling or called number, date and time.
- Ad-hoc CDR on Demand reporting.
- Report export.
- Historical CDR import.
- User and role management.
- Report history for auditability.
- Storage and retention controls.
- Application and security logging.
- Managed update and rollback workflow.

Deployment model

CDR Search Tool is designed to run locally on Windows. The application exposes its user interface over HTTP and includes an SFTP receiver for CUCM file delivery.

The default application HTTP port is 3080. SFTP uses port 22.

The application is not a CUCM management platform. It consumes CDR data generated by CUCM and provides a searchable reporting layer over that data.

Public edition

The public edition is intended to remain free to use. Its retained searchable record history is limited to 30 days. This keeps the public build useful for operational troubleshooting while keeping the product simple to distribute and support.

Version 1.1.0 adds a permanent Full Licence. A one-time A\$100 purchase unlocks longer configurable retention for one organisation and one installation, with no licence expiry and all future Call Records updates included. Both editions use the same installer.

Experimental data verification is excluded from this release. The software and its licence do not certify that the source call records are complete.

Documentation scope

This guide covers installation, initial setup, CUCM file delivery, searching, reporting, retention, users, updates and troubleshooting.

Where an organisation has its own security, firewall, change-management or software-distribution requirements, those local requirements take precedence over this guide.

INSTALLATION

CDR Search Tool is distributed as a Windows release package. The release package should also contain a copy of this user guide and release notes.

Before installation

Confirm that the Windows host has:

- A stable IP address or DNS name if CUCM will send CDR files to it.
- TCP port 3080 available for the application interface.
- TCP port 22 available if the built-in SFTP receiver will be used.
- Sufficient storage for the configured record-retention period and received CDR files.
- Local permissions appropriate for installing and running the application.

For a server or shared workstation deployment, use an address that will not change unexpectedly. CUCM must be able to reach the SFTP service on the host.

Windows Firewall

If Windows Defender Firewall is enabled, inbound rules are required for the application and SFTP receiver.

Example PowerShell commands:

```
New-NetFirewallRule -DisplayName "CDR Search Tool HTTP" -Direction Inbound -Protocol TCP  
-LocalPort 3080 -Action Allow  
New-NetFirewallRule -DisplayName "CDR Search Tool SFTP" -Direction Inbound -Protocol TCP  
-LocalPort 22 -Action Allow
```

Apply firewall changes according to your organisation's security policy.

Install the release

Run the installer from the release package and complete the installation. After installation, start CDR Search Tool using the installed application shortcut or service workflow provided by the release.

Open a browser on the host and browse to:

```
http://localhost:3080
```

From another device, use the Windows host's IP address or DNS name:

```
http://<host>:3080
```

First validation

Before configuring CUCM, confirm:

- The application interface loads.
- You can sign in with the initial administrative account supplied by the release.
- The SFTP receiver can be enabled.
- The application reports a healthy running state.
- The data/storage location has sufficient free space.

Change any supplied default administrative password before placing the application into normal use.

INITIAL CONFIGURATION

After installation, complete the local application setup before enabling production CDR delivery.

Sign in

Open the application interface and sign in using an administrative account.

Administrative users can manage application settings, users, retention and the SFTP receiver. Access available to other users depends on their assigned role.

Configure the SFTP receiver

Open the application settings and enable the SFTP receiver when the host is ready to accept CDR files.

Record the following information because it will be required when configuring CUCM:

- Windows host IP address or DNS name.
- SFTP port, normally 22.
- SFTP username.
- SFTP password or authentication details used by the release.
- Remote upload directory. The receiver uses `/incoming` for CDR delivery.

Configure retention and storage

Set the required retention policy before importing large historical datasets or enabling a busy CUCM cluster.

The application can enforce storage policy using record retention and storage limits. The public edition is limited to 30 days of searchable record retention.

Retention should be selected with consideration for:

- Daily call volume.
- Available disk capacity.
- Local audit requirements.
- The difference between retained source files and indexed database data.

Create users

Create named user accounts for people who require access.

Use the least-privileged role appropriate to each user. Administrative access should be limited to people who need to manage configuration, users or application operation.

Validate time

Accurate time is important when searching call records. Confirm the Windows host has the correct time, date and timezone before live ingestion begins.

CUCM CDR AND SFTP

CDR Search Tool receives CDR files from Cisco Unified Communications Manager using SFTP.

Application-side details

Before making CUCM changes, confirm the CDR Search Tool receiver is enabled and reachable.

Typical destination details are:

- Protocol: SFTP
- Port: 22
- Destination host: the Windows host running CDR Search Tool
- Remote directory: `/incoming`

The exact username and authentication details are defined by the local CDR Search Tool installation.

CUCM configuration

Configure CUCM CDR delivery using the normal Cisco CDR Repository Manager destination workflow for the CUCM version in use.

