



CALL RECORDING

Screen Recording

Administrator

 **MOMENTUM**

Powered By:  **MiaRec**

1. Screen Recording Introduction

This guide describes the procedures that may be completed by Administrators (as required) for the optional (\$) add-on Call Recording screen recording application.

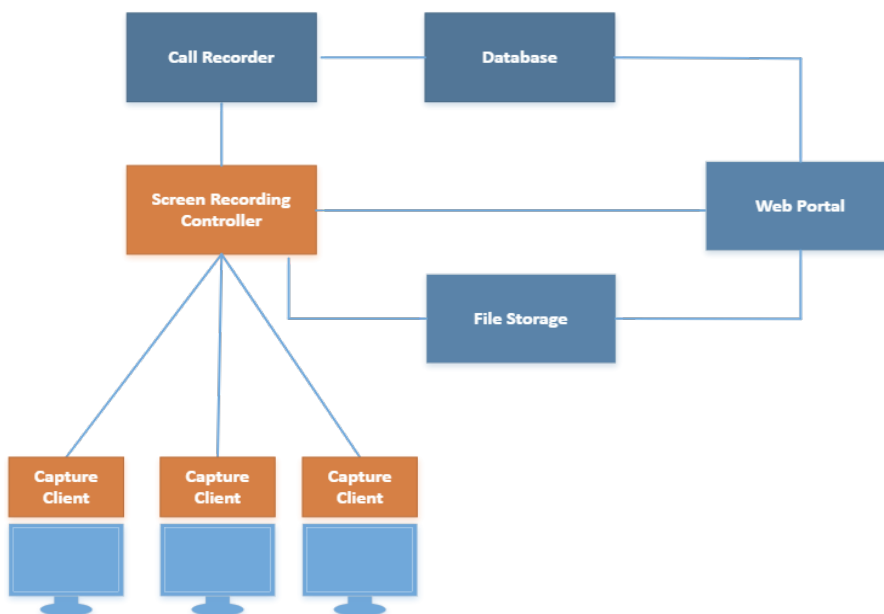
2. How it works

2.1 Architecture

Call Recording solution relies on Screen Recording Client running on agent desktops to perform screen captures during a call.

The controller application is responsible for the authentication of clients and initiating the capture process when the agent handles a new call.

The following diagram illustrates a high-level architecture of the Call Recording screen recording solution. The next chapters cover the architecture in more detail.



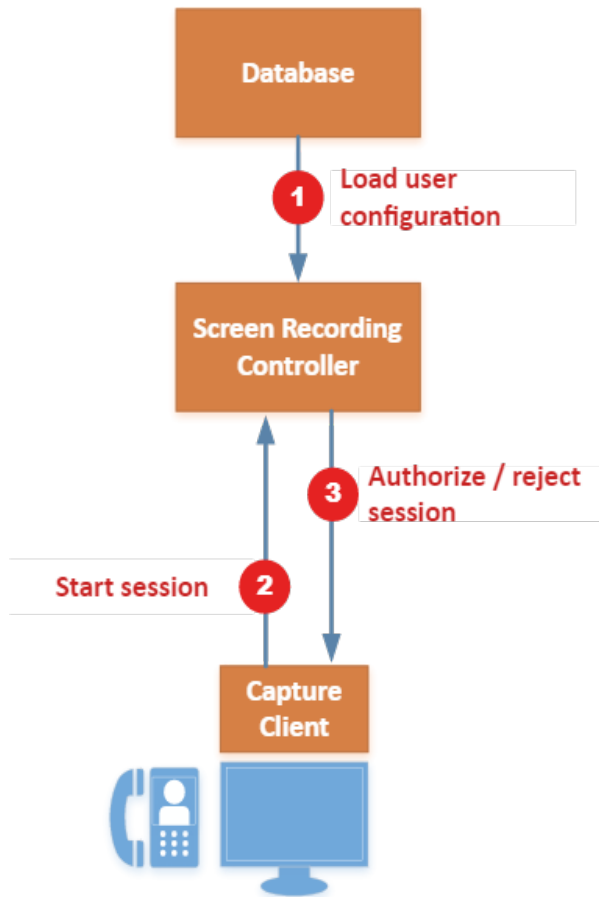
Components:

- The Screen Recording Client runs on the Agent's workstations as a Windows Service.
- The Screen Recording Controller authenticates all clients and controls a recording process, i.e. starts/stops screen capturing when agents receive/make calls.
- When the call ends, the Client uploads the video file to the server for storage and playback.

2.2 Authorization phase

When the Client application is deployed on a new computer, it has to be authorized first by the system administrator (menu Screen recording -> Screen recording workstations).

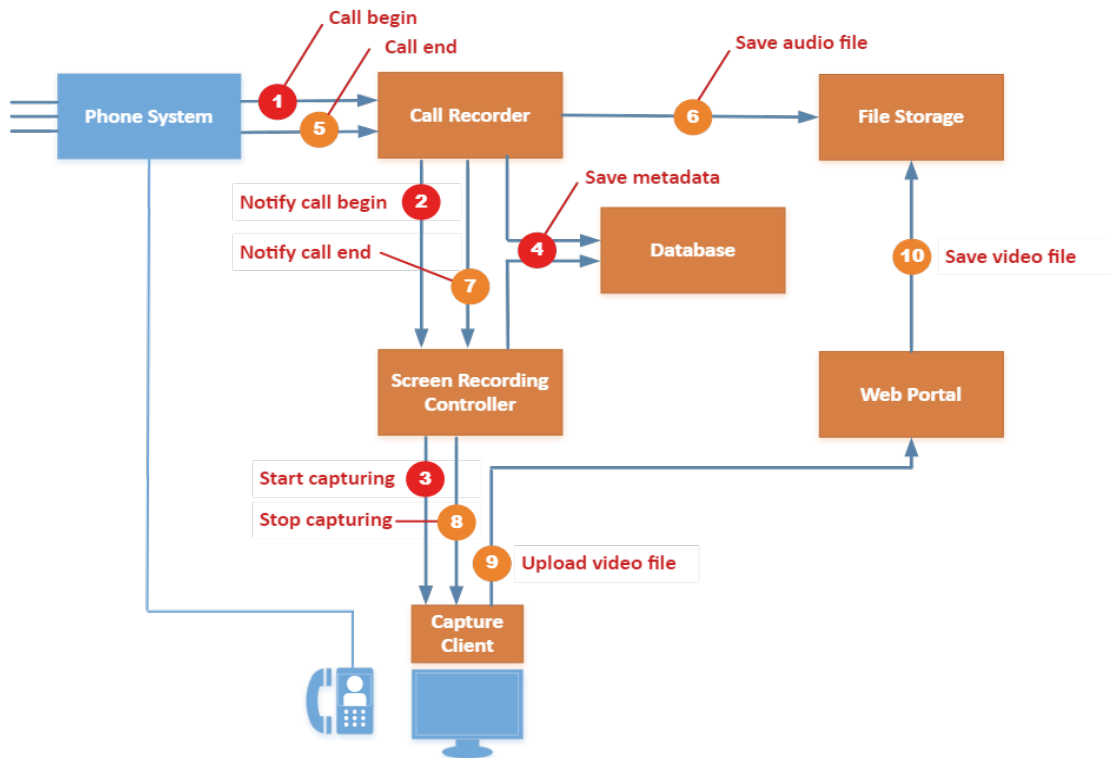
The following diagram illustrates the authorization phase:



2.3 Recording phase

Once the Screen Capture Client is authorized and associated with the corresponding agent profile, it automatically starts screen recording when the agent receives/makes calls.

The following diagram illustrates a recording process in detail:



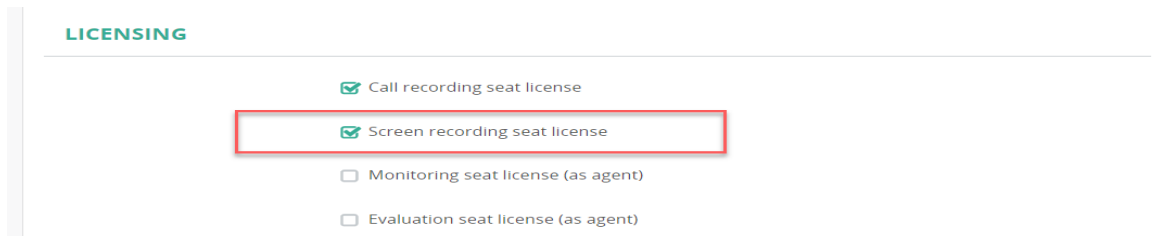
1. The Call Recording **Call Recorder** detects a new call from the **Phone System**.
2. The **Call Recorder** notifies the **Screen Recording Controller** about the particular agent has a new call
3. The **Screen Recording Controller** locates the active session for that agent and sends **Start capturing** command to the **Capture Client**
4. Both **Call Recorder** and **Screen Recording Controller** save metadata in **Database**, so users can playback audio and video recordings using the **Web Portal**.
5. The **Call Recorder** detects the call end event.
6. The **Call Recorder** saves the recorded audio file to the **File Storage**.
7. The **Call Recorder** notifies the **Screen Recording Controller** about the call end.
8. The **Screen Recording Controller** sends **Start capturing** command to the **Capture Client**. If wrapup recording is enabled, then the screen capturing process continues for a pre-defined amount of time, usually for a couple of minutes. Otherwise, a screen capturing is completed immediately.
9. The **Capture Client** uploads the recorded video file to the **Web portal**.
10. The **Web Portal** service stores the file in the **File Storage**

3. Installation

3.1 Configure licensing

3.1.1 Assign licenses to users

Navigate to **Administration -> User Management -> Users**. On user profiles, check the **Screen recording seat license** for each of the eligible users.