Use the CDR Search Tool host as the SFTP destination and `/incoming` as the remote directory.

This guide intentionally does not prescribe organisation-specific CUCM change procedures. CUCM configuration should be performed by an authorised voice administrator and follow local change-management requirements.

File delivery behaviour

CUCM may deliver CDR files frequently. A busy system can generate and transfer files at intervals shorter than the nominal CDR file time setting. The application is designed to process files as they arrive rather than assuming one file per configured interval.

Validation

After the destination is configured:

- Place one or more test calls.
- Confirm files arrive in the SFTP receiver.
- Confirm ingestion completes without error.
- Search for the test call using the relevant number and time.
- Check application logs for failed or rejected files.

Do not treat successful SFTP authentication alone as proof that CDR ingestion is complete. Validate that records are visible in search results.

SEARCH RECORDS

Search Records is the primary operational view in CDR Search Tool.

Search criteria

Searches can be narrowed using:

- Calling number.
- Called number.
- Date range.
- Time range.

Use the smallest useful time range when investigating a specific incident. This makes results easier to interpret and reduces unnecessary processing on large datasets.

Number searches

Enter the number available from the incident or user report. Depending on CUCM dial-plan behaviour, the stored value may reflect the number as processed by CUCM rather than the exact digits a user remembers dialling.

If an expected call is not returned:

- Broaden the time range.
- Search the alternate call leg or known destination.
- Check whether transformations, prefixes or external presentation altered the stored number.
- Confirm the CDR file covering that time was ingested.

Results

Search results are presented in a table so the operator can compare call records and identify the relevant call leg or sequence.

The records should be treated as CUCM-generated call-detail data. Interpretation may require knowledge of the organisation's dial plan, route patterns, trunks, gateways and call flows.

Reporting

When a search needs to be retained or shared, use the available reporting/export workflow rather than manually copying raw CDR data.

CDR ON DEMAND

CDR on Demand provides an ad-hoc report workflow for investigations that need a defined dataset rather than an interactive search only.

Build a report

Choose the required report criteria and time period, then run the report.

Use a clearly defined date and time window wherever possible. Large, open-ended reports may contain significantly more records than required for the investigation.

Export

Completed reports can be exported for authorised operational use.

Exported call-record data can contain phone numbers and operational metadata. Store and distribute exports in accordance with the organisation's privacy, security and records-management requirements.

Report history

Running an on-demand report creates a report-history entry. Report history is intended to remain an immutable audit record of who ran a report and when.

There is no normal UI workflow for deleting report-history entries, including for administrative users.

Operational practice

For repeat investigations, record enough context outside the application to explain why a report was generated. The application records the report event; the surrounding incident or ticketing system should record the operational reason.

REPORT HISTORY

Report History records generated reports so there is a durable application-side record of reporting activity.

Source-of-truth behaviour

Report History is intentionally immutable from the user interface.

No application role, including an administrator, should be able to delete individual report-history entries through the UI.

This behaviour is deliberate. The history is intended to answer basic audit questions such as:

- Who ran a report?
- When was it run?
- What report activity occurred during an investigation period?

Access

Access to report history depends on the permissions assigned to the signed-in user.

Where a report or export is associated with a formal incident, request or investigation, keep the external ticket or case reference in the organisation's normal record-keeping system.

Administration

Do not use direct database modification as a routine method of altering report history. Any maintenance that affects audit data should be treated as an exceptional administrative action and documented accordingly.

USERS AND ROLES

CDR Search Tool supports named user accounts and role-based access.

The application uses three primary roles:

- Admin
- Super User
- User

Admin

Administrative users can manage application configuration and user accounts in addition to using operational functions.

Admin access should be restricted to people who are responsible for the application itself.

Super User

Super User access is intended for operators who require broader reporting or operational capability without full application administration.

User

User access is intended for normal operational use with the lowest level of privilege required to search or work with records.

User management

Administrative workflows include:

- Create users.
- Edit users.
- Assign or change roles.
- Reset a user's password to the application's default-reset state.
- Delete user accounts when they are no longer required.

Password handling

After a password reset, the affected user should change the temporary/default password as soon as possible.

Do not share named accounts between staff. Individual accounts improve accountability in logs and report history.

Session handling

The application header identifies the signed-in user and provides a sign-out action. Users should sign out when using a shared workstation.

RETENTION AND STORAGE

CDR Search Tool stores received CDR data locally. Retention and storage controls prevent the application from consuming unlimited disk capacity.

Public edition retention

The public edition is limited to 30 days of searchable record retention.

The limit is designed for ongoing operational troubleshooting rather than long-term enterprise call-record archiving.

Full Licence activation

The Full Licence costs A\$100 once for one organisation and one installation. It has no expiry and includes all future updates to Call Records. It unlocks configurable retention beyond 30 days, up to the application's supported setting of 36,500 days. Available disk space and your storage policy still limit retained data.