3.2 Configure storage

Navigate to menu **Administration -> Storage -> Storage Targets**. Click **Add** to create a storage target for screen recording files (*.mp4). Files can be stored:

- Locally on the same server as the Call Recording web application
- Remotely on FTP, SFTP server
- Remotely in Amazon S3 bucket

The following screenshot demonstrates configuration of local storage in directory `/var/Call Recording/screen_recordings`.

On Linux system, configure folder permissions.

For local storage target, configure permissions for the directory. This directory should be writable by Apache web server process. On Centos 6/7, execute the command:

```
chown -R apache:apache /var/Call Recording/screen_recordings
```

On Ubuntu:

```
chown -R www-data:www-data /var/Call Recording/screen_recordings
```

On Windows, there is no need to configure permissions for folder.

3.3 Configure screen recording settings

Navigate to menu Administration -> Screen Recordings -> Screen Recording Settings. Configure the following settings:

- **Storage Target** (created in the previous steps)
- **Capture frame rate** (how often to capture screen per second)
- **Bit-rate** (compression level)
- **Maximum screen recording duration** (limits maximum size of video file).
- **Maximum width/height** of the captured image. Call Recording automatically resizes the image. This setting is per-monitor, i.e. in multi-monitor configuration, the picture is downsized only when either of monitors has larger resolution.
- **Multi-monitor** recording. Record a primary monitor only or all monitors.

Administration > Screen Recording > Screen Recording Settings

Edit Screen Recording Settings

STORAGE SETTINGS

Storage Host URL

URL of the storage server for screen recordings (it should be accessible from outside by the clients). The clients automatically upload the recorded video files to that server. In a single-server setup, it should be the same as the web portal. In a multi-server setup, it is possible to a dedicated server the file upload traffic. Format examples: http://miarec.example.com, https://10.0.0.5:8443

Storage Target *

Video file name format *

Parameterized file name format

RECORDING SETTINGS

Capture rate (fps) *

Wrap-up time (seconds) seconds
The screen recording continues for the specified amount of time after the voice interaction completes

Max recording duration (seconds) seconds
The recording is automatically terminated after the the specified amount of time passes. This value should be at least as large as the longest call.

Max file duration (seconds) seconds
The recording session may consists of multiple smaller files. This option specifies the maximum duration of individual file.

Multi-monitor support

Record primary monitor only

Record all monitors

Max image width pixels
Maximum width of the captured screen image. If the actual monitor width is bigger, then the screen image is automatically resized

Max image height pixels
Maximum height of the captured screen image. If the actual monitor height is bigger, then the screen image is automatically resized

Video file bitrate kbps
 The lower bitrate, the smaller file size and the worse quality. The higher bitrate, the bigger file size and the better quality

NETWORK SETTINGS

Controller TCP port
 Listening TCP port for Client -> Controller communication (use 0 to disable TCP)

Controller TLS port
 Listening TLS port for encrypted Client -> Controller communication (use 0 to disable TLS)

SSL private key file
 Location of PEM-encoded private key file for inbound TLS connections from clients. The private key will be automatically generated if does not exist yet.

SSL certificate file
 Location of PEM-encoded certificate file for inbound TLS connections from clients. The certificate will be automatically generated if does not exist yet.

SSL CA certificates (optional)
 This optional directive sets CA certificates used to verify the client certificate on Client Authentication. It should point to all-in-one file containing concatenated PEM-encoded CA

Important! If Call Recording is deployed on Linux, then make sure the Apache process has write permissions to the storage target directory.

On Centos, run as an example:

```
chown -R apache:apache /var/Call Recording/screen-recordings
```

On Ubuntu, run:

```
chown -R www-data:www-data /var/Call Recording/screen-recordings
```

Assuming that directory `/var/Call Recording/screen-recordings` is used for storing of uploaded video files

3.4 Generate security token

3.4.1 A single-tenant configuration - generate token

This step applies only to a single-tenant configuration!

Navigate to Administration -> Screen Recording -> Screen Recording Settings to view the current Screen recording token (see below screenshot).

This token should be used during installation of the Screen Recording Client application.

Administration > Screen Recording

Screen Recording Settings

[Edit Configuration](#)

SCREEN RECORDING TOKEN

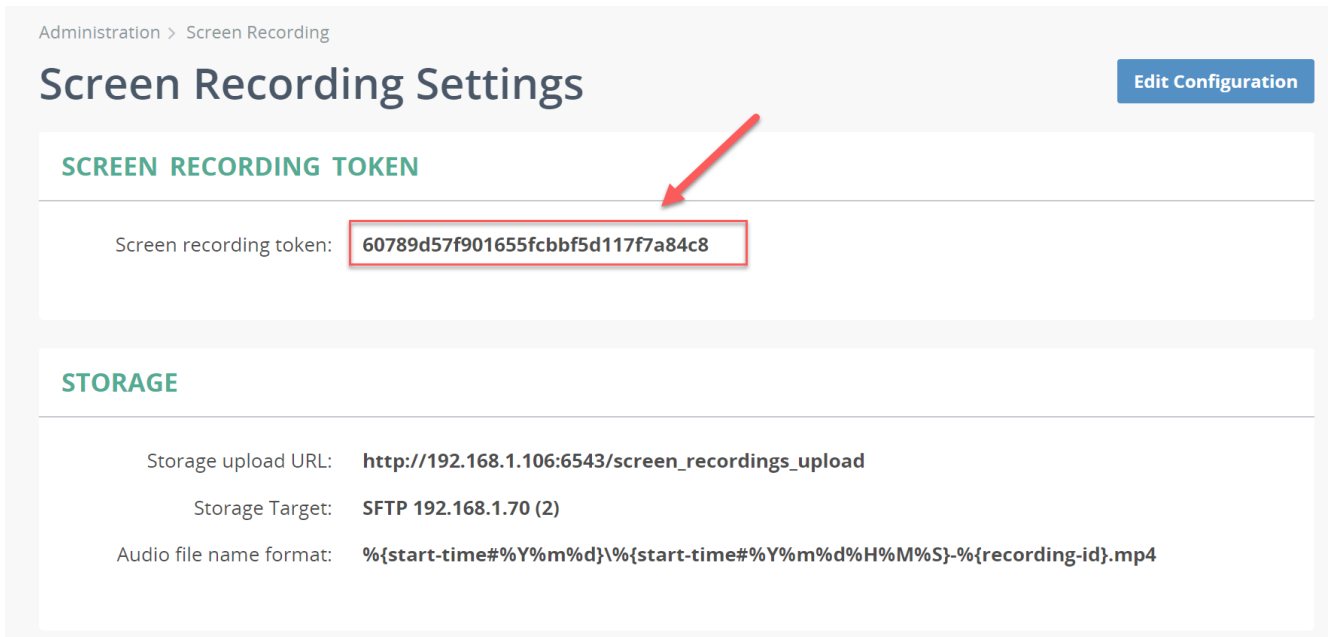
Screen recording token: **60789d57f901655fcbbf5d117f7a84c8**

STORAGE

Storage upload URL: **http://192.168.1.106:6543/screen_recordings_upload**

Storage Target: **SFTP 192.168.1.70 (2)**

Audio file name format: **%{start-time#%Y%m%d}\%{start-time#%Y%m%d%H%M%S}-%{recording-id}.mp4**



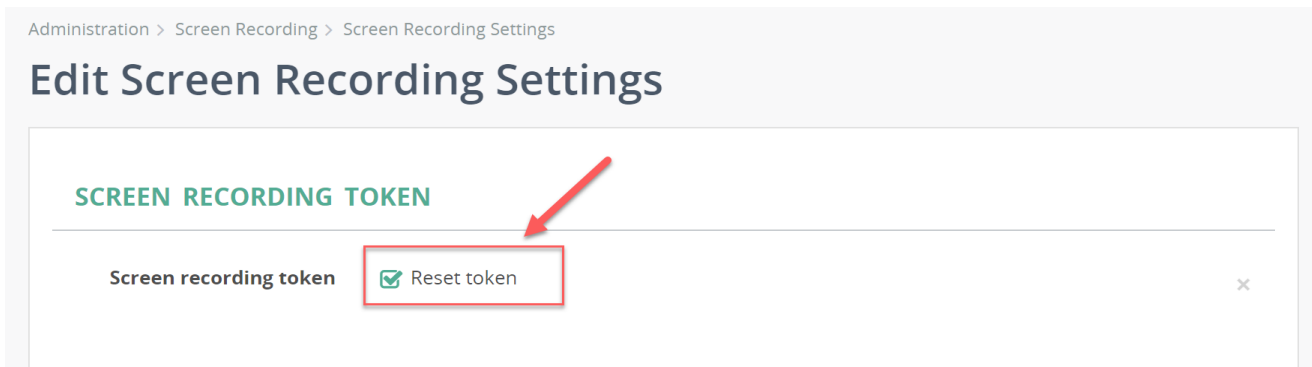
To generate new token, click **Edit Configuration** button and check **Reset token** option.

Administration > Screen Recording > Screen Recording Settings

Edit Screen Recording Settings

SCREEN RECORDING TOKEN

Screen recording token Reset token ×



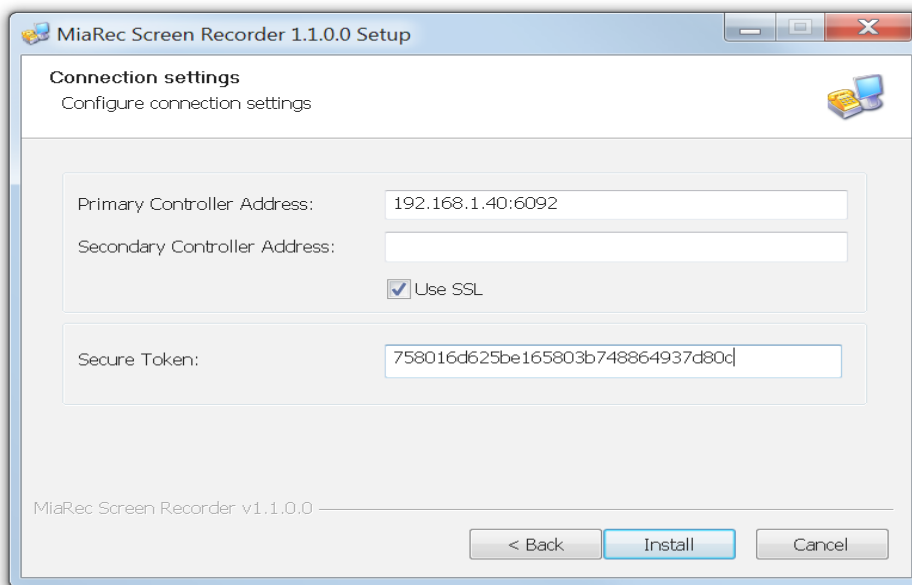
3.5 Install client application

Contact your service provider to get the Call Recording Screen Recorder application. Once provisioned, they can be installed on the agent desktops.

Supported operating systems: Windows 7, 8, 10, Server 2008/2012/2016 with the latest windows updates installed.

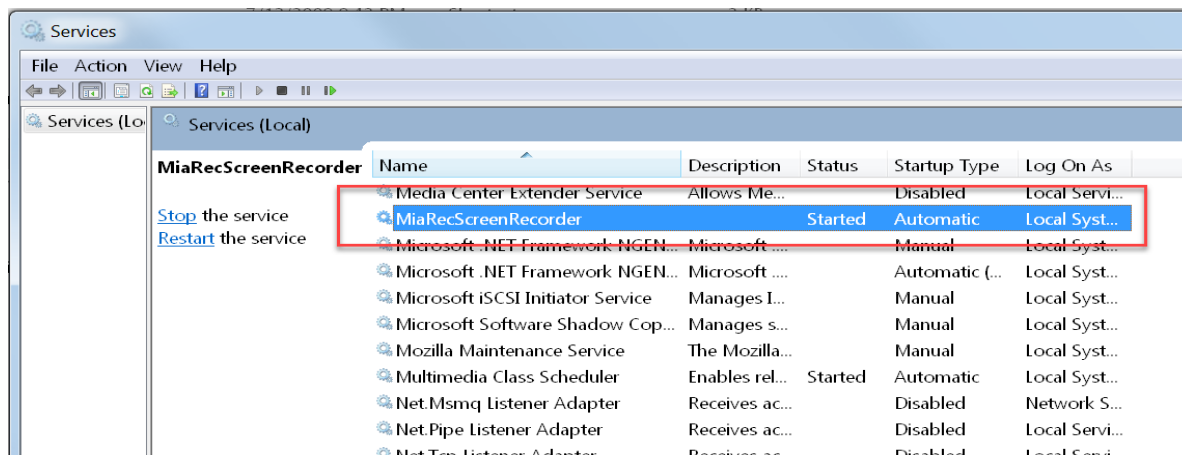
During installation, provide the address of the Call Recording Screen Controller server and "Secure Token". You can retrieve the secure token on the tenant profile page (see above).

Enter the IP-address or DNS name of Call Recording server in the Primary Controller Address field. By default, port 6092 is used for SSL connection and 6091 for non-SSL connection (see Administration -> Screen Recording -> Screen Recording Settings for exact port values).



3.5.1 Verify installation

Call Recording Screen Recording Client silently works in background. It is visible Control Panel -> Services.

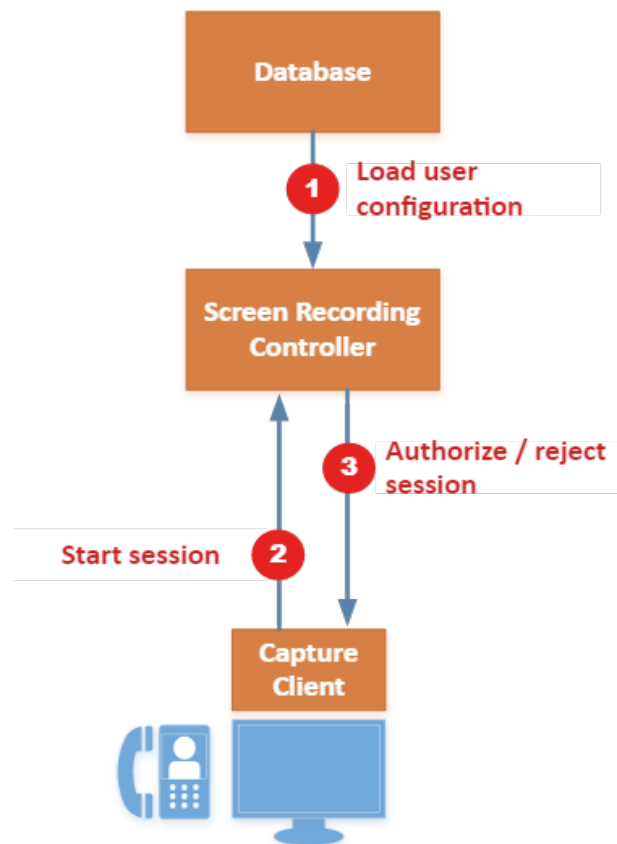


Also, you can see the application in the list of running processes.

| Image Name | User Name | CPU | Memory (...) | Description |
|---------------------------------|---------------|-----|--------------|------------------------------------|
| lsass.exe | SYSTEM | 00 | 2,260 K | Local Security Authority Process |
| lsm.exe | SYSTEM | 00 | 1,296 K | Local Session Manager Service |
| MiaRecScreenRecorder.exe | SYSTEM | 00 | 1,144 K | MiaRecScreenCaptureService |
| MiaRecScreenRecorderCapture.exe | IEUser | 00 | 568 K | MiaRecScreenCapture |
| MiaRecScreenRecorderService.exe | SYSTEM | 00 | 404 K | ServiceWrapper |
| MiaRecScreenRecorderService.exe | SYSTEM | 00 | 504 K | ServiceWrapper |
| mmc.exe | IEUser | 00 | 2,760 K | Microsoft Management Console |
| msdtc.exe | NETWORK SE... | 00 | 2,028 K | Microsoft Distributed Transacti... |
| SearchFilterHost.exe | SYSTEM | 00 | 836 K | Microsoft Windows Search Filte... |
| SearchIndexer.exe | SYSTEM | 00 | 4,608 K | Microsoft Windows Search Inde... |
| SearchProtocolHost.exe | SYSTEM | 00 | 1,268 K | Microsoft Windows Search Prot... |
| services.exe | SYSTEM | 00 | 3,248 K | Services and Controller app |
| smss.exe | SYSTEM | 00 | 196 K | Windows Session Manager |
| spoolsv.exe | SYSTEM | 00 | 3,784 K | Spooler SubSystem App |
| sppsvc.exe | NETWORK SE... | 00 | 1,392 K | Microsoft Software Protection P... |
| svchost.exe | SYSTEM | 00 | 2,164 K | Host Process for Windows Serv... |
| svchost.exe | NETWORK SE... | 00 | 2,224 K | Host Process for Windows Serv... |

3.6 Authorize new workstations

The capturing client application automatically establishes a network connection with the Call Recording screen recording controller. New workstation requires authorization before it can record screen.



Every workstation is uniquely identified using the automatically generated secure workstation token. The administrator can authorize new workstations using Call Recording Web UI. Navigate to menu Administration -> Screen Recording -> Screen Capture Workstations.

New workstations are shown in the Pending authorization tab. Select the corresponding workstation(s) and authorize them.