- Open **Administration**, then the **Licensing** card.
- Copy the installation **Instance ID** before purchasing.
- Enter that exact ID and your organisation name at checkout.
- Paste the licence key from the confirmation page or purchase email into the Licensing card.
- Select **Activate full licence**.
- Set your preferred retention period in **CDR storage** and save the policy.

Activation does not run cleanup or change your current retention setting. A key for another installation or another app is rejected. Pasting a bad key does not replace an existing valid licence.

Keep the complete data folder backed up: it contains your installation identity and activated licence as well as records and settings. Preserve it during updates. Contact support before replacing an installation identity. If an installed key becomes invalid, cleanup is paused while the licence needs attention so a licence problem alone does not delete existing records.

Storage policy

The application storage policy considers both received CDR files and indexed application data.

When planning capacity, allow for:

- Incoming CDR source files.
- Database growth.
- Report/export files where applicable.
- Application logs.

- Update and rollback files.
- Temporary working space during upgrades.

Retention changes

Reducing a retention value may result in older data becoming eligible for removal.

Before making a significant retention or storage-policy change, confirm the organisation does not rely on the application as its only copy of required historical records.

Backups

Application backups should be included in the organisation's normal backup plan if the retained data or configuration is operationally important.

The managed updater creates a pre-update backup for rollback purposes. That mechanism is not a substitute for a broader backup strategy.

HISTORICAL IMPORT

Historical Import allows existing CDR files to be loaded into CDR Search Tool through the application interface.

This is useful when:

- The application is deployed after CDR files have already been collected elsewhere.
- Records need to be loaded for a defined historical investigation.
- A test installation needs representative CDR data without waiting for live SFTP delivery.

Import process

Use the historical import interface to select the CDR files intended for ingestion.

Import only files from a trusted source and from a CUCM environment whose records you are authorised to handle.

Retention still applies

Imported records are subject to the application's configured retention and storage policy.

For the public edition, historical data outside the supported 30-day retention window should not be relied on as permanently searchable data.

Validation

After import:

- Confirm the application reports successful processing.
- Search for a known record from the imported period.
- Review logs for any rejected or failed files.
- Confirm the imported time range is inside the active retention window.

UPDATES AND ROLLBACK

CDR Search Tool includes a managed updater designed to protect the existing installation before a new version is applied.

The project page lists the current release, version notes and SHA-256 checksum. The main download links to the current release. A permanent Full Licence includes future Call Records updates and remains valid for updates to that licensed installation. Preserve the data folder so the installation identity and licence survive the update.

Before updating

Before applying an update:

- Confirm the new version is intended for the installed release.
- Ensure sufficient free disk space is available.
- Avoid updating during an active operational investigation where possible.
- Confirm no manual file copy or antivirus action is holding application files open.

Compatibility check

The updater performs a compatibility check before applying an update.

Do not bypass compatibility warnings unless the release documentation explicitly instructs you to do so.

Pre-update backup

A backup copy is created before the update is committed. This provides the source for rollback if the new version fails validation.

Update validation

After updating:

- Confirm the application starts.
- Sign in.
- Confirm the expected version is displayed.
- Confirm the SFTP receiver state.
- Run a basic search.
- Review logs for startup or migration errors.

Rollback

If the updated build cannot be validated, use the managed rollback process to restore the previous working copy.

Rollback protects application continuity, but operators should still maintain normal backups for important configuration and data.

LOGS AND TROUBLESHOOTING

The Logs page provides application and security information required for routine troubleshooting.

Logs support pagination and search so operators can narrow a busy log history.

CDR files are not arriving

Check:

- The SFTP receiver is enabled.
- TCP port 22 is reachable from CUCM.
- CUCM has the correct host, credentials and `/incoming` path.
- Windows Firewall or another security product is not blocking the connection.
- The Windows host address has not changed.

Files arrive but calls are not searchable

Check:

- Ingestion logs for parsing or processing errors.
- The search date, time and timezone.
- The number format stored by CUCM.
- The active retention window.
- That the expected CDR file was processed successfully.

Web interface is unavailable

Check:

- The application is running.
- TCP port 3080 is listening.
- Windows Firewall permits access.
- The browser is using the correct host and port.

For local testing, try:

```
http://localhost:3080
```

User cannot sign in

Confirm the account exists, is enabled and has the expected role.

An administrator can reset the user's password using the user-management workflow.

Update fails

Review the updater output and application logs. Common causes include:

- Application files being locked by another process.
- An incomplete release package.
- Missing runtime components in a package.
- Insufficient permissions or disk space.

If the update cannot be validated, use rollback rather than repeatedly modifying the installed application in place.

Escalation information

When raising an issue, capture:

- Application version.
- Windows version.
- Approximate time of the problem.
- Relevant log entries.
- Whether the problem affects ingestion, search, reporting, login or updating.
- Whether the issue can be reproduced.