Administration > Screen Recording

Screen Capture Workstations

Search by Domain, Computer Name, IP address Search

All Clients Authorized Pending Authorization Forbidden

Authorize Forbid Delete Selected rows: 3 0-13 of 13

| <input type="checkbox"/> | AUTHORIZATION | DOMAIN | COMPUTER NAME | IP-ADDRESS | |
|-------------------------------------|---------------|--------|---------------|------------|------|
| <input checked="" type="checkbox"/> | Pending | | | | View |
| <input checked="" type="checkbox"/> | Pending | | | | View |
| <input checked="" type="checkbox"/> | Pending | | | | View |
| <input type="checkbox"/> | Pending | | | | View |

3.7 Configure users for screen recording

Navigate to Administration -> User Management -> Users and click Edit for the corresponding user profile.

3.7.1 Step 1. Configure Screen Recording Login

Under Recording settings, configure the Windows login name in the Screen recording login attribute. This value should match to username, the user is using to login to Windows machine. Optionally, you can specify a domain name if your organization has multiple domains.

RECORDING SETTINGS

Record Always On-demand Never Default

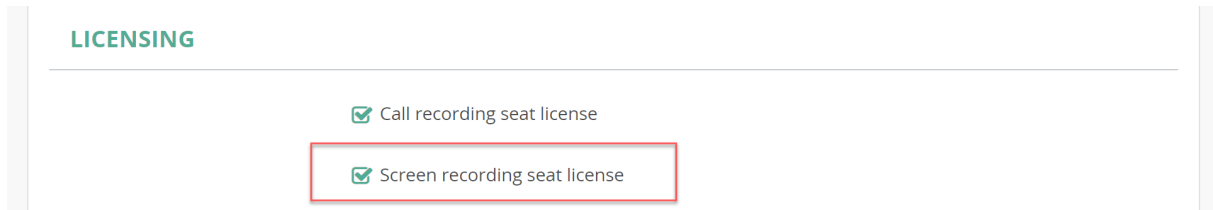
Record direction Inbound Outbound

Extension ×
[Add Extension](#)

Confidential calls Automatically mark all calls of this user as confidential

Screen Recording Login
Supported formats: NETBIOS\login, DOMAIN\login, login

3.7.2 Step 2. Assign Screen recording license



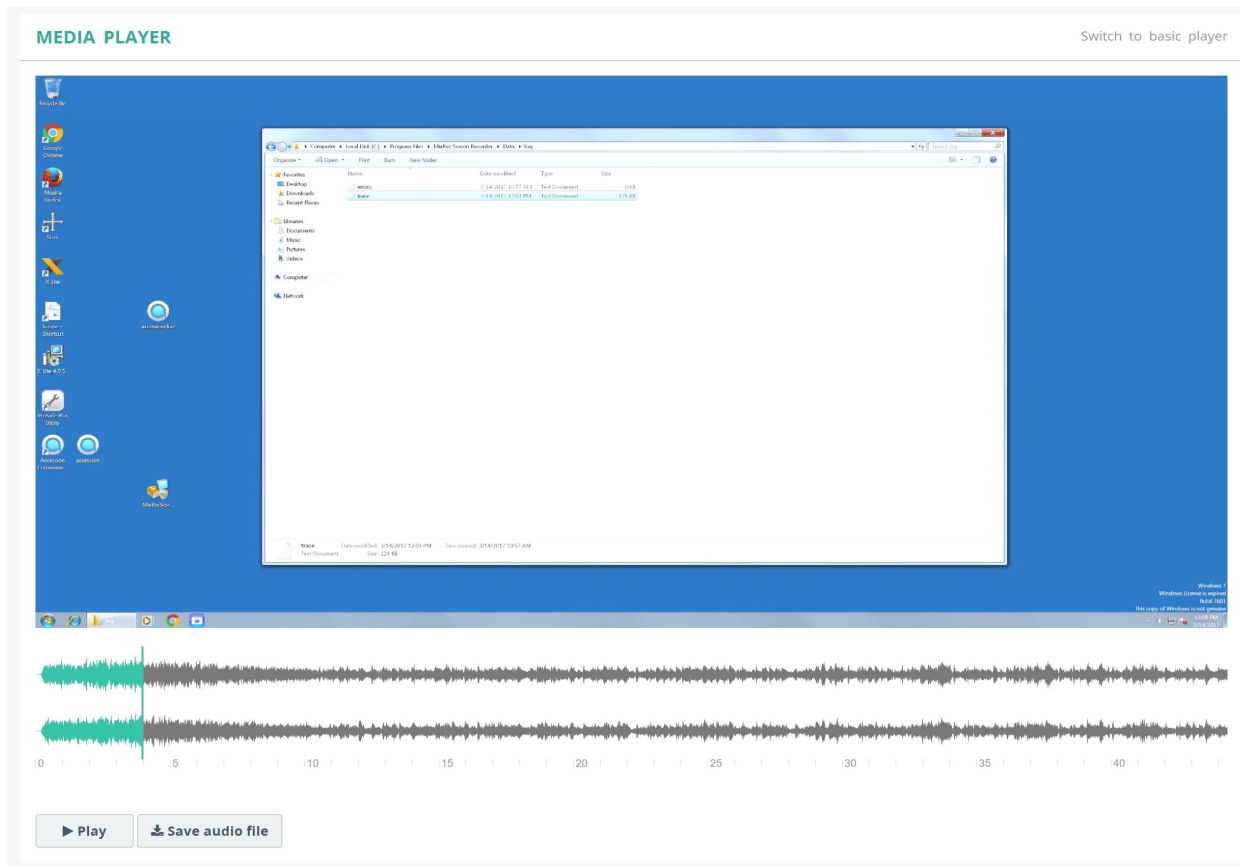
Under Licensing, assign the Screen recording seat license to user.

If user logs into to the authorized workstation using the configured login name, a screen capture will be activated automatically.

3.8 Verify screen recording

Make a test call to verify screen recording.

Once a call is completed, the video file should be automatically uploaded to the central storage server. You will be able to playback both audio and screen recordings simultaneously.



Upload process may take some time depending on network speed between client and server. The message Screen recording file is not uploaded yet is shown when upload is not completed yet:

Call 281558487 -> 300

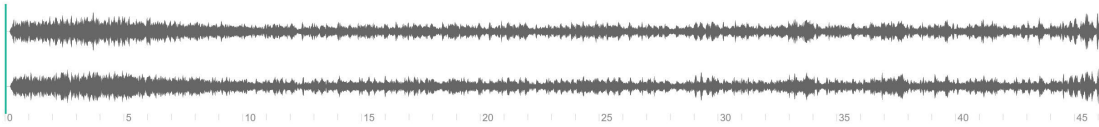
[Mark as confidential](#)

[Delete Call](#)

MEDIA PLAYER

[Switch to basic player](#)

Screen recording file is not uploaded yet



[▶ Play](#)

[📄 Save audio file](#)

INFO

Tenant: [Flexus](#)
Date: [Today](#)
Connect Time: [12:01:46 PM](#)
Disconnect Time: [12:02:33 PM](#)
Duration: [0:47](#)
Watermark: [View](#)

FROM

User:
Phone Number: [281558487](#)
Phone Name:
Phone Id: [281558487](#)
Ip-address: [192.168.1.106 \(3000\)](#)
[📍 Live monitor phone 281558487](#)

TO

User: [Justin Amado](#)
Group: [Users](#)
Phone Number: [300](#)
Phone Name:
Phone Id: [300](#)
Ip-address: [192.168.1.40 \(5070\)](#)
[📍 Live monitor phone 300](#)

4. Troubleshooting

4.1 Troubleshooting on Client Side

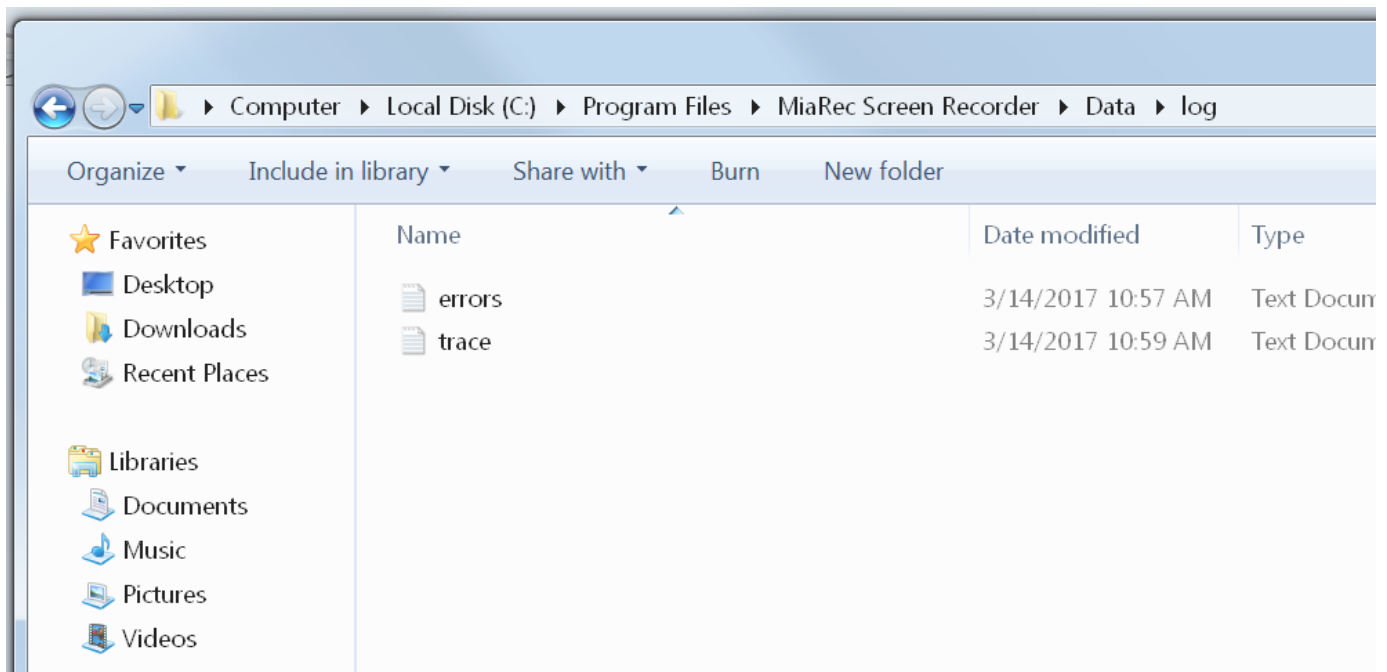
4.1.1 Enable logging for service application

By default, the client application doesn't write logs. Navigate to `INSTALL-FOLDER\Bin` and edit the file `Call RecordingScreenRecorder.ini`. Change `Enable` to 1 in the section `[Trace]`:

```
[Trace]
Enable=1
File=<INSTALL-FOLDER>\Data\log\trace.log
```

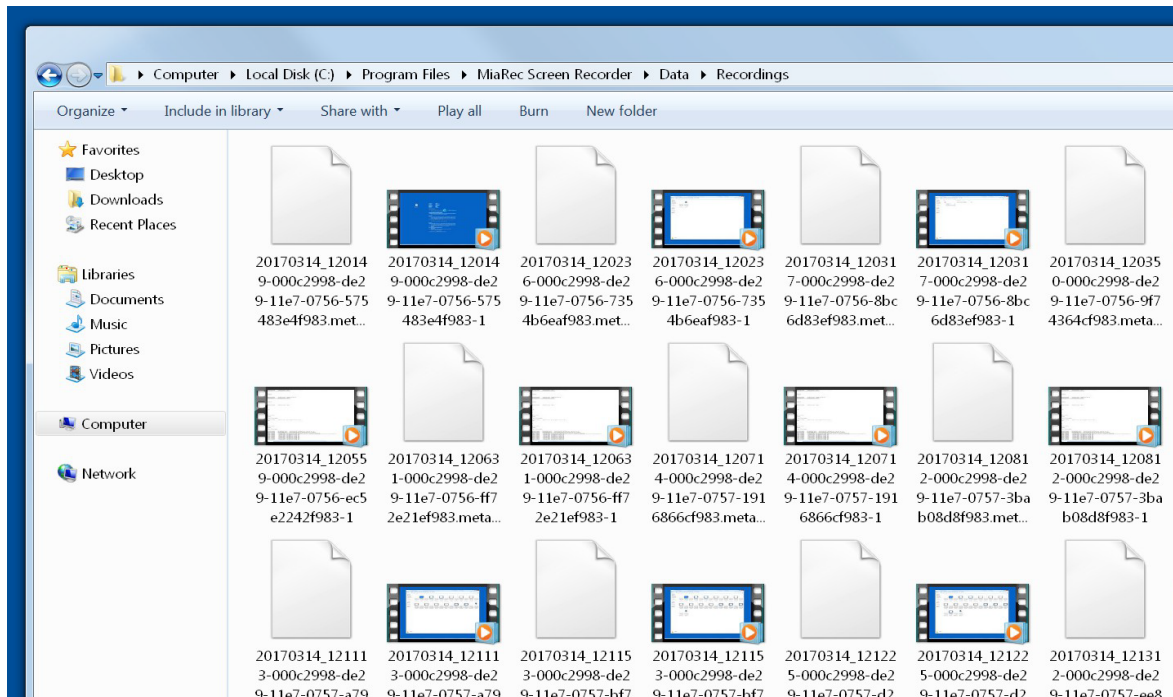
Restart Service Call Recording Screen Recorder.

Once enabled, the logs are written into `INSTALL-FOLDER\Data\log\trace.log` file. Optionally, you can change the location of the log file by editing the `File` parameter in the INI file.



The video files are stored temporarily in the directory `INSTALL-FOLDER\Data\Recordings`. The client application

automatically uploads the recorded files to the central storage server after call completion. Once uploaded, the files are removed from local storage. You can verify if any of the files are recorded by the client but not uploaded yet.



4.1.2 Enable logging for desktop capturing process

To enable logging for the capturing process, first, create a new directory on the computer where non-privileged users can write files. It should be outside of C:\Program Files. For example, create the directory C:\Call RecordingLogs

Then, navigate to **INSTALL-FOLDER\Bin** and edit the file `Call RecordingScreenRecorder.ini`

Under section [Recording] edit the parameter CaptureProcessArgs. Change it to:

```
CaptureProcessArgs = -t tttt -o C:\Call RecordingLogs\ScreenRecDesktop.log
```

Note, the directory C:\Call RecordingLogs should exist, and it should be writable by non-privileged users.

4.2 Troubleshooting on Server Side

If the screen recording doesn't appear on the server for too long, then you need to check logs on both the server and the client. First, check System Log on the server (menu **Administration -> Maintenance -> System Log**).

One of the common issues is insufficient permissions to the upload directory. The following screenshot shows one of such cases.

```

response = handler(request)
File "/var/www/miarec/pyenv/lib/python3.4/site-packages/pyramid-1.5.6-py3.4.egg/pyramid/router.py", line 163, in handle_
response = view_callable(context, request)
File "/var/www/miarec/pyenv/lib/python3.4/site-packages/pyramid-1.5.6-py3.4.egg/pyramid/config/views.py", line 596, in _
return view(context, request)
File "/var/www/miarec/pyenv/lib/python3.4/site-packages/pyramid-1.5.6-py3.4.egg/pyramid/config/views.py", line 329, in a
return view(context, request)
File "/var/www/miarec/pyenv/lib/python3.4/site-packages/pyramid-1.5.6-py3.4.egg/pyramid/config/views.py", line 305, in p
return view(context, request)
File "/var/www/miarec/pyenv/lib/python3.4/site-packages/pyramid-1.5.6-py3.4.egg/pyramid/config/views.py", line 385, in v
result = view(context, request)
File "/var/www/miarec/pyenv/lib/python3.4/site-packages/pyramid-1.5.6-py3.4.egg/pyramid/config/views.py", line 491, in _
response = getattr(inst, attr)()
File "/var/www/miarec/app/miarecweb/views/admin/screen_recording_upload_views.py", line 604, in view_upload_file_content
os.makedirs(new_directory, exist_ok=True)
File "/usr/local/lib/python3.4/os.py", line 227, in makedirs
makedirs(head, mode, exist_ok)
File "/usr/local/lib/python3.4/os.py", line 237, in makedirs
mkdir(name, mode)
PermissionError: [Errno 13] Permission denied: '/var/miarec/screen_recordings'
    
```

In this case, you just need to grant the write permission on that folder to the Apache web server user account:

```

mkdir -p /var/Call Recording/screen_recordings
chown apache:apache /var/Call Recording/screen_recordings
    
```

Additionally, you can enable trace on the server side. Navigate to menu Administration -> Screen Recording -> Screen Recording Settings and enable detailed trace logging.

TRACE LOG SETTINGS

Enable * Enable writing of trace log information into file

Trace log file name * Full path to file trace log file

Trace level * Depth of trace information (from 1 to 5). Default is 5

Rotate * When rotating the log file will be renamed into new one with name "**.yyyyMMdd-hhmmss.EXT" (EXT is file extension)

Rotate day * For weekly rotation, one of [Mon, Tue, Wed, Thu, Fri, Sat, Sun, 1, 2, 3, 4, 5, 6, 0]. For monthly rotation a day from 1 to 31. For monthly rotation a day from 1 to 31

Rotate time * For hourly rotation format is MM (minutes). For daily, weekly and monthly rotation format is HH:MM (hour and minutes)

5. Deploy Screen Capture Client with Windows Group Policy

5.1 Create a Transform (MST) file

This article describes how to prepare Transform (MST) file for Windows installer.

What is a Transform?

A Transform (*.MST) file allows you to collect installation options for programs that use the Microsoft Windows Installer in a file. They can be used on the Installer (MSIEXEC.EXE) command line, or used in a software installation Group Policy in a

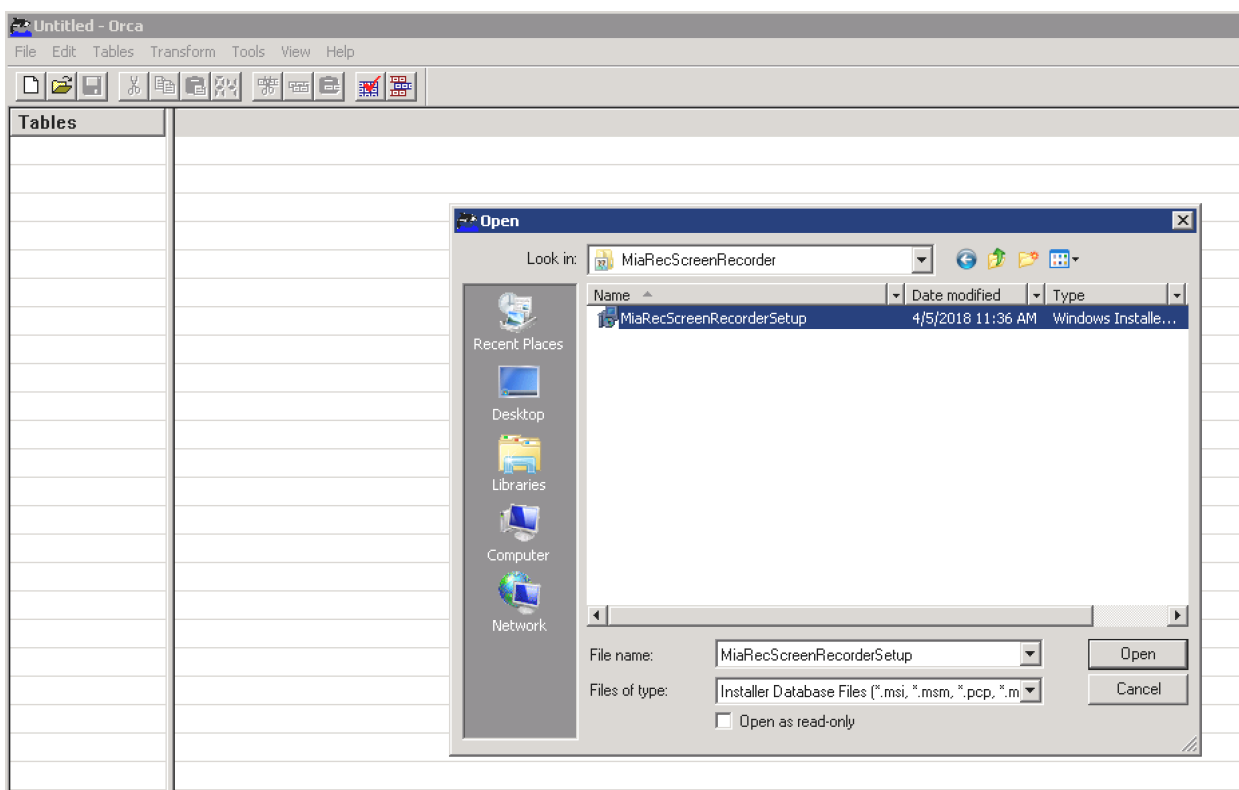
Microsoft Active Directory domain.

Use Orca utility to prepare a packaged installation of Call Recording screen recording client. You can download Orca as a part of Windows SDK or by contacting your Call Recording representative.

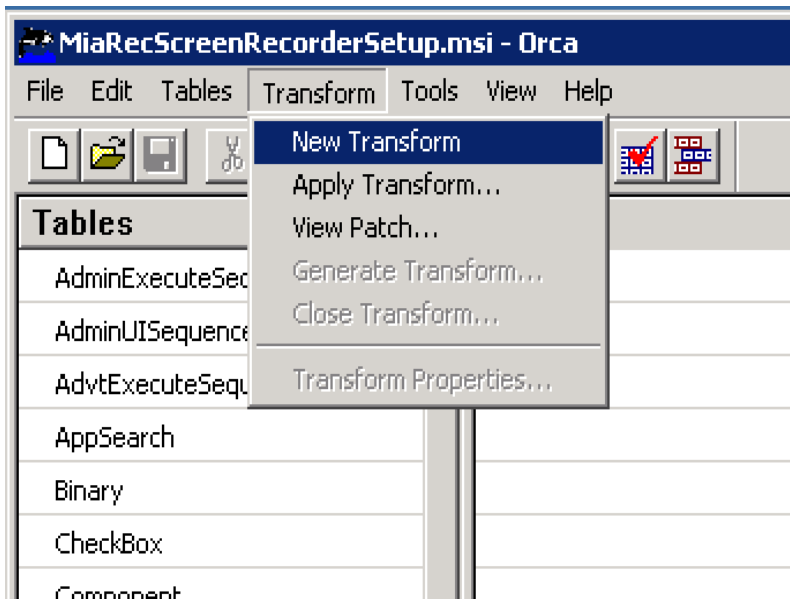
What is Orca?

Orca.exe is a database table editor from Microsoft for creating and editing Windows Installer packages and merge modules. The tool provides a graphical interface for validation, highlighting the particular entries where validation errors or warnings occur. More details can be found on Microsoft web-site.

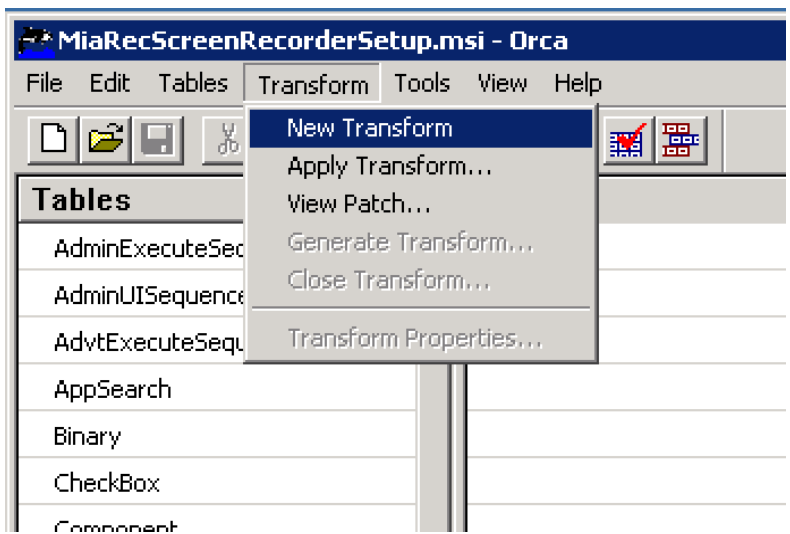
Open Call RecordingScreenRecorderSetup.msi in Orca utility.



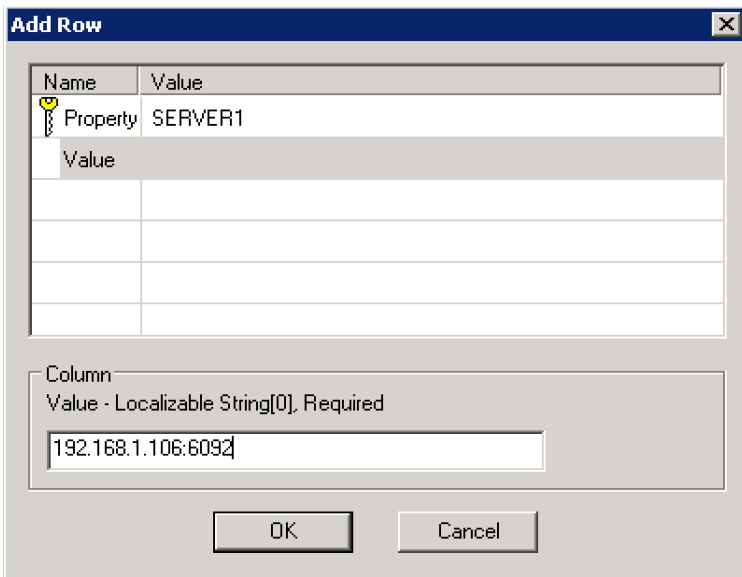
Select New Transform from the Transform menu.



Select Property in the Tables pane on the left.



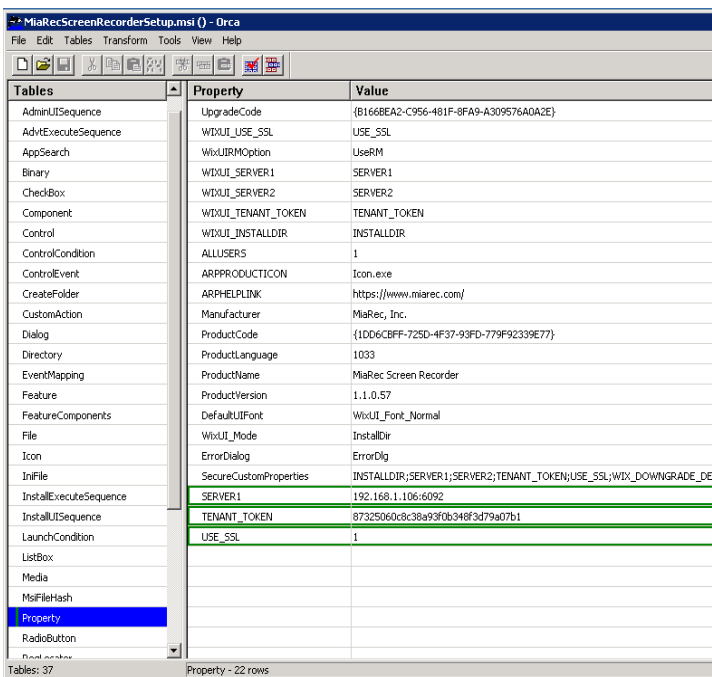
In the right pane, right-click on empty space and choose Add Row.



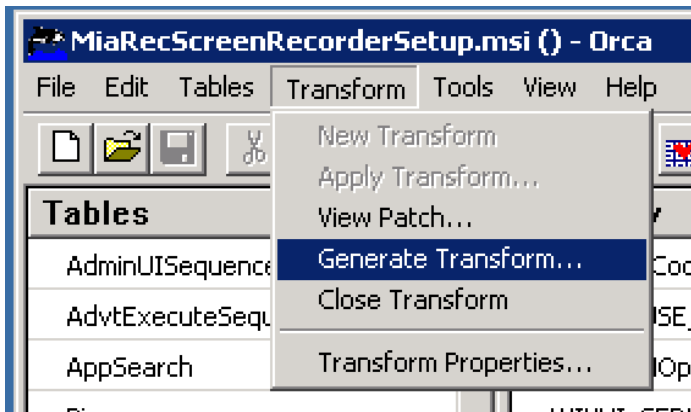
Create the following parameters:

| Property | Value | Description |
|--------------|---------|--|
| SERVER1 | IP:PORT | 1st Call Recording screen recording server |
| SERVER1 | IP:PORT | 2nd Call Recording screen recording server (optional) |
| TENANT_TOKEN | STR | Screen recording token as configured in Call Recording web portal |
| USE_SSL | 1 or 0 | Set to 1 if encrypted channel is used (default port is 6092). Set to 0 if encrypted channel is not used (default port is 6091) |

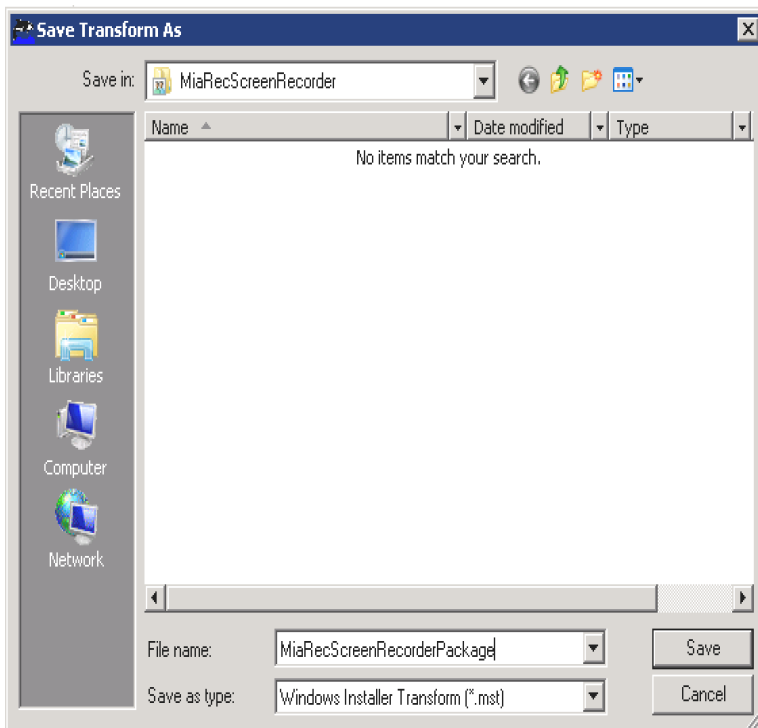
The following screenshot shows an example configuration



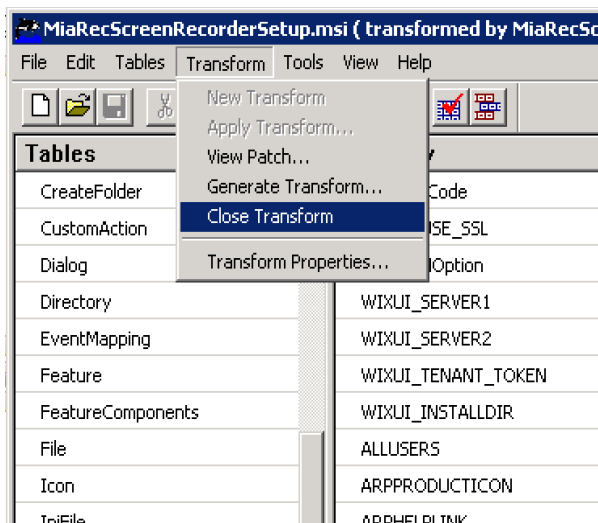
When finished, select "Generate Transform..." from menu "Transform"



Save the generated Windows Installer Transform file (*.mst).



Select "Close Transform" from the menu "Transform"

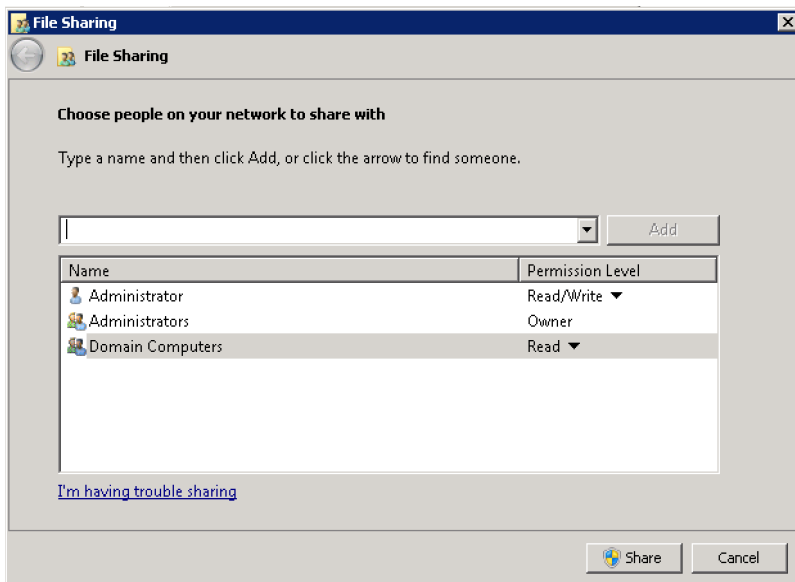
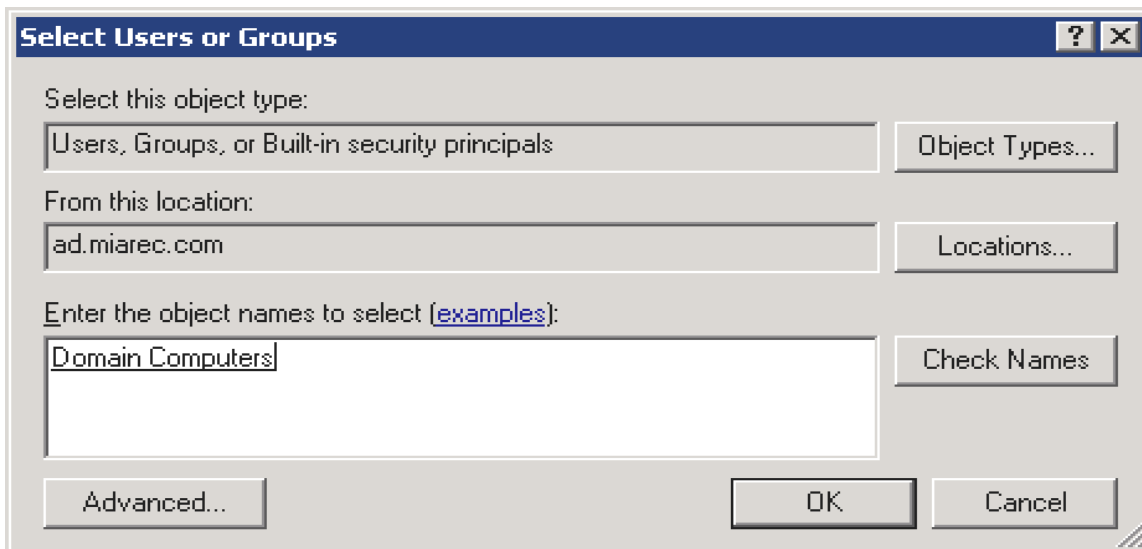


5.2 Put the MSI and MST files in a file share

You need to create a folder somewhere on your server that you can remember and find, like the documents folder or the desktop. You need to put the MSI as well as MST files in this new folder, and then right-click the folder, and go to "Share with" -->

"Specific people".

Type "Domain Computers" in the search box, and then give the "Domain Computers" account read permissions and click "Share".



5.3 Create a new GPO

5.3.1 Step 1. Create GPO

Open Group Policy Management from Start --> Administrative Tools --> Group Policy Management. If it is not installed, go to the Server Manager (also in Administrative tools) and go to the Features tab on the left hand side and then click Add

Features in the pane on the right. Check the box in the new window that says Group Policy Management, and then click through the next few screens. It will install and then you can open it like described before.

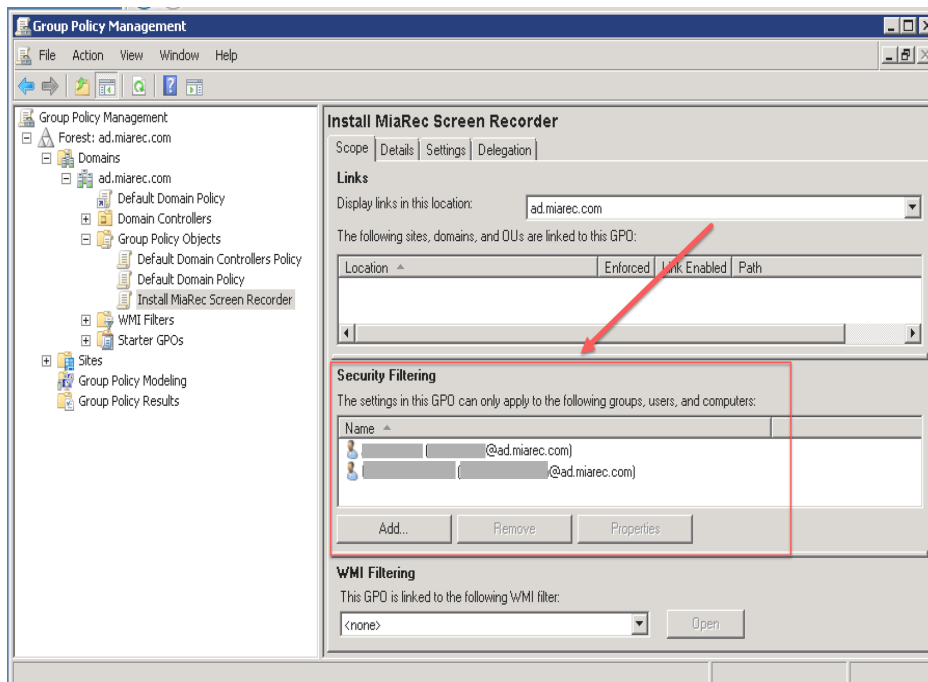
Navigate to Forest: YOURDOMAIN --> Domains --> YOURDOMAIN --> Group Policy Objects. Right click the folder Group Policy Objects and click New. Type in a name for your GPO. Once you create your new GPO, it will show up under the Group Policy Objects folder.

5.3.2 Step 2. Select computers on which to deploy the software

Click on the new GPO with the name that you just assigned. In the right pane on the bottom, there is a box that says Security Filtering. Click on and remove the Authenticated Users entry.

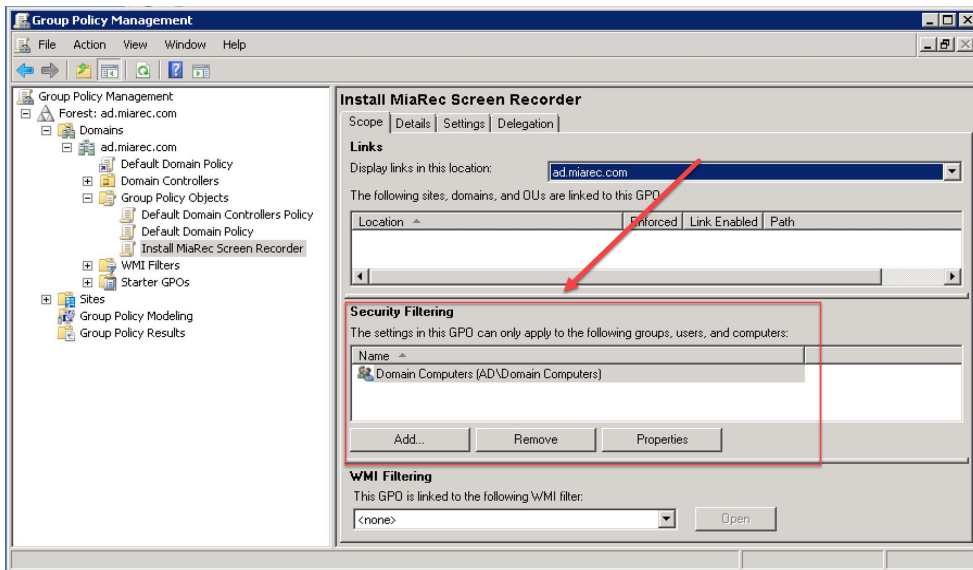
Option 1. Deploy software for certain users

If you want this program deployed on certain computers, add all of the specific computer names that you want the software to be deployed on.



Option 2. Deploy on all domain computers

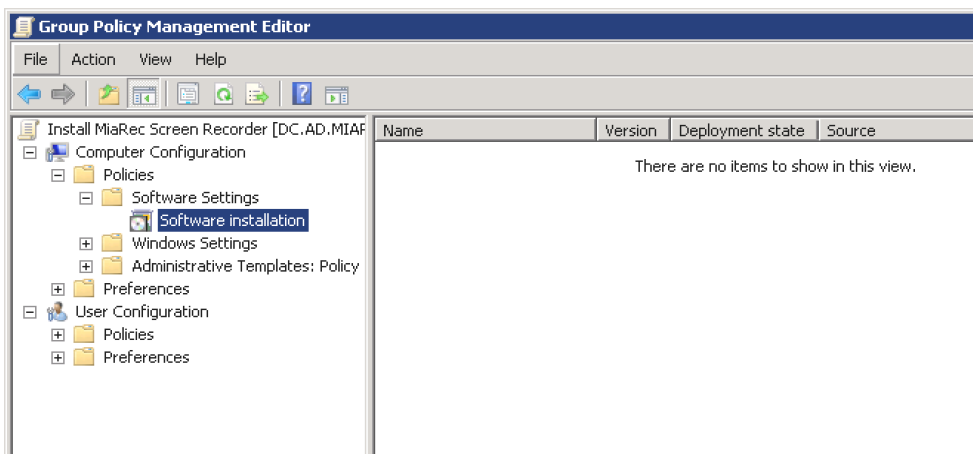
if you want it on all computers, add the group "Domain Computers". Go back up to the "YOURDOMAIN" folder (in the navigation pane) and right-click it. Click "Link an existing GPO". Click your new GPO's name and click OK.



5.3.3 Step 3. Create a Software installation

Now go back to the GPO under Group Policy Objects folder, and right-click it. Click on Edit.

A new window will open. Navigate to Computer Configuration --> Policies --> Software Settings --> Software installations.



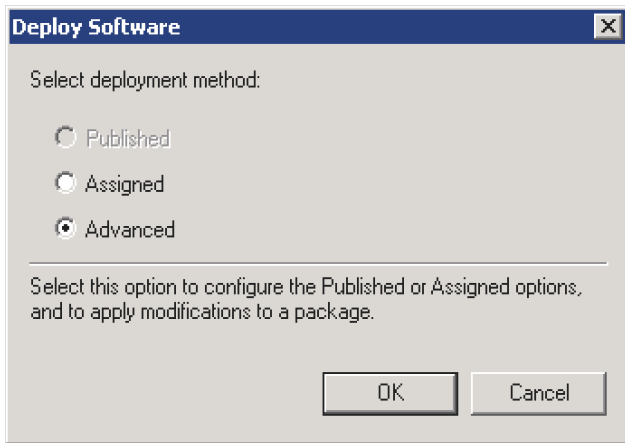
Right click inside the empty pane on the right and go to New --> Package...

In the new windows that pops up, Navigate to the share that you created earlier using the full Universal Naming Convention

(UNC) path like (\\YOURSERVERNAME\FOLDERNAME), not the physical folder on the server (C:\FAKEPATH\FOLDERNAME) and select your MSI.

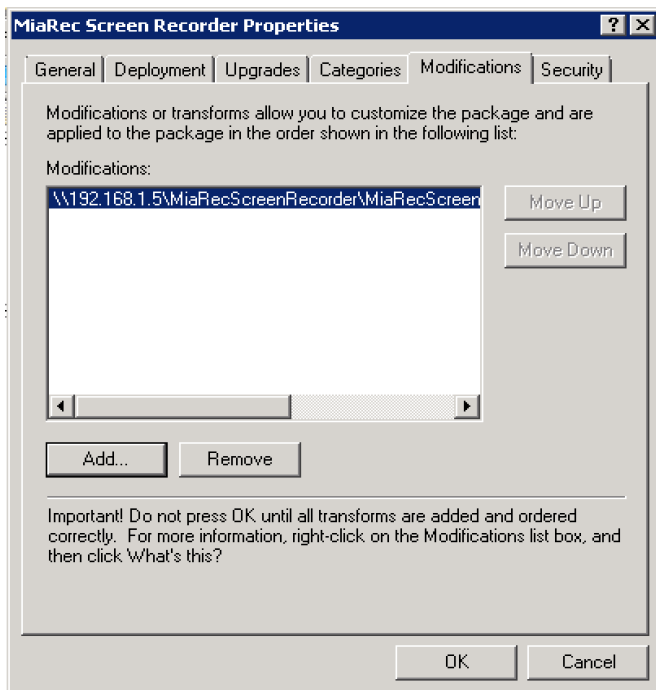
Click Open.

On Select deployment method, select Advanced. If you select another option, you won't be able to apply the MST file you created.



Open Modifications tab. Select your MST file (that customizes your installation) from the network share.

Note: Again, it is very important to use a UNC to the file (to the network share), rather than a local/network drive path.



Click OK to complete the setup.

Close the Group Policy snap-in, click OK, and then close the Active Directory Users and Computers snap-in.

5.3.4 Reboot workstations (optional)

When the workstations re-start, the software package is automatically get installed with the pre-configured parameters (Note: It may take 2-3 restarts for the server to update the GPO on the workstations).